Программа сетевой академии
Cisco CCNA® 1 и 2
Вспомогательное руководство

Третье издание, исправленное и дополненное

Cisco Networking Academy Program
CCNA® 1 and 2 Companion Guide

Revised Third Edition

Cisco Press

201 West 103rd Street
Indianapolis, IN 46290 USA

Программа сетевой академии
Cisco CCNA® 1 и 2
Вспомогательное руководство

Третье издание, исправленное и дополненное

ВИЛЬЯМС

Москва • Санкт-Петербург • Киев
2008

ББК 32.973.26-018.2.75
П78
УДК 681.3.07

Издательский дом "Вильямс"

Зав. редакцией *С.Н. Тригуб*

Перевод с английского *С. Балицкого*, *Г. Клапанова*, *А.Н. Крикуна*, канд. физ.-мат. наук *А.В. Мысника*, *А.П. Павленко*, *А.Н. Узниченко*

Под редакцией канд. физ.-мат. наук *А.В. Мысника*

По общим вопросам обращайтесь в Издательский дом "Вильямс" по адресу:
info@williamspublishing.com, http://www.williamspublishing.com
115419, Москва, а/я 783; 03150, Киев, а/я 152

Корпорация Cisco Systems, Inc.

П78 Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-е изд., с испр.: Пер. с англ. — М.: Издательский дом "Вильямс", 2008. — 1168 с.: ил. — Парал. тит. англ.

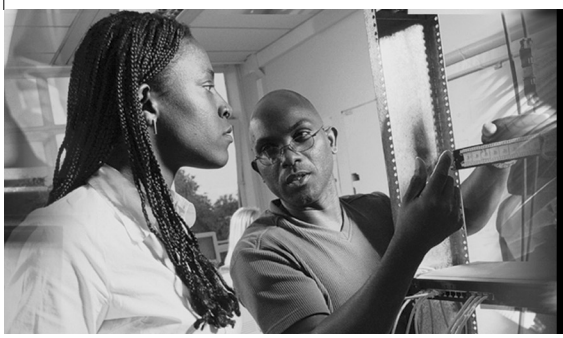
ISBN 978-5-8459-0842-1 (рус.)

Эта книга предназначена для приобретения и закрепления знаний и практических навыков в построении, настройке и обслуживании локальных компьютерных сетей. Концепции и понятия, подробно изложенные в ней, позволят получить неоценимые сведения по установке кабельных систем, маршрутизации, IP-адресации, протоколах маршрутизации и обслуживанию сетей. В книге рассмотрены основы модели OSI, описаны такие понятия, как коллизии, сегментации сетей. В издание включены новые главы, посвященные технологии Ethernet и коммутации в сетях Ethernet. Кроме того, в этом учебном пособии более подробно рассмотрены особенности операционной системы IOS, протоколов TCP/IP и списков управления доступом.

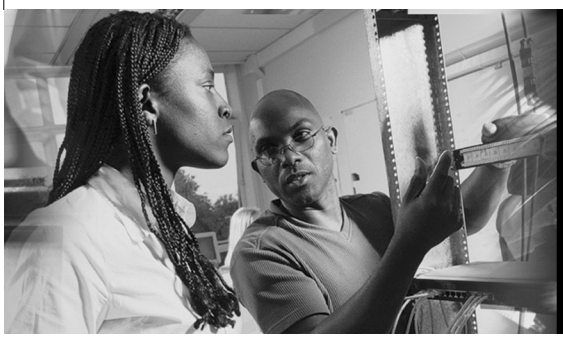
ББК 32.973.26-018.2.75

Книга подготовлена при участии Региональной сетевой академии Cisco, http://www.academy.ciscopress.ru.

ISBN 978-5-8459-0842-1 (рус.)
ISBN 1-58713-150-1 (англ.)



Оглавление



Содержание

Отзывы

Издательство Cisco Press стремится создавать высококачественные книги, подробно рассказывающие о технических вопросах сетевых технологий. Каждое издание подвергается строгому редактированию. В книгах используются материалы, предоставленные сертифицированными экспертами и ведущими специалистами в рассматриваемой области.

Отзывы читателей — это естественное развитие процесса обсуждения книги. Если у вас есть какие-либо комментарии или предложения, как можно улучшить данную книгу или изменить ее таким образом, чтобы она лучше соответствовала потребностям читателей, вы можете связаться с издательством по электронной почте `networkingacademy@Ciscopress.com`. В сообщении указывайте, пожалуйста, полное название книги и номер ISBN.

Издательство и корпорация Cisco благодарят вас за помощь.

Технические рецензенты

Билл Чэпмэн (Bill Chapman) в данный момент преподает информатику в средней школе в Аркадии (Arcadia). Он ведет курсы по компьютерным приложениям, языкам программирования C++ и Java, курсы, связанные с сертификационными экзаменами CCNA и CompTIA A+. Билл является членом академического комитета преподавателей по методическим вопросам (Academic Mentor Planning Committee), комитета по чрезвычайным ситуациям (Emergency Planning Committee), а также сертифицированным инструктором по новым технологиям (Certified District Technology Instructor) для сотрудников учебных заведений. Билл также ведет курсы на кафедре компьютерных технологий колледжа города Пасадена (Pasadena) и принимает участие в работе нескольких комитетов, которые занимаются вопросами материалов для курсов Cisco и CompTIA A+ в рамках программы по трудоустройству округа Лос-Анджелес (Los Angeles County Regional Occupational Program). Периодически Билл выступает с презентациями по методам преподавания курсов Программы сетевых Академий Cisco на Калифорнийской промышленной конференции в секции, посвященной сотрудничеству и обучению специалистов. Билл является сертифицированным инструктором Cisco по программе CCNA и имеет сертификаты CompTIA A+, Network+ и I-Net+.

Аллан Джонсон (Allan Johnson) является владельцем собственного дела в течение 10 лет. Он стал преподавателем в 1999 году и посвятил большую часть своих сил обучению молодежи и взрослых. Аллан имеет два диплома магистра университета A&M-Corpus Christi штата Техас: магистерские степени по бизнес-управлению и педагогике. На сегодняшний день он является инструктором по информационным технологиям средней школы Мэри Кэрролл (Mary Carroll High School) и колледжа Дель Мар (Del Mar) университета Corpus Christi штата Техас. Кроме всего прочего, Аллан часть своего времени тратит на работу в службе поддержки инструкторов CCNA/CCNP Программы академий Cisco.

Рик Грациани (Rick Graziani) работает в сфере компьютерных сетей и телекоммуникационных технологий более 20 лет. На данный момент он является преподавателем компьютерных наук и технологий в колледже Кабрилло (Cabrillo) города Аптос (Aptos), Калифорния. Имеет диплом бакалавра искусств университета Лойола Мэримаунт (Loyola Marymount) и степень магистра искусств по компьютерным наукам и теории систем государственного университета Калифорнии Монтерей Бэй (California State University Monterey Bay). Рик интересуется протоколами маршрутизации, в частности, протоколом OSPF версии 3, и сетями MANET. Он также имеет сертификаты CCNP и CCAI. Рик хотел бы поблагодарить своих друзей и коллег Марка Булутиана (Mark Boolootian), Дэйва Барнетта (Dave Barnett), Джима Ворнера (Jim Warner) и Фреда Бейкера (Fred Baker) за их помощь и советы в течение долгих лет совместной работы и отдельно хотел бы сказать спасибо своей жене Тери (Teri) за помощь и поддержку.

Элани Хорн (Elanie Horn) была инструктором региональной Академии Cisco и преподавателем обучающего центра академий (CATC), начиная с 1998 года. У нее есть дипломы бакалавра искусств и магистра естественных наук государственного университета Огайо по специальности, связанной с преподаванием математики. Элани преподает более 27 лет. На данный момент она работает в образовательной компьютерной ассоциации Tri-Rivers (так называется обучающий центр академий — CATC, Cisco Academy Training Centre) и занимается поддержкой и подготовкой инструкторов сетевых академий Cisco в штатах Кентукки, Мичиган, Огайо. Элани имеет сертификаты CCNA, CCDA и инструкторский сертификат CCAI.

Эндрю Лардж (Andrew Large) был инструктором региональной сетевой Академии с 1998 года. У него есть диплом бакалавра искусств и магистра педагогики, а также степень специалиста по образованию университета Южной Алабамы. Эндрю работал в сфере образования 13 лет и выступал в качестве преподавателя корпорации Cisco во многих странах мира. В настоящий момент Эндрю владеет своим собственным консультационным агентством по компьютерным сетям и является инструктором локальной и региональной Академий Cisco в рамках соответствующей программы. Он имеет сертификаты CCNA, CCNP и CCAI.

Энтун В. Рафи (Antoon W. Rufi) — сетевой профессионал, который работал на военно-воздушные силы Соединенных Штатов Америки до июня 2000 года. Более 20 лет он имел дело с военной авиацией и разнообразными системами, начиная с межконтинентальных баллистических ракет Титан II и заканчивая современными высокоточными метеорологическими и навигационными сетями. После увольнения из армии Тони работал в коммерческом технологическом колледже ECPI в Вирджинии. На данный момент он является директором отделения последипломного образования данного колледжа. Тони получил диплом по специальности инженер-электронщик в колледже военно-воздушных сил, степень магистра наук в университете Южного Иллинойса по индустриальным технологиям и степень магистра в университете Мэриленд (Maryland) по информационным технологиям. Тони имеет сертификаты CCNA, CompTIA Network+ и сдал экзамены по маршрутизации и средствам удаленного доступа, которые связаны с сертификатом CCNP.

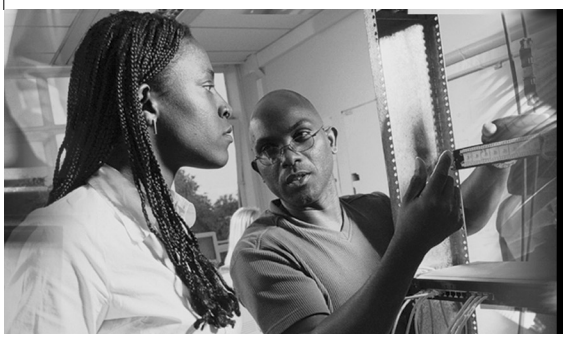
Условные обозначения сетевых устройств Cisco Systems

В документации и литературе корпорации Cisco Systems, Inc для обозначения сетевых устройств и топологий используются стандартные пиктограммы и значки. На рисунке ниже показаны пиктограммы, которые используются в данной книге.

Соглашения по синтаксису команд

Представленные ниже соглашения по синтаксису команд аналогичны соглашениям, используемым в *Справочнике по командам операционной системы IOS* (IOS Command Reference). В упомянутом справочнике используются следующие соглашения:

- вертикальной чертой (|) разделяются альтернативные, взаимоисключающие элементы;
- в квадратных скобках [ ] указываются необязательные элементы;
- в фигурных скобках { } указываются необходимые элементы;
- **полужирным** шрифтом выделяются команды и ключевые слова, которые вводятся буквально, как показано; в примерах реальной конфигурации и сообщений системы (а также необычный синтаксис команд) с помощью жирного шрифта указываются команды, которые вводятся пользователем вручную (например, команда **show**).



Предисловие

Сеть Internet предоставила практически неограниченные возможности общения и обмена информацией как для специалистов, так и для их работодателей во всем мире. Коммерческие компании и государственные организации столкнулись с неимоверным ростом производительности за счет инвестирования средств в устойчивые телекоммуникационные технологии. В последнее время в специализированной прессе появились статьи, которые оптимистично обещают существенный прирост производительности и рост оборотов в отраслях, связанных с телекоммуникациями. Рост производительности, эффективности производства, его прибыльности и общего уровня жизни косвенным образом связан с телекоммуникациями.

Рост производства и валового продукта нельзя обеспечить просто закупкой сетевого оборудования. Чтобы заставить современные сети работать, чтобы спланировать, разработать, установить, сконфигурировать, поддерживать, сопровождать современные телекоммуникации, находить и устранять неисправности, нужны высококвалифицированные специалисты. Сетевые администраторы должны быть уверены, что обеспечен необходимый уровень безопасности сети и что ее работоспособность будет поддерживаться на должном уровне. Сеть должна обеспечивать необходимый уровень производительности. Сетевым администраторам также следует внедрять новые технологии, которые предоставят дополнительные возможности, будут отвечать растущим запросам предприятия или организации и способствовать расширению сети.

Чтобы удовлетворить постоянно растущий спрос на квалифицированных специалистов по объединенным сетям, корпорация Cisco Systems основала академическую программу Сетевых Академий (Cisco Networking Academy Program — CNAP). Программа Сетевых Академий — это сложный и разносторонний курс, который позволит читателям данной книги и слушателям курсов получить необходимые навыки по работе с Internet-технологиями и стать квалифицированными специалистами. В программе Сетевых Академий органично объединены обучение с преподавателем, Web-ориентированные интерактивные материалы, интерактивные экзамены, интерактивные "зачетки", практические занятия и лабораторные работы, консультации и подготовительные курсы к экзамену на сертификат международного образца.

Разработанная корпорацией Cisco система обучения является смешанной. Она основана на интерактивных экзаменах, которые сдаются непосредственно на обучающем Web-сайте компании, и опирается на опыт и поддержку сертифицированных инструкторов, которые ведут разнообразные курсы по многим темам по всему миру. Следует также отметить, что корпорация Cisco обеспечивает круглосуточную поддержку своих учебных центров и Академий семь дней в неделю круглый год. Курсы, которые разработаны компанией и преподаются в Сетевых Академиях, постоянно улучшаются и дополняются на основании статистики, которую Cisco

Systems ведет на основании отзывов учащихся и результатов тестирования. Программа курса достаточно часто изменяется и отражает пожелания учащихся и новые тенденции в сетевых технологиях. Инфраструктура глобальной системы обучения корпорации Cisco (Cisco Global Learning Network) была создана для обеспечения полнофункциональной интерактивной персонализированной программы обучения для слушателей курсов Cisco во всем мире. Основной девиз компании звучит так: "Сеть Internet изменяет образ жизни, образ мышления, принцип обучения и игры человека". Программа Сетевых Академий корпорации Cisco воплощает этот девиз в жизнь.

Эта книга является одним из бестселлеров серии изданий для программы Сетевых Академий. Серия разработана совместно группой Worldwide Education (всемирная группа по образованию) и издательством Cisco Press и преставляет собой дополнительные учебные материалы к интерактивной версии программы Сетевых Академий Cisco, которые доступны на специализированном Web-сайте. Книги этой серии являются единственными авторизированными учебниками Сетевых Академий от корпорации Cisco Systems и комплектуются материалами на компакт-дисках, которые содержат сопроводительные лабораторные работы и видеоматериалы, оказывающие неоценимую помощь в изучении сетевых технологий.

Я надеюсь, что, как выбранная вами профессия, так и ваше обучение по программе Cisco Systems и технологиям сети Internet будут успешными. Я также надеюсь, что вы продолжите свое обучение в сфере сетевых технологий и телекоммуникаций после того, как завершите курсы Сетевых Академий. В дополнение к книгам, которые непосредственно связаны с образовательной программой корпорации Cisco, издательство публикует огромное количество как общеобразовательной литературы по сетевым технологиям, так и пособий для подготовки ко многим сертификационным экзаменам, справочники и руководства. Корпорация Cisco, со своей стороны, с помощью авторизированных партнеров по обучению (Cisco Learning Partners) предоставляет множество специализированных и общих курсов по соответствующим темам. Партнеры по обучению предлагают различные виды курсов, интерактивное обучение (e-lrarning), курсы для самостоятельного изучения (self-paced) и обычные курсы под руководством квалифицированных преподавателей. Инструкторы, которые имеют право преподавать курсы, сертифицированы корпорацией Cisco и читают лекции по материалам, подготовленным ведущими специалистами компании. Когда вы прочтете эту книгу до конца, выполните все лабораторные работы, обратитесь к разделу Learning & Events (раздел по обучению) на Web-сайте корпорации за дополнительной информацией о сертификатах, информации о других курсах или с вопросами к технической поддержке образовательной программы компании .

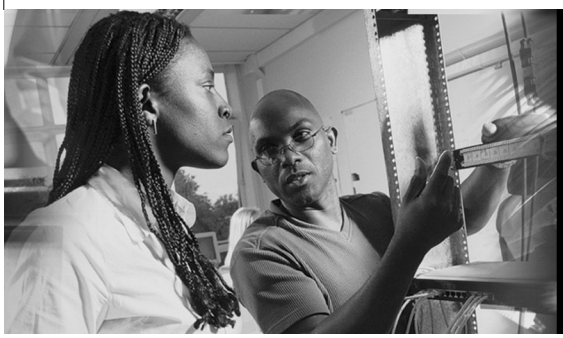
Спасибо Вам за то, что вы купили эту книгу и приняли решение участвовать в образовательной программе Сетевых Академий корпорации Cisco.

Кевин Ворнер (Kevin Warner)

Ответственный директор отдела маркетинга,

Всемирная образовательная программа,

корпорация Cisco Systems, Inc.



Введение

Эта книга представляет собой дополнительное издание по теоретическим и лабораторным занятиям, которые проводятся по программе Сетевых Академий Cisco. Учебный план академий разработан таким образом, чтобы помочь в трудоустройстве и дальнейшем обучении в области сетевых технологий и телекоммуникаций.

Книга, как и интерактивные материалы, использующиеся в Сетевых Академиях, посвящена основным вопросам, которые входят в сертификационный экзамен CCNA (Cisco Certified Network Associate). Стилистика и оформление книги совпадают с форматом, который принят для всех материалов, используемых в Академиях.

Данная книга предназначена для закрепления и расширения знаний и практических навыков в построении, настройке и обслуживании локальных компьютерных сетей (Local Area networks — LAN). Концепции и понятия, которые подробно изложены в книге, позволят получить неоценимые сведения по установке кабельных систем, маршрутизации, IP-адресации, протоколах маршрутизации и обслуживании сетей. В книге рассмотрены основы модели OSI, описаны такие понятия, как коллизии, сегментации сетей. В издание включены новые главы (которых не было в предыдущем курсе), посвященные технологии Ethernet и коммутации в сетях Ethernet. Кроме того, в данном учебном пособии более подробно рассмотрены особенности операционной системы IOS, протоколов TCP/IP и списков управления доступом (ACL — Access Control List).

Книга может служить пособием не только при подготовке к сертификационному экзамену CCNA, а также и к сертификационному экзамену CompTIA Network+.

Цель книги

Цель данной книги — расширение знаний о поддерживаемых компанией Cisco сетевых технологиях, о дизайне и принципах построения сетей, о настройке маршрутизаторов Cisco. Она предназначена для использования совместно с электронными учебными пособиями, которые применяются при подготовке специалистов по программе Сетевых Академий Cisco.

Для кого предназначена эта книга

Основная аудитория книги — это сетевые администраторы и студенты, увлекающиеся сетевыми технологиями. Пособие предназначено как для будущих студентов сетевых академий, так и для всех, кто хочет изучать принципы построения компьютерных сетей. В процессе обучения в Академиях книга может служить дополнительной литературой при работе с интерактивными материалами.

Книга также может быть использована в тренировочных центрах корпораций и персоналом компаний для повышения общего уровня знаний сотрудников. Она рассчитана на читателей без технического образования, не перенасыщена техническими терминами и поэтому удобна для тех, кому не нужны технические подробности.

Особенности книги

Книга построена таким образом, чтобы облегчить восприятие принципов построения сетей и маршрутизации. Пособие содержит следующие элементы:

- **В данной главе...** Каждая глава начинается со списка основных терминов, понятий и тем. После прочтения главы читатель должен досконально разбираться во всех перечисленных в начале главы пунктах;
- **Ключевые термины.** В каждой главе приводятся определения основных понятий, используемых в сетевых технологиях. Они также могут использоваться для закрепления пройденного материала или в качестве средства самоконтроля при переходе к изучению последующих глав книги;
- **Рисунки, примеры, таблицы и сценарии.** Книга содержит множество рисунков, примеров и таблиц, которые используются для пояснения теоретического материала, концепций, команд и последовательности настройки устройств и служат для закрепления и лучшего визуального восприятия содержимого главы. Кроме указанных элементов, специфические сценарии, которые описывают реальные ситуации, раскрывают часто встречающиеся практические проблемы и методы их решения;
- **Резюме.** В конце каждой главы представлен обобщенный список всего изложенного в ней материала. Краткое содержание всей главы может пригодиться в дальнейшем для повторения пройденного материала;
- **Контрольные вопросы.** В конце каждой главы приведены обзорные вопросы, которые используются для оценки усвоения материала главы, проверки степени готовности к изучению новых разделов книги;
- **Ссылки на лабораторные работы.** В книге встречаются ссылки на упражнения и лабораторные работы, описанные на компакт-диске, который прилагается к пособию. Эти упражнения позволяют совмещать теорию, изложенную в определенных главах, с практическими навыками и методами работы. Ссылки на лабораторные работы сопровождаются следующей пиктограммой:

- **Ссылки на дополнительные материалы на компакт-диске.** В каждой главе содержатся ссылки на интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные

понятия и термины, которые изложены в данной главе. Ссылки на дополнительные материалы сопровождаются следующей пиктограммой:

Как построена эта книга

Книга содержит 22 главы, 3 приложения и состоит из двух частей: CCNA1 и CCNA2.

Часть I, "Курс CCNA 1: основы сетевых технологий"

- **Глава 1, "Введение в компьютерные сети",** содержит описание основных принципов подключения к сети Internet. В ней читатель ознакомится с различными системами счисления и методами преобразования чисел из одной системы в другую.
- **Глава 2, "Основы сетевых технологий"**. В ней описана сетевая терминология и различные типы сетей, рассмотрено соотношение модели OSI и стандартов построения сетей, коротко рассказывается об основных функциях каждого из уровней модели OSI. В конце главы приведено описание различных сетевых устройств и топологии построения сетей.
- **Глава 3, "Сетевая среда передачи данных",** посвящена теоретическим вопросам электричества. Она необходима для понимания сетевых процессов, проходящих на физическом уровне модели OSI. В этой главе сравниваются различные среды передачи данных, использующиеся при построении сетей; подробно рассмотрены экранированная витая пара, неэкранированная витая пара, коаксиальный кабель, волоконно-оптический кабель и беспроводные сети.
- **Глава 4, "Тестирование кабелей".** В этой главе рассматриваются особенности процесса тестирования кабелей, используемых на физическом уровне методов проверки среды при построении локальных сетей (Local Area Networks — LANs). Сетевая среда передачи данных в этом случае рассматривается как магистраль компьютерной сети. Низкое качество сетевых кабелей приводит к отказам или ненадежной работе сети передачи данных. Оборудование, которое применяется для тестирования сетевой среды, использует определенные электротехнические и математические понятия, такие, как сигнал, волна, частота, шум. Понимание этих терминов необходимо для изучения методов построения сетей, принципов работы структурированной кабельной системы, процесса ее установки и тестирования сетей.
- **Глава 5, "Кабельные соединения сетей LAN и WAN",** посвящена вопросам каблирования сетей WAN и LAN. Несмотря на то что двух одинаковых сетей LAN не существует, многие аспекты дизайна сети являются общими. В этой главе описаны некоторые дополнительные элементы технологии Ethernet, локальных Ethernet-сетей и общих устройств. Для подключения к сети WAN на сегодняшний день используется множество разнообразных средств: от соединения

через обычную телефонную сеть посредством модема до широкополосного доступа. Разные методы подключения имеют разную стоимость, разную полосу пропускания и требуют разного оборудования. В главе приводится описание основных видов подключения и концепций.

- **Глава 6, "Основы технологии Ethernet"**. В этой главе обсуждаются принципы работы протокола Ethernet, процесс формирования фреймов протокола Ethernet (framing), обработка ошибок и различные типы коллизий в сетях Ethernet. Кроме того, рассматриваются такие понятия, как домен коллизий и широковещательный домен. В последней части главы обсуждаются понятие сегментации и устройства, использующиеся для создания сетевых сегментов.
- **Глава 7, "Технологии Ethernet",** посвящена методам коммутации и объединения сетей второго уровня модели OSI. В ней описаны основы протокола STP (Spanning-Tree Protocol — протокол распределенного связующего дерева), рассмотрен принцип его работы и перечислены состояния портов протокола коммутаторов. В данной главе также описаны наиболее распространенные разновидности технологии Ethernet, для того чтобы помочь усвоить наиболее общие понятия и подходы среды данного типа. В главе подробно описаны гигабитовая и 10-гигабитовая технология Ethernet, упомянуты более быстрые технологии, которые на сегодняшний день только разрабатываются.
- **Глава 8, "Ethernet-коммутация",** рассказывает о вопросах коммутации в сетях Ethernet. Мосты были разработаны для того, чтобы решить проблемы производительности, которые возникают с ростом величины сетевых сегментов и увеличением числа коллизий. Коммутаторы были разработаны на основе технологий мостов и стали ведущими устройствами современных локальных Ethernet-сетей. В этой главе рассматривается влияние коллизий и широковещания на производительность сети и сетевой трафик; описывается, как мосты, коммутаторы и маршрутизаторы используются для сегментации сетей и увеличения производительности сетевой инфраструктуры.
- **Глава 9, "Стек протоколов TCP/IP и IP-адресация",** представляет собой обзор стека протоколов TCP/IP, начиная с истории его разработки и заканчивая его будущими стандартами, которые на сегодняшний день только обсуждаются. В ней проводится сравнение модели TCP/IP с моделью OSI; сравнивается и описывается каждый из уровней модели стека протоколов TCP/IP с эталонной моделью.
- **Глава 10, "Основы маршрутизации и принципы построения подсетей",** охватывает темы, касающиеся протокола IP. В этой главе также рассматриваются различия между протоколами маршрутизации и маршрутизируемыми протоколами и рассказывается, как маршрутизаторы отслеживают путь между двумя участниками сетевого обмена. В последней части главы проведен обзор различных типов протоколов маршрутизации: дистанционно-векторных (distance-vector), протоколов с отслеживанием состояния канала (link-state) и гибридных протоколов, а также описано, как каждый из протоколов решает основные задачи маршрутизации.

- **Глава 11, "Уровень приложений и транспортный уровень стека протоколов TCP/IP",** посвящена темам, связанным с транспортным уровнем эталонной модели. В ней также описывается, как транспортный уровень применяет возможности сетевого уровня модели OSI, например, такие, как механизм выбора наилучшего маршрута следования данных и логическая адресация, которая используется для обеспечения непосредственного соединения между отправителем и получателем данных. В данной главе рассматриваются вопросы управления потоком информации от отправителя к получателю, надежность и аккуратность доставки.

Часть II, "Курс CCNA2: маршрутизаторы и основы маршрутизации"

- **Глава 12, "Распределенные сети и маршрутизаторы",** содержит описание основных устройств, технологий и стандартов распределенных сетей. В ней обсуждается роль маршрутизаторов в распределенных сетях.
- **Глава 13, "Основы работы с маршрутизаторами",** посвящена тому, как правильно произвести первую загрузку маршрутизатора, какие последовательности команд необходимо использовать для начальной настройки маршрутизатора. В этой главе также описана последовательность загрузки маршрутизатора и рассмотрен интерактивный диалог начальной настройки (setup dialog), который используется для создания базового конфигурационного файла для текущей версии операционной системы Cisco IOS.
- **Глава 14, "Настройка маршрутизаторов"**. В этой главе описываются режимы командной строки маршрутизатора и методы обновления его файла конфигурации; в ней делается упор на такие важные аспекты работы устройства, как процессы, происходящие во время загрузки маршрутизатора, и принцип работы операционной системы Cisco IOS. В данной главе приводится последовательность действий, необходимых для восстановления пароля доступа к маршрутизатору.
- **Глава 15, "Получение информации о соседних устройствах",** содержит описание протокола обнаружения устройств Cisco (Cisco Discovery Protocol — CDP), особенностей его работы настройки, его применения и использования в сетях.
- **Глава 16, "Управление программным обеспечением Cisco IOS",** посвящена исследованию этапов загрузки маршрутизатора, использования команд установки различных источников загрузки операционной системы Cisco IOS, резервирования и обновления файлов конфигурации и образов операционной системы. В ней также обсуждаются назначение конфигурационных регистров и методы определения версии образа операционной системы. В последней части главы приводятся примеры использования TFTP-сервера в качестве источника загрузки маршрутизатора.
- **Глава 17, "Маршрутизация и протоколы маршрутизации".** В этой главе описывается использование маршрутизаторов и их возможностей для выполнения основных функций межсетевого взаимодействия в соответствии с третьим

уровнем эталонной модели взаимодействия открытых систем (OSI) — сетевым уровнем. В ней также описано отличие протоколов маршрутизации от маршрутизируемых протоколов и рассмотрен процесс определения маршрутизаторами расстояния между различными точками сети. В данной главе рассматриваются дистанционно-векторные, гибридные и протоколы маршрутизации по состоянию каналов, а также указано, как именно разные классы протоколов решают основные задачи маршрутизации.

- **Глава 18, "Дистанционно-векторные протоколы маршрутизации",** посвящена рассмотрению этапов конфигурирования маршрутизатора и включения протоколов маршрутизации RIP и IGRP; в ней описаны команды для контроля активных протоколов маршрутизации.
- **Глава 19, "Сообщения об ошибках и управляющие сообщения протокола TCP/IP".** В ней описывается протокол ICMP, формат сообщений протокола ICMP, типы сообщений об ошибках и различные возможные ситуации, которые вызывают специфические сообщения об ошибках протокола ICMP. В главе также перечислены и описаны различные управляющие сообщения протокола ICMP, которые используются в современных сетях, и причины появления таких сообщений.
- **Глава 20, "Поиск и устранение неисправностей в маршрутизаторах",** содержит основную информацию о описке и устранении неисправностей в сетях. В этой главе подчеркивается необходимость использования структурированного подхода к тестированию и обнаружению неисправностей в сетях, приводятся основные этапы процесса поиска неисправностей, связанных с настройкой маршрутизатора.
- **Глава 21, "Стек протоколов TCP/IP"**. В этой главе подробно рассматриваются принцип работы протокола TCP/IP и гарантированная доставка данных через любой набор взаимосвязанных сетей, описываются отдельные компоненты стека протоколов TCP/IP: протоколы для передачи файлов, электронной почты, удаленного доступа к устройствам и других приложений. В ней также рассматриваются отличия между протоколами транспортного уровня с гарантированной и негарантированной доставкой и особенности передачи дейтаграмм пользователя без предварительной установки соединения на сетевом уровне. В последней части главы описан принцип работы протоколов ARP и RARP.
- **Глава 22, "Списки управления доступом",** содержит советы, анализ структуры, рекомендации по применению и общие правила использования списков управления доступом (ACL), включая команды конфигурации, необходимые для их создания. В конце главы приводятся примеры конфигурирования стандартного и расширенного списков управления доступом и показано, как их следует примененять на интерфейсах маршрутизатора.

Часть III, Приложения

- **Приложение А, "Структурированная кабельная система",** содержит обзор структурированных кабельных систем, их стандартов, кодов обозначения и нормативных актов; в нем также описаны методы обеспечения безопасности при укладке структурированной кабельной системы, описаны и проиллюстрированы базовый профессиональный инструментарий, процесс установки кабельной системы, финальные этапы кабельного проекта, приведен обзор коммерческих вопросов. В данном приложении содержится учебный пример создания проекта кабельной сети, который поможет разобраться в том, как осуществить кабельные проекты в реальной жизни. Материал приложения не представлен в интерактивном курсе CCNA, но дает некоторую важную информацию, необходимую для получения соответствующего сертификата.
- **Приложение Б, "Ответы на контрольные вопросы",** содержит ответы на контрольные вопросы, которые приводятся после каждой главы.
- **Приложение В, "Словарь терминов",** содержит полный список ключевых терминов книги.

Сопроводительные материалы

Компакт-диск, который поставляется вместе с книгой, предназначен для закрепления материала и приобретения дополнительного опыта. Он содержит главы, которых нет в других электронных материалах, системы тестирования с вопросами, которые охватывают курс CCNA, интерактивные лабораторные работы, фотографии сетевого оборудования и инструментария, видеоролики и анимацию, посвященные наиболее сложным для понимания вопросам. Материал предназначен для самостоятельного изучения и позволяет получить дополнительную квалификацию вне аудиторных занятий. На компакт-диске также записано программное обеспечение Packet Tracer версии 3.1, которое позволяет эмулировать работу оборудования, для того чтобы создавать, конфигурировать и настраивать "виртуальные" сети уровня сложности специалиста CCNA.

Данное учебное пособие не только акцентирует внимание на важных материалах, но и позволяет приобрести практический опыт в изучаемых темах. Компакт-диск поможет вам разобраться в маршрутизации и коммутации, объединить теорию с практикой.

Обращение к читателю

Третье дополненное и исправленное издание книги, которое вы держите в руках, было специально разработано как учебник и дополнительная литература к интерактивному курсу версии 3.1 Программы Сетевых Академий Cisco (Cisco Networking Academy Program). Оно было разработано экспертами корпорации Cisco Systems таким образом, чтобы максимизировать отдачу от очных курсов в Сетевых Академиях и позволить самостоятельно проработать некоторые наиболее сложные темы. Содержание книги практически полностью эквивалентно соответствующему курсу CCNA; иллюстрации в книге, презентации и видеоматериалы на прилагающемся компакт-диске очень близки к тем, которыми сопровождается одноименный интерактивный курс: они помогут читателю легко разобраться в наиболее запутанных концепциях и теоретических вопросах.

Эта книга позволит продолжить обучение, когда компьютер и интерактивный курс недоступны. Эксперты корпорации Cisco Systems, которые разрабатывали интерактивный курс, очень высоко оценили книгу и настоятельно рекомендуют использовать ее в качестве учебника, чтобы получить максимум знаний, будучи слушателем курса CCNA.

После окончания курса CCNA по Программе Сетевой Академии Cisco большинство студентов готовится к сдаче сертификационного экзамена на звание сетевого специалиста (Cisco Certified Network Associate). И в этом случае учебник, который вы держите в руках, окажет неоценимую помощь в процессе подготовки к экзамену. В будущем, когда соответствующий сертификационный экзамен уже будет пройден, эта книга может послужить неплохим справочником по техническим вопросам сетевых технологий.

Книга и дополнительные материалы на компакт-диске будут актуальны долгие годы.

От издательского дома “Вильямс”

Вы, читатель этой книги, и есть главный ее критик. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо либо просто посетить наш Web-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится ли вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название книги и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг. Наши координаты:

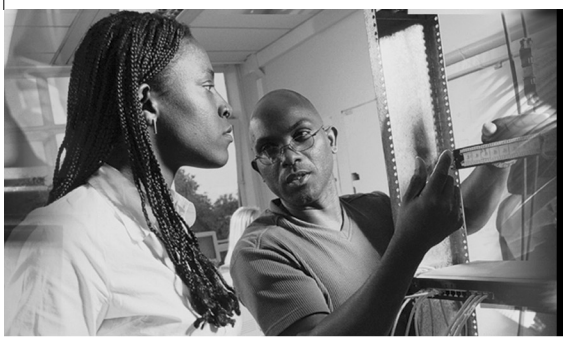
E-mail: info@williamspublishing.com

WWW: http://www.williamspublishing.com

Информация для писем из

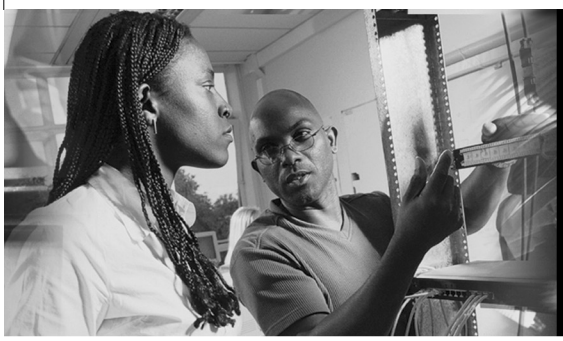
России: 115419, Москва, а/я 783

Украины: 03150, Киев, а/я 152



ЧАСТЬ I

КУРС CCNA 1: ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ



ГЛАВА 1

Введение в компьютерные сети

В этой главе...

- рассказывается о том, как определить необходимые требования для подключения к сети Internet;
- показано, как идентифицировать основные компоненты персонального компьютера;
- описано, как распознать Ethernet-адаптер, используемый для портативных компьютеров;
- приведено описание функций сетевых адаптеров (NIC);
- представлен список комплектующих, необходимых для установки сетевого адаптера;
- описаны функции команды **`ping`**;
- перечислены возможности Web-браузеров;
- приведено описание единиц измерения, используемых для обозначения размера передаваемых цифровых данных;
- описано, как перевести десятичные числа в двоичные;
- описано, как перевести двоичные числа в десятичные числа;
- описано, как перевести шестнадцатеричные числа в двоичные;
- описано, как перевести двоичные числа в шестнадцатеричные;
- рассмотрена булева, или бинарная, логика;
- описано понятие IP-адреса;
- приведено сравнение портативных переносных и стационарных настольных компьютеров;
- подробно описана шестнадцатеричная система.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце.

сеть Internet, с. 41,
физическое соединение, с. 42,
логическое соединение, с. 42,
программное обеспечение, с. 42,
Web-браузер, с. 42,
протокол передачи файлов, с. 42,

протокол, с. 42,
протокол управления передачей/протокол Internet, с. 42,
звуковая плата, с. 43,
параллельный порт, с. 43,
последовательный порт, с. 44,
порт мыши, с. 44,
порт клавиатуры, с. 44,
шнур питания, с. 44,
USB-порты, с. 44,
печатная плата, с. 45,
привод для компакт-дисков, с. 45,
центральный процессор, с. 45,
привод накопителей на гибких дисках, с. 45,
привод накопителей на жестких дисках, с. 45,
микропроцессор, с. 46,
материнская плата, с. 46,
шина, с. 46,
память, с. 46,
ПЗУ, с. 46,
гнездо расширения, с. 47,
системный блок, с. 47,
блок питания, с. 47,
PCMCIA, с. 47,
модем, с. 49,
ping, с. 52,
сетевой адаптер, с. 43,
видеоплата, с. 43,
язык гипертекстовой разметки, с. 53,
гиперссылки, с. 53,
американский стандартный код обмена информацией, с. 56,
бит, с. 57,
байт, с. 57,
килобит, с. 58,
килобайт, с. 58,
мегабит, с. 58,
мегабайт, с. 58,
гигабайт, с. 58,
терабайт, с. 58,
килобиты в секунду, с. 58,
килобайты в секунду, с. 58,
мегабиты в секунду, с. 58,
мегабайты в секунду, с. 58,
гигабиты в секунду, с. 58,
терабиты в секунду, с. 58,
двоичная система, с. 60,
точечно-десятичная запись, с. 66,
MAC-адрес, с. 66,
октет, с. 67,
булева логика, с. 69,
IP-адрес, с. 70,
маска подсети, с. 70.

В этой главе представлены основы компьютерной техники и описано, как подключиться к сети Internet. В ней также рассмотрены различные системы счисления и алгоритмы преобразования чисел из одной системы счисления в другую.

Обратите внимание на относящиеся к данной главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Подключение к сети Internet

Сеть Internet на сегодняшний день является ценным источником информации, средством коммуникации и общения и широко используется в коммерции, промышленности и образовании. Установка сети, которая будет подключена к сети Internet, требует тщательного предварительного планирования. Отдельный пользователь, который подключает свой персональный компьютер к такой сети, должен выполнить некоторое планирование и принять определенные решения. Даже простое подключение к обычной локальной сети, например, компьютера с установленной в нем сетевой картой или любого другого устройства, требует некоторых минимальных знаний и умений. Подключение же к распределенной сети может оказаться не менее сложной задачей. Необходимо выбрать правильный протокол и правильно его сконфигурировать, чтобы сеть или персональный компьютер могли быть подключены к сети Internet; также необходимо уметь установить и правильно настроить Web-браузер. Этот раздел посвящен именно тем темам, которые связаны с перечисленными выше умениями и знаниями.

Требования к подключению к сети Internet

Чтобы понять функции компьютеров в сетях, рассмотрим сеть *Internet*.

Сеть Internet может быть представлена в виде дерева с компьютерами в качестве листьев. Компьютеры — это отправители и получатели информации, передаваемой через сеть Internet. Компьютеры могут функционировать без сети Internet, но сеть Internet не может существовать без компьютеров. Она стремительно развивается, и пользователи становятся все более зависимыми от бесчисленных служб.

Компьютеры являются неотъемлемой частью сети, а также играют важную роль как орудия труда. Предприятия используют компьютеры в различных процессах: для хранения важных данных и учетных записей служащих, для обслуживания потребителей. Они применяют электронные таблицы для упорядочивания финансовой информации, текстовые редакторы — для ведения документации и корреспонденции, браузеры — для доступа ко внешним и внутренним Web-сайтам.

Высокоскоростные подключение к сети Internet — с использованием кабельных модемов и служб DSL (Digital Subscriber Line — цифровая абонентская линия) — теперь доступно и для домашнего использования или использования в небольших офисах, что повышает требования к предоставляемым услугам. На сегодняшний день недостаточно просто подключить к сети Internet один компьютер; пользователям

необходимы инструментальные средства, которые позволят совместно использовать подключение к глобальной сети.

Internet — это самая большая сеть передачи данных в мире. Она состоит из множества малых и больших сетей, которые некоторым образом соединены друг с другом. В конечных точках такой большой сети находятся индивидуальные компьютеры пользователей.

Соединение с сетью Internet может быть разделено на такие компоненты:

- *физическое подключение* — это физическое соединение с сетью, которое осуществляется посредством подсоединения к компьютеру кабеля и установки в него специализированных карт расширения, таких, как модем или сетевой адаптер. Физическое соединение используется для передачи сигналов между персональным компьютером в локальной сети и удаленными устройствами в сети Internet;
- *логическое подключение* представляет собой логическое соединение и использует стандарты, называемые протоколами. *Протоколом* называют формальное описание набора правил и соглашений, которые определяют, как именно устройства в сети обмениваются данными. Для подключения к сети Internet может использоваться множество протоколов. Набор протоколов *TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол Internet*) является основным протоколом сети Internet. Стек TCP/IP — это набор протоколов, которые взаимодействуют между собой и обеспечивают отправку и получение данных. Подробнее протокол TCP/IP рассматривается в главе 9, “Стек протоколов TCP/IP и IP-адресация”;
- *прикладные программы* — это программное обеспечение, которое интерпретирует данные и отображает информацию в понятном пользователю формате; является последним звеном в установке соединения. Прикладные программы работают с протоколами для передачи и получения данных через сеть Internet: *Web-браузеры* отображают язык гипертекстовой разметки (HyperText Markup Language — HTML) как Web-страничку, *протокол передачи файлов (File Transfer Protocol — FTP*) используется для загрузки файлов и программ из сети Internet. Web-браузеры также используют соответствующие подключаемые модули для отображения специфических типов данных, таких, как видео, звук и анимация.

Из сказанного выше может показаться, что работа со средой Internet проста, однако, как показано далее в этой главе, а впоследствии намного более подробно описано, пересылка данных через сеть Internet является довольно нетривиальной задачей.

Структура персональных компьютеров

Компьютеры являются важной частью сети, поэтому необходимо знать и свободно идентифицировать основные компоненты персональных компьютеров. Можно представить себе внутренние компоненты персонального компьютера как сетевые

устройства, подключенные к системной шине. В такой аналогии каждый компьютер можно рассматривать как небольшую компьютерную сеть.

Множество сетевых устройств, таких, как маршрутизаторы и коммутаторы, — это специализированные компьютерные системы, которые состоят из тех же основных частей, что и обычный персональный компьютер. Чтобы компьютер был надежным средством получения информации, он должен находиться в рабочем состоянии. Необходимо уметь распознавать и проводить диагностику компонентов компьютера (это также относится и к портативным компьютерам), описанных в этом разделе.

ВНИМАНИЕ!

В этой главе компоненты и принципы работы персонального компьютера описаны вкратце. Если основы компьютерных технологий вам не знакомы, обратитесь за подробной информацией к курсу *IT Essentials* или одноименной книге.

Компоненты материнской и объединительной плат

Материнская плата — основная печатная плата компьютера. Это очень важный элемент компьютера, т.к. плата является "нервным центром" персонального компьютера. Все остальные элементы системы вставляются в ее гнезда и контролируются материнской платой, которая в некоторых системах называется объединительной; она ответственна за коммуникацию между устройствами в системе.

ВНИМАНИЕ!

В некоторых компьютерах сетевой адаптер, звуковая плата, видеоплата и другие модули могут быть интегрированы в материнскую плату.

Под *объединительной платой (backplane)* подразумевается большая печатная плата, которая содержит разъемы для плат расширения. Ниже перечислены основные компоненты объединительной платы.

- *Сетевой адаптер (Network Interface Card — NIC)* — это печатная плата, которая предоставляет возможность обмена данными с сетью. Большинство современных настольных и портативных компьютеров имеют встроенный адаптер сети Ethernet.
- *Видеоплата* — это плата расширения для отображения графической информации. Видеоплаты обычно содержат встроенный микропроцессор и дополнительную память для ускорения и улучшения качества графической информации.
- *Звуковая плата* — это плата расширения, которая обеспечивает вывод звуковой информации.
- *Параллельный порт* — это интерфейс, через который может передаваться более одного бита одновременно. Он используется для подключения различных внешних устройств, например, принтера.

- *Последовательный порт* — это интерфейс, используемый для последовательной передачи данных, в котором за единицу времени передается только один бит. К последовательному порту могут подключаться внешние модемы, плоттеры и последовательные принтеры. Он также может быть использован для подключения консоли сетевых устройств, например, маршрутизаторов и коммутаторов.
- *Порт мыши* используется для подключения устройства типа "мышь" к компьютеру.
- *Порт клавиатуры* используется для подключения клавиатуры к компьютеру.
- *Шнур питания* подключает устройство к электрической розетке для подачи напряжения.
- *Порт универсальной последовательной шины (Universal Serial Bus port — USB port)* — интерфейс для подсоединения внешних устройств, таких, как "мышь", модемы, клавиатуры, сканеры и принтеры, которые могут подключаться и отключаться без перезагрузки системы. В будущем USB-порты, возможно, заменят последовательные и параллельные порты.

Практическое задание 1.1.2. Изучение аппаратного обеспечения персонального компьютера.

Это практическое задание поможет изучить основные компоненты персональных компьютеров и их соединения, в том числе и подключение к сети. Рассмотрите внутреннюю конфигурацию персонального компьютера и определите основные компоненты. В процессе загрузки и в панели управления операционной системы Windows обратите внимание на найденные аппаратные устройства.

Электронные компоненты компьютера

Особенностью электронных компонентов является то, что они разработаны для управления и передачи данных и сигналов в электронном виде. Большинство таких компонентов расположены на материнской плате компьютера и платах расширения, которые вставляются в материнскую плату. Рассмотрим некоторые наиболее распространенные компоненты подробнее.

- **Транзистор** — это устройство, которое усиливает сигнал или размыкает и замыкает электрическую цепь. Микропроцессоры могут содержать миллионы транзисторов.
- **Интегральная схема** — это устройство, изготовленное из полупроводниковых материалов. Стандартная интегральная схема содержит множество транзисторов и выполняет определенные задачи.
- **Резистор** — это устройство, изготовленное из материала, который создает сопротивление электрическому току.
- **Конденсатор** — электрический компонент, который сохраняет энергию в виде электростатического поля. Он состоит из двух проводящих металлических пластин, разделенных диэлектрическим материалом.

- **Разъем** — это порт или интерфейс, в который вставляется кабель, например: последовательный (COM), параллельный (LPT), USB (Universal Serial Bus — универсальная последовательная шина) и дисковый интерфейс.
- **Светодиод (Light Emitting Diode — LED)** — это полупроводниковое устройство, которое излучает свет, когда через него протекает электрический ток. Обычно используется для световой индикации.

Дополнительная информация: компоненты персонального компьютера

Компонентами персонального компьютера обычно являются встроенные или внешние модули, которые обеспечивают разнообразные дополнительные функции компьютера. К ним относятся приводы сменных носителей информации, память, жесткие диски, процессоры и источники питания.

Рассмотрим наиболее общие компоненты компьютерных устройств.

- *Печатная плата (Printed circuit board — PCB)* — тонкая плата, на которой расположены микросхемы и другие электрические компоненты. В качестве примера такого компонента могут служить материнская плата и различные платы расширения.
- *Привод для компакт-дисков (CD-ROM)* — оптический привод, который считывает информацию с компакт-дисков. Существуют еще устройства для записи компакт-дисков (CD-R, CD-RW) или DVD-дисков, а также их различные комбинации.
- *Центральный процессор (Central Processing Unit — CPU)* — "мозг" компьютера, в котором выполняется большинство вычислительных операций (рис. 1.1).
- *Привод накопителей на гибких дисках (Floppy Disk Drive — FDD)* — устройство, которое позволяет считывать и записывать информацию на гибкие диски (рис. 1.2).
- *Привод накопителей на жестких дисках (Hard Disk Drive — HDD)* считывает и записывает данные на жесткий диск и является основным устройством для хранения данных в компьютере.

Рис. 1.1. Центральный процессор

Рис. 1.2. Привод накопителей на гибких дисках

- *Микропроцессор* — кремниевый кристалл, содержащий интегральные схемы. Обычно компьютер содержит множество микропроцессоров, включая главный процессор.
- *Материнская плата* — основная печатная плата компьютера (рис. 1.3). Такая плата — один из самых важных компонентов, т.к. она является "нервным центром" компьютера. Все остальные элементы системы вставляются в ее разъемы и контролируются материнской платой; кроме того, эта плата ответственна за процессы коммуникации между устройствами в системе.
- *Шина* — набор электрических цепей, через которые передаются данные от одной части компьютера к другой. Шина соединяет все внутренние компоненты компьютера и центральный процессор. Структура, соответствующая промышленному стандарту (Industry-Standard Architecture — ISA), и шина соединения периферийных устройств (Peripheral Component Interconnect — PCI) — это два разных типа шины.
- *Память с произвольным доступом (Random-Access Memory — RAM)*, также называемая оперативной памятью, позволяет записывать новые данные и считывать сохраненные. Память RAM — это основная рабочая зона, используемая центральным процессором для большинства вычислений и операций. Недостатком оперативной памяти является то, что требуется электрическая энергия для сохранения информации. При выключении или сбое питания компьютера все данные, сохраненные в оперативной памяти, теряются, за исключением тех, которые предварительно были записаны на диск. Модули с микросхемами оперативной памяти вставляются в материнскую плату.
- *Постоянным запоминающим устройством (Read-Only Memory — ROM, ПЗУ)* называют тип компьютерной памяти, в которой данные предварительно записаны. После записи данных на микросхему ПЗУ данные не могут быть удалены и доступны только для чтения. В тип ПЗУ, которая известна как электронно перезаписываемая ПЗУ, — ЭППЗУ (Electronically Erasable Programmable Read-Only Memory — EEPROM) могут быть программно записаны данные. Такую память называют Flash-памятью. Базовая система ввода-вывода (Basic Input/Output System — BIOS) в большинстве компьютеров хранится в памяти ЭППЗУ.

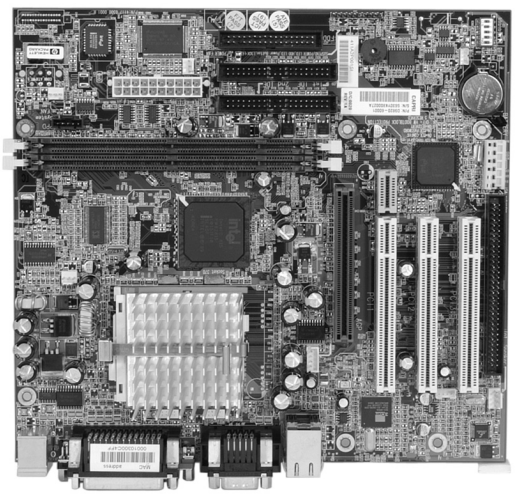


Рис 1.3. Материнская плата

- *Гнездо расширения* — разъем в компьютере, обычно на материнской плате, в который вставляются карты расширения для добавления новых возможностей компьютера (рис. 1.4).
- *Системный блок* — это основная часть персонального компьютера. Под системным блоком обычно подразумевается корпус, материнская плата, источник питания, микропроцессоры, основная (оперативная) память, шина, карты расширения, приводы накопителей (гибких дисков, компакт-дисков, жестких дисков и т.д.) и порты ввода-вывода. Системный блок не включает в себя клавиатуру, монитор и другие периферийные и внешние устройства, подключенные к компьютеру.
- *Блок питания* обеспечивает электрическое питание компьютера.

Сравнение настольных и портативных компьютеров

Портативные и карманные персональные компьютеры (КПК) становятся все более популярными. Основное отличие между настольными персональными компьютерами и портативными, если не считать, что компоненты портативных компьютеров имеют меньший размер, чем аналогичные компоненты персональных, состоит в том, что портативные компьютеры предоставляют большую свободу передвижений, чем персональные. В портативных компьютерах часто используют специальные платы и гнезда расширения, соответствующие стандарту *Международной Ассоциации производителей плат памяти для персональных компьютеров (Personal Computer Memory Card International Association card — PCMCIA card)*, или просто *PC card*. Существуют сетевые адаптеры, модемы, жесткие диски и другое периферийное оборудование (обычно размером с толстую кредитную карточку), подключаемое к разъемам PCMCIA. На рис. 1.5 показан адаптер беспроводной сети (WLAN — Wireless LAN) с PCMCIA-интерфейсом.

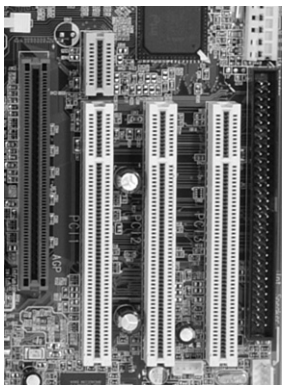


Рис. 1.4. Гнездо расширения

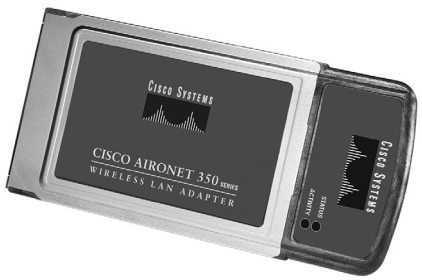


Рис. 1.5. PCMCIA-адаптер беспроводной сети

Сетевые адаптеры

На рис. 1.6 показан адаптер сети Ethernet, зачастую также называемый адаптером локальной сети (LAN adapter). Он выполнен в виде печатной платы, которая вставляется в разъем материнской и используется для подключения персонального компьютера к сети передачи данных.

Рис. 1.6. Сетевой адаптер

ВНИМАНИЕ!

Если основы компьютерных технологий вам не знакомы, обратитесь к курсу *IT Essentials* или одноименной книге за подробной информацией. В этих источниках подробно описаны такие понятия, как запрос на прерывание (Interrupt ReQuest — IRQ), адреса ввода-вывода (I/O), процессоры, функции и настройки операционных систем.

Сетевой адаптер взаимодействует с сетью через кабель (или радиоволны в беспроводных технологиях связи), а с компьютером — через гнездо расширения. При установке сетевого адаптера в компьютер ему необходимо указать номер **запроса на прерывание** (IRQ) для обработки данных центральным процессором, диапазон адресов ввода-вывода и буфер в оперативной памяти для передачи данных операционной системе (например, Windows или Linux), установить драйверы, которые необходимы для взаимодействия устройства с системой. Сигнал запроса на прерывание сообщает центральному процессору, что произошло событие, требующее немедленной обработки. Этот сигнал посылается центральному процессору через аппаратную линию к микропроцессору. Примером прерывания может служить нажатие клавиши на клавиатуре. Центральный процессор должен перенести данные, полученные от клавиатуры, в оперативную память. Адреса ввода-вывода (I/O) служат для поиска в памяти персонального компьютера области, используемой для получения и отправления данных от компьютера вспомогательному устройству.

При выборе сетевого адаптера для сети необходимо учесть следующие факторы:

- **тип сети.** Различные типы сетей требуют различных сетевых адаптеров, например, Ethernet-адаптеры разработаны для использования в локальных сетях Ethernet. Кроме Ethernet, существуют также сети Token Ring и Fiber Distributed Data Interface (FDDI — распределенный интерфейс передачи данных по волоконно-оптическим каналам), однако Ethernet — это наиболее распространенная разновидность локальных сетей;

- **тип среды передачи данных —** тип порта или сетевого разъема, используемого для подключения к разным средам передачи данных, например: витая пара, коаксиальный кабель, волоконно-оптический кабель или беспроводная сеть. Коаксиальный кабель все меньше и меньше используется в современных сетях;
- **тип системной шины.** Существуют различные типы системной шины, например, PCI и ISA. Т.к. PCI-шина позволяет передавать данные быстрее, чем шина ISA, то последняя постепенно отходит на второй план.

Мультимедийная презентация: сетевая карта.
В данной презентации показана типичная сетевая карта.

Установка сетевой платы или модема

Подключение к сети Internet требует наличия специального адаптера: модема или сетевой карты.

Модем — это электронное устройство, используемое компьютером для обмена данными через телефонные линии. Он позволяет передавать данные от одного компьютера другому через открытую коммутируемую телефонную сеть (Public Switched Telephone Network — PSTN). На рис. 1.7 показан внешний модем. Обычно модемы посылают данные блоками. После каждого блока следуют контрольные данные, математически рассчитываемые из последовательности байтов блока, и устройство получателя сравнивает расчетные контрольные данные с полученными. При несоответствии расчетных и полученных данных весь блок посылается заново. Модем-отправитель преобразовывает цифровые данные в аналоговый сигнал для передачи через коммутируемую телефонную сеть общего пользования, затем модем-получатель преобразовывает аналоговый сигнал в цифровой.

Рис. 1.7. Внешний модем

Термин *модем* произошел от названия функций, которые выполняет это устройство. Процесс преобразования цифровых данных в аналоговый сигнал и наоборот называется *модуляцией/демодуляцией*. Модемы могут быть установлены внутри компьютера или подключены через внешние интерфейсы: последовательные порты или

порт USB. Для подключения компьютера к сети модемы набирают телефонный номер другого компьютерного модема, который обычно находится у провайдера услуг Internet (Internet Service Provider — ISP). Модемы поддерживают сравнительно невысокую скорость передачи данных, теоретический предел составляет 56 Кбит/с, на практике максимальная скорость не превышает 53 Кбит/с. Кабельные и DSL-модемы позволяют получить более высокую скорость передачи, чем описываемые в данной главе устройства, однако требования к телефонным линиям и оборудованию АТС также достаточно высоки.

Сетевая плата используется для непосредственного подключения к сети и является одним из основных коммуникационных компонентов компьютера. Могут быть использованы различные типы сетевых адаптеров в зависимости от конфигурации компьютера. Портативные компьютеры могут иметь встроенный сетевой интерфейс или подключаться к сети с помощью PCMCIA-адаптера. Персональные компьютеры также могут иметь встроенный интерфейс или карту расширения для подключения к сети.

Ситуации, когда системному или сетевому администратору необходимо установить сетевой адаптер, перечислены ниже.

- Сетевой адаптер в персональном компьютере отсутствует.
- Установленная сетевая плата повреждена или работает с перебоями.
- Необходимо заменить сетевой адаптер с пропускной способностью 10 Мбит/с на сетевой адаптер с пропускной способностью 100 Мбит/с.

Для установки сетевого адаптера (см. рис. 1.8) необходимо обладать перечисленной ниже информацией.

- Необходимо знать особенности конфигурации адаптера, включая положение переключателей и установку программного обеспечения. Большинство современных сетевых адаптеров не имеет переключателей и поддерживает технологию автоматического распознавания и конфигурирования (plug-and-play), поэтому они практически или совсем не требуют какой-либо конфигурации. При необходимости сетевые платы могут быть настроены с помощью программного обеспечения, поставляемого вместе с сетевым адаптером.
- Необходимо проверить работоспособность сетевой карты с помощью поставляемых производителем средств диагностики и провести петлевой тест (за дополнительной информацией обратитесь к документации сетевого адаптера).
- Необходимо уметь разрешать аппаратные конфликты, связанные с прерываниями IRQ, адресами ввода-вывода, адресами прямого доступа к памяти (Direct Memory Address — DMA), который используется для непосредственной передачи данных из оперативной памяти устройству без участия центрального процессора.

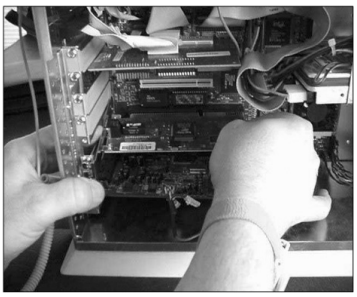


Рис 1.8. Установка сетевого адаптера

Обзор высокоскоростных и коммутируемых соединений

В начале 1960-х годов были разработаны модемы для подключения простых терминалов ввода-вывода к центральному компьютеру. Поскольку иметь собственный компьютер в то время было слишком дорого, многие компании арендовали компьютерное время. Скорость соединения была очень низкой — 300 битов в секунду (бит/с), т.е. такая линия позволяла передавать примерно 30 символов в секунду.

Персональные компьютеры стали появляться в 1970-х годах, как раз тогда появились первые электронные доски объявлений (Bulletin Board Systems — BBS), которые позволяли пользователям посылать и читать сообщения на досках объявлений. Скорость 300 бит/с была достаточной для коммуникации, потому что она превышала скорость чтения или набора текста большинства людей. Электронные доски объявлений не были широко распространены до начала 1980-х годов, когда появилась необходимость передавать файлы и графическую информацию. Скорости в 300 бит/с уже было явно недостаточно, что подтолкнуло промышленность к разработке модемов большей пропускной способности. К 1990 г. скорость модемов достигла 9600 бит/с и поднялась до текущего стандарта — 56000 бит/с, к 1998 г.

Неизбежным было появление высокоскоростных служб передачи данных, как для корпоративных пользователей, так и для домашних, таких, как цифровые абонентские линии (Digital Subscriber Line — DSL) и доступ к сети по кабельному модему. Эти технологии не требуют дорогого оборудования или дополнительной телефонной линии. Кроме того, такие соединения являются службами *постоянного подключения*, которые предоставляют пользователю непрерывный доступ и не требуют установки соединения для каждого сеанса обмена данными, что повышает их надежность и гибкость. В результате разработки и повсеместного внедрения указанных выше технологий значительно упростилось совместное использование подключения к сети Internet для небольших офисов и домашних сетей.

Конфигурирование протоколов TCP/IP

TCP/IP — это набор протоколов или правил, которые обеспечивают взаимодействие компьютеров и совместное использование ресурсов с помощью сети. Чтобы получить доступ к сети Internet, в компьютере должно быть запущено программное

обеспечение, обрабатывающее запросы стека протоколов TCP/IP. Запустить набор протоколов TCP/IP на рабочей станции можно с помощью программных средств операционной системы. Для персонального компьютера необходимо настроить IP-адрес, маску сети, адрес стандартного шлюза и адрес сервера доменных имен (Domain Name Server — DNS). Все перечисленные параметры можно выставить вручную или получить с помощью протокола динамической конфигурации узла (Dynamic Host Configuration Protocol — DHCP). Обычно информация, необходимая для настройки стека протоколов TCP/IP, предоставляется сетевым администратором или провайдером услуг Internet. Процедура настройки набора протоколов одинакова вне зависимости от типа используемой операционной системы: Windows, Apple Macintosh, Unix. Принцип работы протоколов TCP/IP, DHCP и DNS описан в следующих главах.

Практическое задание 1.1.6. Сетевые настройки набора протоколов TCP/IP для персонального компьютера.
Это практическое задание позволит ознакомиться с методами определения типа сетевого соединения компьютера, имени компьютера, MAC-адреса (адреса второго уровня) и сетевого адреса (адреса третьего уровня).

Проверка соединения при помощи команды ping

Ping — это программа, используемая для проверки настроек набора протоколов TCP/IP. Она получила свое название по аналогии с гидролокатором (сонаром), который используется для обнаружения подводных объектов и измерения расстояния до них. Название *Ping* расшифровывается как Packet Internet Groper — отправитель пакетов сети Internet.

Принцип работы команды **`ping`** основан на отправлении нескольких IP-пакетов определенному получателю, на каждый из которых получатель должен ответить специализированным ответом. Выводимая командой **`ping`** информация содержит соотношение количества успешно полученных ответов к отправленным и среднее время прохождения пакетов к получателю. По этой информации можно определить, возможно ли установить соединение с получателем. Команда **`ping`** используется для тестирования функций приема и передачи сетевого адаптера, проверки конфигурации стека протоколов TCP/IP, проверки возможности соединения с удаленным устройством. Ниже приведены несколько примеров использования команды **`ping`**.

- **`ping 127.0.0.1`** (проверка внутренней обратной петли) — проверяет работоспособность стека протоколов TCP/IP и функции приема и передачи сетевого адаптера (рис. 1.9).
- **`ping`** *`локальный IP-адрес компьютера`* — проверяет конфигурацию адреса набора протоколов TCP/IP для локального устройства.
- **`ping`** *`IP-адрес стандартного шлюза`* — проверяет подключение маршрутизатора к локальной сети и возможность доступа к другим сетям.

- **ping** *IP-адрес удаленного устройства* — проверяет возможность соединения с удаленным устройством.

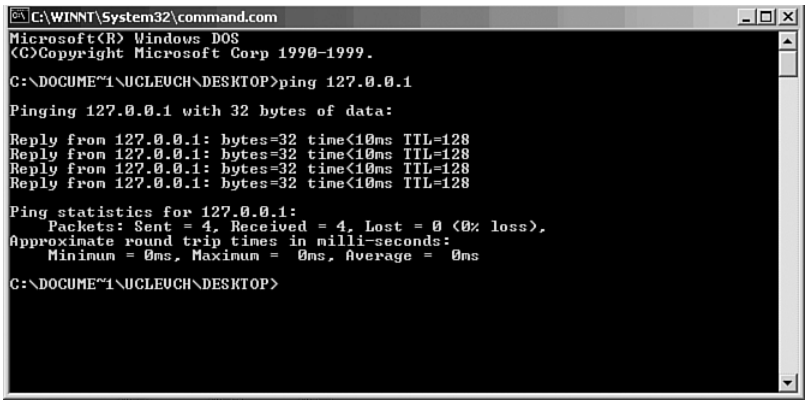


Рис. 1.9. Результат выполнения команды `ping 127.0.0.1`

Практическое задание 1.1.7. Использование команд `ping` и `tracert`.
В этом практическом задании необходимо с помощью команд **`ping`** и **`traceroute`** проверить подключение к сети. В процессе выполнения работы обратите внимание на процесс преобразования имен в IP-адреса.

Web-браузеры и подключаемые приложения

Web-браузеры — это приложения, выполняемые на стороне пользователя, которые осуществляют следующие функции:

- устанавливают соединение с Web-сервером;
- запрашивают информацию;
- получают информацию;
- отображают информацию на экране компьютера.

Браузеры интерпретируют *язык гипертекстовой разметки* (HyperText Markup Language — HTML), один из языков, используемых для описания и программирования содержимого Web-страниц. Другие языки разметки, такие, как стандартный обобщенный язык разметки[1] (Standard Generalized Markup Language — SGML) и расширяемый язык разметки (Extensible Markup Language — XML), предоставляют более широкие возможности для создания динамических и интерактивных Web-страниц по сравнению с языком HTML. HTML является самым распространенным языком разметки, он позволяет отображать графику и проигрывать звуковые, видео- и другие мультимедийные файлы. *Гиперссылки* — управляющие команды, которые

[1] *Стандарт описания офисных документов, утвержденный организацией ISO. — Прим. ред.*

позволяют осуществить переход на другие HTML-файлы на Web-сервере или определенные точки в том же документе и предоставляют ускоренную навигацию по документам.

Internet Explorer (IE) и Netscape — два наиболее популярных Web-браузера. Несмотря на то что они выполняют одни и те же функции, между ними существуют различия. Некоторые Web-сайты могут не поддерживать тот или иной браузер, поэтому рекомендуется устанавливать на компьютере обе программы.

В табл. 1.1 приведены сравнительные характеристики обоих браузеров.

Таблица 1.1. Сравнение браузера Internet Explorer компании Microsoft и Netscape Communicator

Internet Explorer	Netscape Communicator
Интегрирован с другими продуктами Microsoft	Первый популярный браузер
Занимает больше дискового пространства	Занимает меньше дискового пространства
Отображает HTML-файлы, обслуживает передачу почтовых сообщений, файлов и выполняет другие функции	Отображает HTML-файлы, обслуживает передачу почтовых сообщений, файлов и выполняет другие функции

Стандартные Web-браузеры не могут отображать многие специализированные и запатентованные типы файлов. Для просмотра таких файлов браузер необходимо настроить для использования *подключаемых приложений (plug-in)*. Браузер взаимодействует с такими приложениями и с их помощью отображает специальные файлы. Ниже перечислены наиболее распространенные патентованные подключаемые приложения.

- **Flash- и Shockwave-проигрыватель (Flash player, Shockwave player)** — это приложения, которые проигрывают мультимедийные файлы, созданные с помощью программного обеспечения Macromedia Flash.
- **Adobe Acrobat Reader** — программный продукт или модуль, который позволяет пользователю просматривать и распечатывать файлы в формате PDF (Adobe Portable Document Format — формат машинонезависимых документов компании Adobe).
- **Проигрыватель Windows Media** — это приложение, которое позволяет пользователю проигрывать аудио- и видеофайлы.
- **Модуль Quicktime** — приложение, разработанное компанией Apple, которое позволяет пользователю проигрывать видео- и аудиофайлы в соответствующем формате.
- **Real Player** — это приложение, с помощью которого пользователь может прослушивать аудиофайлы.

Практическое задание 1.1.8. Изучение Web-браузеров.
Это практическое задание поможет освоить основы использования браузеров для доступа к Internet-сайтам и научиться пользоваться поисковыми системами для поиска информации в сети Internet, позволит узнать концепцию построения унифицированного указателя информационного ресурса (Uniform Resource Locator — URL). На указанных в работе Web-сайтах будут даны определения сетевых терминов, и посредством гиперссылок можно будет переходить с текущего Web-сайта на другие.

Дополнительная информация: другие компьютерные приложения

Компьютер может выполнять множество разнообразных полезных функций. В процессе работы пользователи регулярно используют набор приложений, которые поставляются в виде *офисного пакета программ*, например, программное обеспечение Microsoft Office и Lotus Smart Suite. Офисные пакеты обычно включают в себя следующие приложения:

- **приложение для работы с электронными таблицами**, позволяющее построить из исходных данных таблицу. Такое приложение используется для математической обработки и анализа данных;
- **текстовый процессор** — это приложение, которое используется для создания и редактирования текстовых документов. Современные текстовые процессоры позволяют пользователю создавать сложные документы, содержащие графику и разнообразные стили форматирования текста;
- **программные средства баз данных** — это приложения, позволяющие пользователю хранить, поддерживать, организовывать, сортировать и фильтровать записи в базе данных. *Запись базы данных* — это некоторый набор информации, который можно идентифицировать по определенному признаку, например, по имени заказчика;
- **программное обеспечение для проведения презентаций** — это приложение, которое позволяет пользователю разработать и создать презентацию для представления на встречах, обсуждениях или демонстрациях товара;
- **программное обеспечение для управления личной информацией** — приложение, которое позволяет отправлять электронную почту, хранить список контактов, составлять календарь и распорядок дня.

Поиск и устранение неисправностей подключения к сети Internet

Рекомендуется придерживаться следующей последовательности действий при поиске и устранении неисправностей в соединении компьютера с сетью.

Этап 1. Определите проблему.

Этап 2. Соберите требуемую информацию.

Этап 3. Рассмотрите возможные пути решения проблемы.

Этап 4. Создайте план действий.

Этап 5. Выполните нужные действия в соответствии с планом.

Этап 6. Рассмотрите результаты выполненных действий.

Этап 7. Запишите полученные результаты.

Этап 8. Попробуйте создать подобные решенным проблемы и устраните их.

Практическое задание 1.1.9. Поиск и устранение неисправностей компьютера и его подключения к сети.
В этом практическом задании используется базовая модель поиска простых и наиболее распространенных неисправностей в сети, к которым относятся проблемы, вызванные программным и аппаратным обеспечением.

Двоичные числа

В текущем разделе рассматривается способ представления данных внутри компьютера и вид, в котором данные передаются по сети. Читатель также ознакомится с различными системами счисления и логикой, используемой в компьютерах.

Двоичное представление данных

Компьютер — это электромеханическое устройство, состоящее из электрических переключателей, управляемых электрическим током. В зависимости от положения этих переключателей, компьютер производит вычисления и выполняет различные необходимые действия. Поскольку компьютер реагирует на импульсы электрического тока, то цепи компьютера могут обрабатывать два состояния: *наличие* или *отсутствие* тока (соответственно 1 и 0).

Компьютер для работы с данными и их хранения использует электронные переключатели — *триггеры*, которые также могут находиться в двух состояниях: замкнутом и разомкнутом. Компьютеры воспринимают и обрабатывают данные в формате с двумя состояниями (бинарном формате). Единица представляется замкнутым состоянием переключателя или наличием электрического тока, 0 — соответственно разомкнутым переключателем или отсутствием тока. Единица и нуль описывают два возможных состояния электронных компонентов в компьютере и называются двоичными цифрами, или *битами*.

Американский стандартный код обмена информацией (American standard code for information interchange — ASCII) является наиболее распространенным кодом для представления буквенно-цифровых данных в компьютере. В нем используются двоичные числа для представления символов, которые пользователь печатает на клавиатуре. Когда компьютер пересылает информацию через сеть, то электрические, оптические или радиосигналы передают соответствующие значения: 1 или 0. Каждому символу соответствует уникальная восьмибитовая комбинация для представления данных.

Биты, байты и единицы измерения

Биты — это двоичные цифры, каждая из которых имеет значение 0 или 1. В компьютере им соответствуют положения переключателей (включен/выключен) или наличие/отсутствие электрического сигнала, светового импульса или радиоволны.

- Двоичный нуль может быть представлен электрическим напряжением 0 В (Вольт).
- Двоичная единица может быть представлена электрическим напряжением +5 В.

Компьютеры используют группы двоичных цифр, которые состоят из 8 битов. Такая группа из 8 битов называется байтом. В компьютере 1 байт является минимальной адресуемой ячейкой запоминающего устройства. Ячейка запоминающего устройства содержит значение или один символ данных, например, ASCII код.

Общее число комбинаций из восьми переключателей равно 256 (или 2^8). Поэтому значения байта лежат в диапазоне от 0 до 255. Следовательно, байт — это один из самых важных для понимания принципов работы компьютеров и сетей (табл. 1.2).

Зачастую в англоязычной литературе возникает путаница с обозначением величин — KB и Kb, MB и Mb (Кбайт и Кбит, Мбайт и Мбит). Запомните, что для правильных вычислений с использованием скорости передачи данных необходимо различать килобиты и килобайты. Например, программное обеспечение модемов обычно показывает скорость соединения в кило*битах* в секунду (например, 45 Кбит/с, или 45 Kbps). В то же время популярные браузеры показывают скорость загрузки файла в кило*байтах* в секунду. Разная запись означает, что при скорости соединения 45 Кбит/с максимальная скорость загрузки файла будет равна приблизительно 5,6 Кбайт/с. На практике скорость загрузки файла будет меньше за счет разных факторов и служб, которые используют полезную пропускную способность канала. Необходимо также помнить, что размер файлов обычно выражается в байтах, в то время как пропускная способность локальной сети и соединений распределенных сетей — в килобитах в секунду (Кбит/с) или мегабитах в секунду (Мбит/с). Необходимо умножить количество байтов в файле на 8, чтобы правильно определить время загрузки файла.

Таблица 1.2. Единицы информации

Единица измерения	Байты	Биты
Бит (b, или бит)	1/8	1
Байт (B, или байт)	1	8
Килобайт (KB, или Кбайт)	1024 (приблизительно 1000 байтов)	8096 (приблизительно 8000 битов)
Мегабайт (MB, или Мбайт)	приблизительно 1 миллион	приблизительно 8 миллионов
Гигабайт (GB, или Гбайт)	приблизительно 1 миллиард	приблизительно 8 миллиардов
Терабайт (TB, или Тбайт)	приблизительно 1 триллион	приблизительно 8 триллионов

Рассмотрим часто используемые компьютерные единицы измерения.

- *Битом* называется наименьший блок данных в компьютере. Бит принимает значение 1 или 0 и является цифрой двоичного формата данных, который используется компьютером для хранения, передачи и обработки данных.
- *Байтом* называется единица измерения, которая используется для описания размеров файлов данных на жестком диске компьютера или другом носителе информации; для описания количества данных, переданных через сеть. 1 байт равен 8 битам.

- *Килобит (Кбит)* — это 1024 бита, при оценочных вычислениях используется значение в 1000 битов.
- *Килобайт (КБайт)* равен 1024 байтам, при оценочных вычислениях используется значение в 1000 байтов.
- *Мегабит (Мбит)* равен приблизительно 1 миллиону битов.
- *Мегабайт (МБайт)* равен 1 048 576 байтов, при оценочных вычислениях используется значение в 1 миллион байтов. Мегабайт иногда сокращенно называют "мег". Объем оперативной памяти в большинстве компьютеров обычно измеряется в мегабайтах. Большие файлы имеют размер порядка нескольких мегабайт.
- *Гигабайт (Гбайт)* равен приблизительно 1 миллиарду байтов. Иногда используется сокращенное название "гиг". Емкость накопителей на жестких дисках в большинстве персональных компьютеров измеряется в гигабайтах.
- *Терабайт (ТБайт)* равен приблизительно 1 триллиону байтов. Емкость накопителей на жестких дисках в высокопроизводительных системах измеряется в терабайтах.
- *Килобиты в секунду (Кбит/с)* — это одна тысяча битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.
- *Килобайты в секунду (Кбайт/с)* — это одна тысяча байтов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.
- *Мегабиты в секунду (Мбит/с)* — это один миллион битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Обычное соединение технологии Ethernet работает со скоростью 10 Мбит/с.
- *Мегабайты в секунду (Мбайт/с)* — это один миллион байтов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.
- *Гигабиты в секунду (Гбит/с)* — это один миллиард битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Соединение 10 Гбит/с Ethernet работает со скоростью 10 Гбит/с.
- *Терабиты в секунду (Тбит/с)* — это один триллион битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Некоторые высокоскоростные магистральные узлы сети Internet работают на скорости более 1 Тбит/с.
- *Герц (Гц)* — это единица измерения частоты. Описывает скорость изменения состояния периодического процесса в звуковых волнах, переменном токе или периодических процессах, в которых за время, равное 1 с, выполняется один цикл процесса (период).

- *Мегагерц (МГц)* равен миллиону периодов в секунду. Распространенная единица измерения скорости работы микросхем, таких, как компьютерные микропроцессоры. Некоторые беспроводные телефоны работают в том же диапазоне частот, что и процессоры (например, 900 МГц).
- *Гигагерц (ГГц)* равен тысяче миллионов, или миллиарду (1 000 000 000) периодов в секунду. Это распространенная единица измерения скорости микросхем, таких, как компьютерные микропроцессоры. Некоторые беспроводные телефоны и локальные сети работают в этом диапазоне (например, беспроводные сети стандарта 802.11b работают на частоте 2,4 ГГц).

ВНИМАНИЕ!

Процессоры персональных компьютеров постоянно становятся все более быстрыми. Микропроцессоры, которые использовались в 1980-х годах, в основном работали на частоте менее 10 МГц (у оригинального компьютера корпорации IBM частота процессора составляла 4,77 МГц). Используемые в настоящее время процессоры персональных компьютеров достигли скорости свыше 3 ГГц. Ведутся разработки более высокоскоростных процессоров. Подробнее этот вопрос рассматривается в следующих главах.

Поскольку в основе аппаратной логики компьютеров применяются переключатели, бинарные цифры и бинарные числа являются для него "родным языком". Люди используют десятичную систему в повседневной жизни, и им тяжело запомнить длинные последовательности нулей и единиц, которые использует компьютер. Следовательно, компьютерные бинарные числа необходимо переводить в десятичные.

Иногда двоичные числа требуется перевести в шестнадцатеричные. Они используются для записи большого количества двоичных цифр с помощью нескольких шестнадцатеричных, что позволяет их запоминать.

Десятичная система счисления

Система счисления состоит из символов и правил их использования. Существует множество систем счисления, но наиболее распространенной является *десятичная*, или система счисления с базисом 10. Она использует десять символов — цифры 0, 1, 2, 3, 4, 5, 7, 8 и 9. Комбинациями таких цифр можно выразить все возможные числовые значения (см. табл. 1.3).

Таблица 1.3. Десятичная система счисления

Количество символов	Десять			
Символы	0, 1, 2, 3, 4, 5, 7, 8, 9			
Степень базиса	10^3	10^2	10^1	10^0
Множитель знакоместа	1000	100	10	1
Пример: 2 134	2×10^3	1×10^2	3×10^1	4×10^0

Десятичная система счисления основана на степенях числа 10. Значение каждой позиции числа справа налево умножается на число 10 (основу или базис), возведенное в степень (порядок или показатель). Степень, в которую возводится число 10, зависит от позиции цифры относительно десятичной точки. Если рассматривать десятичное число справа налево, то первая цифра (правая) представляет степень 10^0 (1), вторая — 10^1 (10), третья — 10^2 ($10 \times 10 = 100$). Седьмая цифра, соответственно, равна 106 ($10 \times 10 \times 10 \times 10 \times 10 \times 10 = 1\,000\,000$), и т. д., вне зависимости от количества цифр в числе.

В качестве примера запишем число 2134:

$2134 = (2 \times 10^3) + (1 \times 10^2) + (3 \times 10^1) + (4 \times 10^0)$.

В данном примере цифра 4 стоит в позиции единиц, цифра 3 — в позиции десятков, цифра 1 — в позиции сотен и цифра 2 — в позиции тысяч. Приведенный пример кажется слишком очевидным при использовании десятичной системы, он важен для понимания принципов работы с другими системами счисления, такими, как двоичная и шестнадцатеричная. Обе системы счисления используют те же принципы определения числа, что и десятичная, и называются базисными. IP-адрес представляет из себя число, состоящее из 4 байтов, но для записи его в читабельном виде используется так называемая точечно-десятичная запись, в котором каждый байт представляется десятичным числом и байты разделены точками, например, 172.16.14.188. Тем не менее, компьютерные системы воспринимают и обрабатывают IP-адреса в виде последовательности из 32 битов, т.е. тридцати двух нулей и единиц, которые разбиты на группы по 8 символов и соответствуют десятичным числам адреса. Подробнее этот вопрос обсуждается далее в текущей главе.

Двоичная система счисления

Компьютер принимает и обрабатывает данные, используя *двоичную*, или систему счисления с базисом 2. В двоичной системе используются только два символа (0 и 1) вместо десяти, используемых в десятичной (с базисом 10). Значение каждой цифры определяется числом 2 (базовым числом), возведенным в степень позиции (связанную со знакоместом) цифры (2^0, 2^1, 2^2, 2^3, 2^4, и т.д.), как показано в табл. 1.4.

Таблица 1.4. Двоичная система счисления

Число символов	Два							
Символы	0,1							
Степень базиса	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Множитель знакоместа	128	64	32	16	8	4	2	1
Пример: 10110	0	0	0	1	0	1	1	0

Рассмотрим пример преобразования числа.

$10110 = (1\times2^4 = 16) + (0\times2^3 = 0) + (1\times2^2 = 4) + (1\times2^1 = 2) + (0\times2^0 = 0) =$

$= (16 + 0 + 4 + 2 + 0) = 22.$

Если двоичное число (10110) читать слева направо, то 1 находится в позиции 16, 0 — в позиции 8, 1 — в позиции 4, еще одна единица — в позиции 2 и 0 — в позиции 1. Складывая эти числа, получаем десятичное число 22. В компьютере IP-адрес представляется в виде строки из 32 битов (4 байтов).

Дополнительная информация: шестнадцатеричная система счисления

Система счисления с базисом 16 (шестнадцатеричная, hexadecimal, или просто hex) довольно часто используется при работе с компьютером, т.к. с ее помощью можно легко представить двоичные числа в читабельном виде. Компьютер производит вычисления в двоичном виде, но в некоторых ситуациях данные выводятся в шестнадцатеричном виде, поскольку имеют компактный вид и легче в таком виде воспринимаются.

Шестнадцатеричная система счисления использует 16 символов. Комбинацией используемых символов можно представить любое число. Поскольку только 10 символов могут быть представлены арабскими цифрами (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), а для шестнадцатеричной системы необходимо на шесть символов больше, то дополнительно используются буквы: A, B, C, D, E и F. A представляет десятичное число 10, B — число 11, C — число 12, D — число 13, E — число 14 и F — число 15 (см. табл. 1.5).

Позиция каждого символа (цифры) в шестнадцатеричном числе представляет базовое число 16, возведенное в степень позиции числа. Если рассматривать число справа налево, первая позиция представляет 16^0 (или 1), вторая позиция — 16^1 (или 16), третья позиция — 16^2 (или 256), и т.д. В качестве примера отметим, что физический адрес сетевого адаптера выражается строкой из двенадцати шестнадцатеричных символов.

Таблица 1.5. Шестнадцатеричная система счисления

Количество символов	Шестнадцать			
Символы	0, 1, 2, 3, 4, 5, 7, 8, 9, A, B, C, D, E, F			
Степень базиса	16^3	16^2	16^1	16^0
Множитель знакоместа	65536	256	16	1
Пример: 1A2C	1	A	2	C

Рассмотрим пример преобразования шестнадцатеричного числа в десятичное.

$1A2C = (1\times16^3 = 65536) + (10(A)\times16^2 = 2560) + (2\times16^1 = 32) + (12(C)\times16^0 = 12) =$

$= (65536 + 2560 + 32 + 12) = 68144.$

Алгоритм преобразования чисел из десятичной системы счисления в двоичную

Существует множество способов преобразования десятичных чисел в двоичные. Один из них проиллюстрирован на рис. 1.10. В этом алгоритме подбираются такие значения степеней двойки, чтобы в сумме они давали конвертируемое десятичное число. Показанная схема — это один из нескольких методов, которые чаще всего используются на практике. Наилучшим вариантом для специалиста будет выбрать один наиболее удобный для него метод и практиковаться в его применении до тех пор, пока преобразование чисел не будет всегда давать правильный результат.

Рассмотрим проиллюстрированный способ на конкретном примере.

Ниже приведена последовательность преобразования числа 168 в двоичную форму.

Этап 1. 128 больше, чем 168, следовательно, первый слева бит двоичного числа равен 1. 168-128 = 40.

Этап 2. 64 меньше, чем 40, следовательно, второй бит равен 0.

Этап 3. 32 больше, чем 40, следовательно, третий бит слева равен 1. 40-32 = 8.

Этап 4. 16 меньше, чем 8, следовательно, четвертый слева бит равен 0.

Этап 5. 8 равняется 8 (следовательно, можно отнять от остатка степень двойки и не получить отрицательный результат); пятый бит равен 1. 8-8 = 0, следовательно, остальные биты справа также равны 0.

Этап 6. В результате вычислений получаем число 10101000 — двоичный эквивалент десятичного числа 168.

Для дальнейшей практики попробуйте перевести из десятичной системы счисления в двоичную число 255. Результатом должно быть двоичное число 11111111.

С помощью блок-схемы, изображенной на рис. 1.10, можно переводить десятичные числа до 255 включительно. На выходе мы получим восьмизнаковое двоичное число, что является достаточным для перевода десятичных IP-адресов. Большие числа могут быть переведены в двоичную систему счисления с использованием дополнительных этапов, алгоритм начинается с наибольшей возможной степени числа 2, которая будет меньше переводимого числа. Например, для перевода числа 650 необходимо начинать вычитание с числа 29 = 512, что в результате даст десятизнаковое двоичное число.

Практическое задание 1.2.5. Преобразование числа из десятичной системы счисления в двоичную.

В этом практическом задании необходимо попрактиковаться в преобразовании десятичных чисел в двоичные.

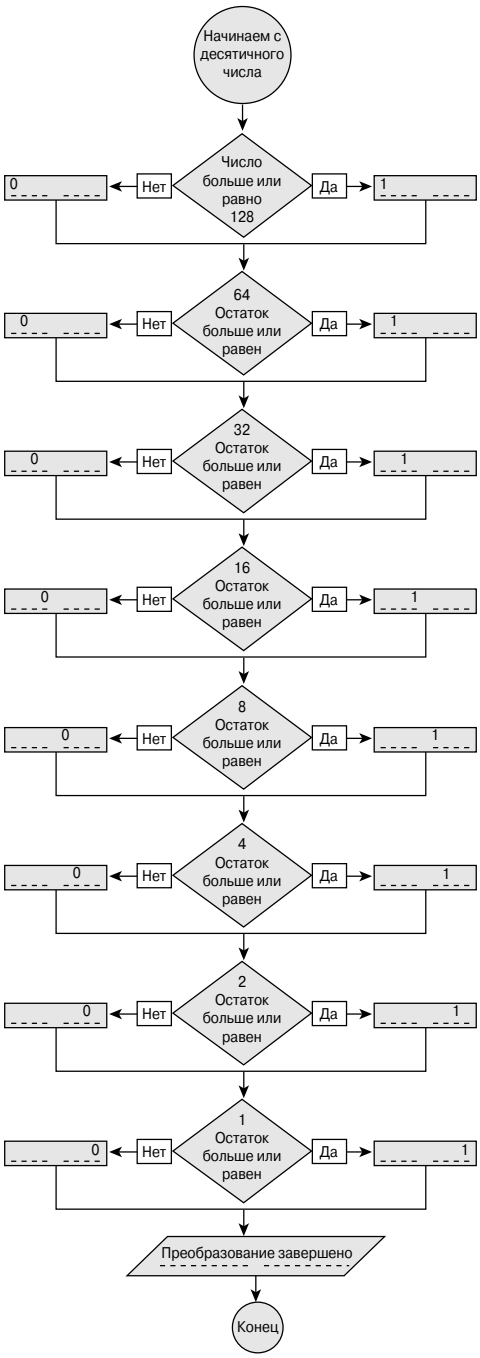


Рис. 1.10. Алгоритм преобразования десятичного числа в двоичное

Преобразование чисел из двоичной системы счисленияя в десятичную

Существует несколько методов пересчета чисел, как и для рассмотренного выше обратного преобразования. На блок-схеме, представленной на рис. 1.11, проиллюстрирован один из них.

Двоичные числа также могут быть конвертированы в десятичные простым умножением бинарных цифр на базисное число, возведенное в степень соответствующего знакоместа.

ВНИМАНИЕ!

Позиции в числе нумеруются справа налево, начиная с нулевой позиции. Любое число, возведенное в нулевую степень, равняется 1, например, $2^0 = 1$.

В качестве примера преобразуем двоичное число 01110000 в десятичное.

$0 \times 2^0 = 0$
+
$0 \times 2^1 = 0$
+
$0 \times 2^2 = 0$
+
$0 \times 2^3 = 0$
+
$1 \times 2^4 = 16$
+
$1 \times 2^5 = 32$
+
$1 \times 2^6 = 64$
+
$0 \times 2^7 = 0$

112

(Сумма степеней числа 2, у которых в их знакоместе стоит цифра 1.)

Как и блок-схема, приведенная выше (см. рис. 1.10), блок-схема на рис. 1.11 может быть использована для чисел до 255 включительно в десятичной системе счисления, что соответствует восьмибитовому двоичному числу. Большие двоичные числа могут быть преобразованы в десятичные с использованием больших степеней числа 2. Например, в двоичном числе, состоящем из 10 битов, десятая цифра будет иметь значение 512, а 9-я — 256, если в позиции цифры будет стоять 1.

Практическое задание 1.2.6. Преобразование числа из двоичной системы счисленияя в десятичную.

В этом практическом задании необходимо попрактиковаться в преобразовании двоичных чисел в десятичные.

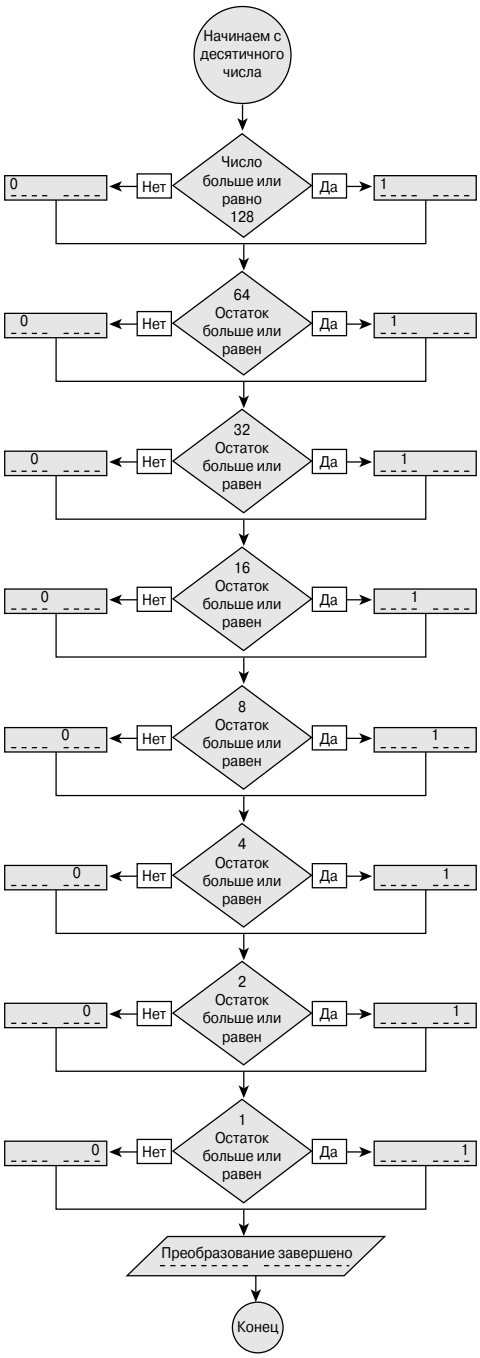


Рис. 1.11. Алгоритм преобразования двоичного числа в десятичное

Точечно-десятичное представление 32-битовых двоичных чисел

В настоящий момент адрес, который назначается компьютерам в сети Internet (IP-адрес), состоит из 32 битов. Для удобства работы с такими адресами 32-битовое число разбивают на группы десятичных чисел, а именно: разделяют двоичное число на четыре группы по 8 битов и затем переводят их в десятичные числа. Алгоритм преобразования чисел совпадает с описанным в разделе "Преобразование чисел из двоичной системы счисления в десятичную".

В стандартной записи полученные десятичные числа разделяются точкой, например, 10.15.129.201. Такая запись называется *точечно-десятичной* и позволяет записывать 32-битовый адрес в компактной и легко запоминаемой форме. Такое представление 32-битовых адресов часто используется в нашей книге, поэтому убедитесь, что его восприятие не вызывает трудностей. При обратном преобразовании в двоичную систему из точечно-десятичной записи необходимо помнить, что каждая группа, которая состоит из нескольких (от одной до трех) десятичных цифр, представляет собой восемь двоичных цифр. Если переводимое десятичное число меньше 128, то необходимо добавить слева к полученному двоичному числу такое количество нулей, чтобы в результате получилось восемь битов.

Так, например, точечно-десятичная запись 10.15.129.201 при преобразовании ее в двоичный эквивалент будет выглядеть как 00001010.00001111.10000001.11001001:

10 = 00001010,

15 = 00001111,

129 = 10000001,

201 = 11001001.

Шестнадцатеричные и двоичные преобразования

Преобразование шестнадцатеричных чисел в двоичные и наоборот — одна из распространенных задач при работе с конфигурационными регистрами маршрутизаторов. В маршрутизаторах корпорации Cisco Systems конфигурационный регистр состоит из 16 битов. Такое шестнадцатибитовое число может быть представлено в виде четырехзначного шестнадцатеричного числа, например, 0010000100000010 в двоичной системе счисления эквивалентно числу 2102 в шестнадцатеричной.

MAC-адреса (Media Access Control addresses — адреса второго уровня модели OSI) также обычно записываются в шестнадцатеричном виде.

ВНИМАНИЕ!

Подробнее MAC-адреса описаны в следующих главах. Сейчас адреса будут использованы только для иллюстрации процесса преобразования чисел из одной системы счисления в другую.

В технологиях Ethernet и Token Ring адрес второго уровня состоит из 48 битов, или 6 октетов (один октет равен одному байту). (*Oct* — от греческого *восемь*.) Поскольку такие адреса состоят из 6-ти отдельных октетов, то их можно представить в виде 12-ти шестнадцатеричных чисел. Каждые 4 бита представляются одним шестнадцатеричным числом ($2^4 = 16$), как показано в табл. 1.6.

Вместо записи вида

10101010.11110000.11000001.11100010.01110111.01010001

можно воспользоваться намного более короткой записью в шестнадцатеричном эквиваленте:

AA.F0.C1.E2.77.51.

A = 1010,

A = 1010,

F = 1111,

0 = 0000,

C = 1100,

1 = 0001,

E = 1110,

2 = 0010,

7 = 0111,

7 = 0111,

5 = 0101,

1 = 0001.

Для упрощения процесса манипулирования шестнадцатеричной записью MAC-адреса точка ставится только через каждые 4 шестнадцатеричных цифры, например AAF0.C1E2.7751.

Наиболее распространенным методом обозначения в компьютерах и программном обеспечении шестнадцатеричных чисел является добавление символов “0x” перед самим числом. Следовательно, если где-либо перед числом стоят указанные символы, то число является шестнадцатеричным, например, запись 0x1234 означает, что это шестнадцатеричное число 1234.

Как и другие базисные системы счисления (двоичная, десятичная и т.д.), шестнадцатеричная система счисления основывается на использовании цифр и базиса (16), возведенного в степень позиции числа. Символы, которые используются в шестнадцатеричной системе счисления, — это десятичные цифры от 0 до 9 и буквы от A до F. В табл. 1.6 показаны двоичные и десятичные эквиваленты шестнадцатеричных цифр.

Чтобы преобразовать шестнадцатеричное число в двоичное, достаточно отдельно перевести каждую цифру в 4 бита. Для преобразования шестнадцатеричного числа AC (т.е. 0xAC) в двоичное сначала преобразуем цифру A в двоичную запись 1010, а

затем цифру C — в 1100 и объединим. В итоге шестнадцатеричное число AC представляется двоичным 10101100.

Обратите внимание, что все возможные комбинации из 4-х бинарных цифр представляются единственной шестнадцатеричной цифрой; в то же время для того, чтобы представить 4 бита в десятичном виде, необходимо использовать две цифры. Именно поэтому с помощью двух шестнадцатеричных чисел можно легко представить любую комбинацию из 8 битов — байт (для сравнения: при использовании десятичной записи необходимы 4 цифры). Кроме того, если записывать байт десятичными цифрами, то может возникнуть путаница при обратном переводе. Так, например, восьмибитовое двоичное число 00011111 при использовании десятичных цифр записывается как 115. Как такую запись воспринимать? Как 11-5 или как 1-15? Если как 11-5, то при обратном переводе получим двоичное число 10110101, которое не совпадает с исходным. Используя шестнадцатеричную запись 1F, при обратном преобразовании всегда получим 00011111.

Таблица 1.6. Двоичный и десятичный эквиваленты шестнадцатеричных цифр

Двоичная запись	Шестнадцатеричная запись	Десятичная запись
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Наиболее просто воспринимать шестнадцатеричные числа как сокращенную запись двоичных. Она сокращает 8-битовое число до двух шестнадцатеричных цифр, при этом более легко воспринимаются длинные строки бинарных цифр и сокращается место, необходимое для их записи. Помните, что шестнадцатеричным числам могут предшествовать два символа 0x, которые не используются в вычислениях, и число 5D может записываться как 0x5D.

Для преобразования шестнадцатеричных чисел в двоичные необходимо просто развернуть каждую шестнадцатеричную цифру в ее четырехбитовый эквивалент.

Практическое задание 1.2.8. Преобразование чисел в шестнадцатеричную систему. В этом практическом задании необходимо попрактиковаться в преобразовании шестнадцатеричных чисел в десятичные и двоичные.

Булева логика

Булева логика используется в цифровых схемах, которые принимают на вход один или два уровня напряжения и на их основе генерируют выходное напряжение. В компьютерах два уровня напряжения соответствуют двум состояниям — логическому нулю и логической единице, которые, в свою очередь, соответствуют двум цифрам двоичной системы счисления. Булева логика — это двоичная логика, которая на основе сравнения двух чисел устанавливает выходное состояние логической схемы. Выделяют три простейших логических схемы (или логических операции) — "И" (AND), "ИЛИ" (OR) и "НЕ" (NOT). За исключением логической операции НЕ, булевы операции имеют схожие функции. Они принимают на вход два числа (0 или 1) и генерируют на выходе результат в соответствии с определенным набором правил.

Ниже рассматриваются булевы операции (начиная с операции НЕ), а затем приведен пример применения булевой логики в сетевых технологиях — операции с масками подсетей, которые используют логическую операцию И.

Логическая операция "НЕ" (табл. 1.7) просто инвертирует входное значение. Если на вход подается 1, то на выходе получим 0, и если на вход подается 0 — на выходе будет 1.

Таблица 1.7. Логическая операция "НЕ" (NOT)

Входное значение	Выходное значение
0	1
1	0

В логической операции "И" (табл. 1.8) используются два входных параметра. Если оба они равняются единице, то на выходе тоже будет единица, в противном случае на выходе будет логический ноль. Из четырех возможных комбинаций входных сигналов три на выходе будут иметь ноль, а одна комбинация — логическую единицу. Логическая операция "И" интенсивно используется при работе с IP-адресами и масками подсетей.

Логическая операция "ИЛИ" (табл. 1.9) также обрабатывает два входных параметра. Если значение одного или всех параметров равно 1, то на выходе будет получено значение, равное единице. Как и в операции "И", существуют четыре комбинации входных сигналов, однако, в отличие от операции "И", три комбинации дают на выходе логическую единицу, а одна комбинация — логический нуль.

Таблица 1.8. Логическая операция “И” (AND)

Логическое “И”	0	1
0	0	0
1	0	1

Таблица 1.9. Логическая операция “ИЛИ” (OR)

Логическое “ИЛИ”	0	1
0	0	1
1	1	1

При работе с масками подсетей и масками шаблонов используются булевы операции для фильтрации адресов, поскольку отдельный адрес идентифицирует конечное устройство в сети. С помощью масок устройства логически группируются в блоки, что упрощает различные сетевые операции.

IP-адреса и маски подсетей

Используемый в сети Internet 32-битовый адрес называется *IP-адресом (Internet Protocol address, IP-address)*. В первой части книги рассматривается соотношение между IP-адресом и масками подсетей. Более детально оба понятия описаны в главе 9, “Стек протоколов TCP/IP и IP-адресация”.

При назначении IP-адреса компьютеру некоторое число битов в левой части IP-адреса используется в качестве сети, при этом количество выделенных битов зависит от класса адреса. Биты в правой части IP-адреса идентифицируют конечный компьютер в сети. Компьютер или другое устройство, подключенное к сети, называется узлом (host). Следовательно, IP-адрес компьютера обычно состоит из двух частей — сетевой и узловой, которые соответственно идентифицируют определенную сеть и определенное устройство в сети.

Для того чтобы определить точку разделения IP-адреса на сетевую и узловую части, используется еще одно 32-битовое число, называемое *маской подсети*. Маска подсети служит для определения количества битов, которые используются в сетевой части адреса. В маске подсети значение каждого бита устанавливается равным 1; до тех пор, пока не будет определена сетевая часть, оставшиеся биты имеют значение 0. Биты в маске подсети, значение которых равно 0, определяют узловую часть адреса устройства в подсети. Ниже приведены примеры масок подсетей.

Пример 1:

11111111.00000000.00000000.00000000, при использовании точечно-десятичной записи — 255.0.0.0.

Пример 2:

11111111.11111111.00000000.00000000, при использовании точечно-десятичной записи — 255.255.0.0.

В первом примере первые восемь битов определяют сетевую часть адреса, оставшиеся 24 бита — узловую часть. Во втором примере первые 16 битов определяют сетевую часть адреса, оставшиеся 16 — узловую часть адреса устройства в подсети.

Преобразовав IP-адрес 10.34.23.134 в двоичный вид, получим 00001010.00100010.00010111.10000110.

Чтобы определить сетевую часть IP-адреса, необходимо выполнить над маской подсети и IP-адресом логическую операцию "И" побитово, записывая при этом полученный результат. Комбинация бита IP-адреса со значением 0 и нулевого бита маски подсети в результате дает 0. Комбинация 0 и 1 также дает 0. Комбинация из двух единиц на выходе даст единицу. Для более наглядной демонстрации рассмотрим конкретные примеры.

Пример 3: используем первую маску (255.0.0.0).

00001010.00100010.00010111.10000110 — IP-адрес.

11111111.00000000.00000000.00000000 — маска подсети.

00001010.00000000.00000000.00000000 — сетевая часть адреса.
В точечно-десятичной записи она будет равна 10.0.0.0.

Пример 4: используем вторую маску (255.255.0.0).

00001010.00100010.00010111.10000110 — IP-адрес.

11111111.11111111.00000000.00000000 — маска подсети.

00001010.00100010.00000000.00000000 — сетевая часть адреса.
В точечно-десятичной записи она будет равна 10.24.0.0.

Важность операций с масками подсетей становится очевидной при длительной работе с IP-адресами. На первом этапе важно понять принципы выполнения битовых операций с маской подсети и IP-адресом.

Резюме

В этой главе были рассмотрены такие ключевые понятия:

- компьютеры являются жизненно важными компонентами любой сети. Чем больше вы знаете о компьютерах, тем легче вам понять принципы работы сетей;
- знание внутренней структуры компьютеров помогает разобраться с принципами работы сетей;
- протокол TCP/IP является основным протоколом сети Internet;
- команда ping — это простейший способ проверить наличие соединения с удаленным устройством;

- программное обеспечение позволяет пользователям взаимодействовать с аппаратной частью компьютера. В сетях Web-браузеры и почтовые клиенты — это наиболее распространенные программные продукты;
- поиск неисправностей персональных компьютеров является одним из самых необходимых навыков при работе с сетями;
- важно разбираться в компонентах персонального компьютера и понимать функции сетевой карты. Необходимо уметь устанавливать новые сетевые адаптеры;
- биты — это цифры двоичной системы счисления. Восемь битов равняются одному байту;
- компьютер воспринимает и обрабатывает данные, используя двоичную систему счисления. Двоичная система счисления состоит из цифр 0 и 1;
- шестнадцатеричная система счисления часто используется при отображении двоичных данных. Шестнадцатеричная система счисления использует следующие символы в качестве цифр: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, и F;
- булева логика — это логика двоичных чисел, она позволяет сравнивать их. Три наиболее распространенных булевых операции — это "НЕ", "И" и "ИЛИ";
- IP-адрес — это 32-битовый адрес, который используется в сети Internet.

Для закрепления материала этой главы воспользуйтесь мультимедийными материалами на компакт-диске.

Ключевые термины

MAC-адрес (Media Access Control address — адрес второго уровня модели OSI). Стандартизированный адрес канального уровня, который назначается каждому устройству или порту, подключенному к локальной сети. Другие сетевые устройства используют такой адрес для нахождения определенных портов в сети, для создания и обновления таблиц маршрутизаций. Длина MAC-адреса равна 6 байтам, уникальность которых контролируется институтом IEEE.

ping. Аббревиатура от Packet Internet Groper, отправитель пакетов Internet. Команда, которая часто используется в IP-сетях для проверки доступности сетевого устройства.

Web-браузер. Клиентское приложение для отображения документов с гипертекстовой разметкой и обеспечения других служб, расположенных на удаленных Web-серверах в сети Internet, например, Internet Explorer и Netscape Navigator.

Американский стандартный код обмена информацией (American standard code for information interchange — ASCII). Наиболее распространенный код для представления буквенно-цифровых данных в компьютере, в котором используются двоичные числа для представления символов, набранных на клавиатуре.

Байт. Единица измерения, которая служит для описания размеров файлов данных, размера места на диске или другом носителе информации, для описания количества данных, переданных через сеть. 1 байт равен 8 битам.

Бит. Наименьшая единица данных в компьютере. Бит принимает значение 1 или 0 и является цифрой двоичного формата данных, который используется компьютером для хранения, передачи и обработки данных. В компьютере таким цифрам соответствуют положения переключателей (включен/выключен) или наличие/отсутствие электрического сигнала, светового импульса или радиоволн.

Блок питания. Блок, который обеспечивает электрическое питание компьютера.

Булева логика. В компьютерных операциях с двоичными значениями с помощью булевой логики вычисляются состояния электрических цепей (замкнутая или разомкнутая цепь) или электромагнитных состояний (наличие или отсутствие заряда). Компьютеры используют логические элементы "И" и "ИЛИ" для сравнения двух двоичных элементов, полученный результат используется для дальнейших вычислений.

Видеоплата, или видеокарта. Плата, устанавливаемая в компьютер, которая обеспечивает вывод графической информации.

Гигабайт (ГБ). Приблизительно равен 1 миллиарду байтов. Иногда используется название "гиг". Емкость накопителей на жестких дисках в большинстве современных персональных компьютеров измеряется в гигабайтах.

Гигабиты в секунду (Гбит/с). Один миллиард битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Технология 10G Ethernet работает со скоростью 10 Гбит/с.

Гиперссылка. Управляющая команда, по которой осуществляется переход на другие HTML-файлы на Web-сервере или определенные точки в том же документе. Предоставляет ускоренную навигацию по документам.

Двоичная система счисления. Система счисления с использованием цифр 0 и 1, которые в компьютерах соответствуют двум состояниям электрической цепи (разомкнутая и замкнутая).

Звуковая плата. Плата расширения, которая обеспечивает вывод аудиоинформации.

Килобайт (КБ). 1024 байта, при оценочных вычислениях используется значение 1000 байтов.

Килобайты в секунду (Кбайт/с). Одна тысяча байтов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.

Килобит (Кб). 1024 бита, при оценочных вычислениях используется значение 1000 битов.

Килобиты в секунду (Кбит/с). Одна тысяча битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.

Логическое подключение. Логическое подключение использует стандарты, называемые протоколами.

Материнская плата. Основная печатная плата компьютера.

Мегабайт (МБ). Равен 1 048 576 байтам, при оценочных вычислениях используется значение 1 миллион байтов. Мегабайт иногда называют "мег". Объем оперативной памяти в большинстве компьютеров обычно измеряется в мегабайтах. Большие файлы имеют размер порядка нескольких мегабайтов.

Мегабайты в секунду (Мбайт/с). Один миллион байтов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.

Мегабит (Мб). Приблизительно равен 1 миллиону битов.

Мегабиты в секунду (Мбит/с). Один миллион битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Обычное соединение Ethernet работает со скоростью 10 Мбит/с.

Международная Ассоциация производителей плат памяти для персональных компьютеров (Personal Computer Memory Card International Association — PCMCIA). Организация, которая разработала стандарт небольших устройств размером с кредитную карту, называемых PCMCIA-картами (иногда — PC-картами). Стандарт, изначально разработанный для расширения памяти портативных компьютеров, в последующем был расширен несколько раз и в текущий момент используется для подключения многих типов устройств.

Микропроцессор. Кремниевый кристалл, содержащий интегральные схемы.

Модем (modem). Устройство, которое преобразует цифровые и аналоговые сигналы. В качестве устройства передачи данных модем преобразует цифровые сигналы в аналоговые, которые затем передаются через аналоговые системы передачи данных. В качестве приемника данных модем преобразует аналоговый сигнал в начальную цифровую форму.

Модули памяти. Микросхемы оперативной памяти, расположенные на панелях памяти, вставляемые в материнскую плату.

Объединительная плата (backplane). Большая печатная плата, которая содержит разъемы для карт расширения.

Октет. 8 битов. В сетевых технологиях часто используется термин *октет* вместо термина *байт*, т.к. в некоторых аппаратных структурах размер байта не равен 8 битам.

Память с произвольным доступом (Random-access memory — RAM). Так называют оперативную память, в которую можно записывать новые данные и считывать сохраненные. При выключении питания содержимое памяти пропадает.

Параллельный порт. Интерфейс, через который может передаваться более одного бита информации одновременно. Используется для подключения различных внешних устройств, например, принтера.

Печатная плата (Printed circuit board — PCB). Тонкая плата, на которой расположены микросхемы и другие электрические компоненты.

Подключаемые программы. Программы, которые устанавливаются как часть Web-браузера и используются для отображения различной мультимедийной информации.

Подсеть. В IP-сетях — сеть, в которой используется общий адрес подсети. Подсети — это сети, произвольно сегментированные системным администратором для построения многоуровневой иерархической структуры, скрытой под общим адресом подключенной сети.

Порт клавиатуры. Используется для подключения клавиатуры к компьютеру.

Порт мыши. Используется для подключения устройства типа "мышь" к компьютеру.

Порт универсальной последовательной шины (Universal Serial Bus port — USB port). Интерфейс для подключения внешних устройств, таких, как "мышь", модемы, клавиатуры, сканеры и принтеры, которые могут подключаться и отключаться без перезагрузки системы.

Последовательный порт. Интерфейс, используемый для последовательной передачи данных, в котором за единицу времени передается только один бит.

Постоянное запоминающее устройство (Read-only memory — ROM). Тип компьютерной памяти, в которой данные предварительно записаны.

Привод компакт-дисков (CD-ROM). Оптический привод, который считывает информацию с компакт-дисков.

Привод накопителей на гибких дисках (Floppy disk drive — FDD). Устройство, которое может считывать и записывать информацию на гибкие диски.

Привод накопителей на жестких дисках (Hard disk drive — HDD). Считывает и записывает данные на жесткий диск, является основным устройством для хранения данных компьютера.

Прикладные программы. Программное обеспечение, которое интерпретирует данные, отображает информацию в доступном формате и является последним звеном в процессе установки соединения. Прикладные программы работают с протоколами для передачи и получения данных через сеть Internet.

Протокол Internet (Internet Protocol — IP). Протокол сетевого уровня в стеке протоколов TCP/IP; обеспечивает передачу данных между сетями без предварительной установки соединения.

Протокол передачи файлов (File Transfer Protocol — FTP). Протокол уровня приложений, часть стека протоколов TCP/IP, который используется для передачи файлов между сетевыми устройствами.

Протокол управления передачей/протокол Internet (Transmission Control Protocol/Internet Protocol — TCP/IP). Название набора протоколов, разработанных министерством обороны США в 1970-х годах для построения всемирной сети. TCP и IP — два наиболее известных протокола из этого стека.

Протокол. Формальное описание набора правил и соглашений, которые описывают, как именно устройства в сети обмениваются данными.

Разъем расширения. Разъем в компьютере, обычно на материнской плате, в который вставляются карты расширения для добавления новых возможностей компьютера.

Сетевой адаптер (NIC). Печатная плата, которая предоставляет возможность обмениваться данными с сетью.

Сеть Internet. Крупнейшая глобальная сеть, объединяющая десятки тысяч сетей по всему миру. Сеть Internet постоянно развивается, стандартизируется, а ее услуги постепенно проникают в сферу быта.

Системный блок. Основная часть персонального компьютера.

Терабайт (ТБ). Приблизительно 1 триллион байтов. Емкость накопителей на жестких дисках в высокопроизводительных системах измеряется в терабайтах.

Терабиты в секунду (Тбит/с). Один триллион битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Некоторые высокоскоростные магистральные узлы сети Internet работают на скорости более 1 Тбит/с.

Точечно-десятичная запись. Синтетическое представление 32-битовых чисел, которое состоит из четырех 8-битовых чисел, записанных в десятичном эквиваленте, и каждая группа из 8 битов разделяется точкой. Используется для представления IP-адресов в сети Internet, например, 192.67.67.20.

Физическое подключение. Физическое соединение с сетью осуществляется через подключение к компьютеру специализированных карт расширения, таких, как модем или сетевой адаптер, и кабеля.

Центральный процессор (Central processing unit — CPU). Процессор — это "мозг" компьютера, в котором выполняется большинство вычислений.

Шина (Bus). Набор электрических цепей, через которые передаются данные от одной части компьютера другой.

Шнур питания. Кабель для подключения электрического устройства к электрической розетке для подачи напряжения.

Язык гипертекстовой разметки (HyperText Markup Language — HTML). Простой язык гипертекстового форматирования документов, в котором используются теги (неотображаемый текст разметки документа) для указания способа представления частей документа программами-просмотрщиками, такими, как Web-браузеры.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. По каким причинам может быть недоступно соединение с сетью Internet?

а) Проблема с физическим соединением.

б) Проблема с логическим соединением.

в) Проблема с программным обеспечением.

г) Все вышеперечисленное.

2. Как называется основная печатная плата компьютера?

а) Подсистема персонального компьютера.

б) Материнская плата.

в) Плата расширений.

г) Память компьютера.

3. Что такое разъем PCMCIA?

а) Разъем расширения, используемый в портативных компьютерах.

б) Разъем расширения, используемый во всех компьютерах.

в) Разъем расширения для установки сетевого адаптера.

г) Разъем расширения для подключения специализированных устройств.

4. Что такое сетевой адаптер?

а) Адаптер распределенной сети.

б) Печатная плата, которая обеспечивает взаимодействие с сетью.

в) Плата, которая используется только в сетях Ethernet.

г) Стандартизированный адрес канального уровня модели OSI.

5. Что из перечисленного ниже является необходимым для установки сетевого адаптера?

а) Документация, в которой описана процедура настройки сетевого адаптера.

б) Средства диагностики сетевого адаптера.

в) Средства обнаружения и устранения аппаратных конфликтов.

г) Все перечисленное выше.

6. В какой системе счисления базисом служит число 2?

а) Восьмеричной.

б) Шестнадцатеричной.

в) Двоичной.

г) ASCII.

7. Расставьте термины в соответствии с их описанием, приведенным ниже.

- Бит.
- Байт.
- Кбит/с.
- Мегагерц.

а) Наименьшая единица измерения информации в компьютере.

б) Распространенная единица измерения скорости передачи данных через сетевое соединение.

в) Единица измерения частоты; скорость изменения состояний или периодичности системы в звуковых колебаниях, переменном напряжении или других циклических волновых процессах.

г) Единица измерения, которая используется для описания размеров файлов данных, места на дисках или других носителях информации или количества данных, переданных через сеть.

8. Какое наибольшее десятичное число может быть записано в 1 байте?

а) 254.

б) 256.

в) 255.

г) 257.

9. Какое двоичное число соответствует десятичному числу 151?

а) 10100111.

б) 10010111.

в) 10101011.

г) 10010011.

10. Какое десятичное число соответствует двоичному числу 11011010?

а) 186.

б) 202.

в) 218.

г) 222.

11. Какое шестнадцатеричное число соответствует десятичному числу 0010000100000000?

а) 0x2100.

б) 0x2142.

в) 0x0082.

г) 0x0012.

12. Какое двоичное число соответствует шестнадцатеричному числу 0x2101?

а) 0010 0001 0000 0001.

б) 0001 0000 0001 0010.

в) 0100 1000 0000 1000.

г) 1000 0000 1000 0100.

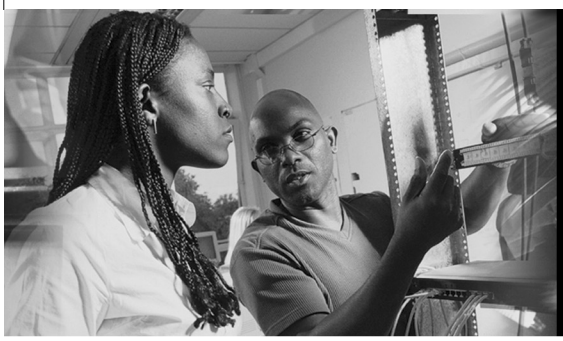
13. Какое из утверждений о команде **`ping`** является верным?

а) Команда **`ping`** используется для проверки сетевого соединения.

б) Ping — аббревиатура от packet Internet groper.

в) Команда **`ping 127.0.0.1`** используется для проверки работоспособности стека протоколов TCP/IP и функций приема и передачи сетевого адаптера.

г) Все перечисленное выше.



ГЛАВА 2

Основы сетевых технологий

В этой главе...

- описана история компьютерных сетей;
- описаны наиболее распространенные сетевые устройства и указано,
- на каких уровнях модели OSI они работают;
- даны определения шинной, звездообразной, расширенной звездообразной, иерархической, полносвязной и неполносвязной топологий;
- даны определения физической и логической топологий и рассмотрены их различия;
- дано определение сетевого протокола;
- определены и описаны функции сетей LAN, WAN, MAN, SAN и технология использования центра обработки данных;
- определены и описаны функции, технологии и преимущества виртуальных частных сетей VPN;
- описаны понятия внутренних и внешних сетей;
- рассмотрена полоса пропускания соединений и ее влияние на сетевую структуру;
- описаны единицы измерения полосы пропускания;
- перечислены ограничения по длине и полосе пропускания каналов;
- приведен пример расчета времени передачи данных;
- рассмотрены различия между цифровыми и аналоговыми сигналами;
- описан процесс коммуникации между уровнями;
- описаны достоинства эталонной модели OSI;
- обсуждаются функции каждого из семи уровней эталонной модели OSI;
- описаны основные процессы взаимодействия уровней эталонной модели OSI;
- рассмотрены уровни сетевой модели TCP/IP;
- описаны процессы инкапсуляции и декапсуляции данных при передаче информации по сети;
- описаны функции повторителя, концентратора, сетевого адаптера, моста, коммутатора и маршрутизатора;
- описаны функции голосового шлюза, мультиплексора DSLAM, системы CMTS и оптических устройств;
- описаны функции брандмауэра, AAA-сервера и VPN-концентратора;
- описаны функции адаптера беспроводной связи, точки доступа к беспроводной сети и моста

- перечислены ограничения по длине и полосе пропускания каналов;
- дано определение понятия *пропускная способность*;
- описаны функции адаптера беспроводной связи, точки доступа к беспроводной сети и моста беспроводной связи.

Ключевые определения главы

Ниже представлен список основных определений главы, полные расшифровки терминов приведены в конце.

локальная сеть, с. 84,
распределенная сеть, с. 85,
плата сетевого интерфейса, с. 87,
повторитель, с. 88,
концентратор, с. 89,
коллизия., с. 90,
домен коллизий, с. 90,
MAC-адрес, с. 90,
мост, с. 91,
лавинная рассылка, с. 92,
широковещание, с. 93,
широковещательный домен, с. 93,
коммутатор, с. 93,
микросегментация, с. 94,
маршрутизатор, с. 95,
брандмауэр, с. 98,
шинная топология, с. 104,
звездообразная топология, с. 105,
расширенная звездообразная тополоти, с. 106,
кольцевая топология, с. 106,
иерархическая топология, с. 107,
полносвязная *топология*, с. 109,
неполносвязная топология, с. 109,
топология, использующая передачу маркера, с. 109,
стек протоколов, с. 110,
протокол, с. 110,
сети хранилищ данных, с. 115,
центр обработки данных, с. 116,
виртуальная частная сеть, с. 117,
сеть Intranet, с. 119,
сеть Extranet, с. 119,
полоса пропускания, с. 120,
пропускная способность, с. 126,
Эталонная модель OSI, с. 132,
уровень приложений, с. 135,
уровень представления данных, с. 135,
сеансовый уровень, с. 135,
транспортный уровень, с. 135,
сетевой уровень, с. 136,
канальный уровень, с. 136,
физический уровень, с. 136,
одноранговая связь, с. 136,
сегмент, с. 137,
пакет, с. 137,
фрейм, с. 137,
инкапсуляция, с. 139,
декапсуляция, с. 141.

В этой главе даны определения некоторых терминов, используемых сетевыми специалистами и применяемых по отношению к различным типам компьютерных сетей. В ней объясняется, каким образом используемые на сегодняшний день стандарты повышают уровень совместимости различных сетевых технологий и расширяют возможности их взаимодействия. В ней также описывается, каким образом сетевая эталонная модель OSI поддерживает сетевые стандарты, а также рассмотрены базовые функции каждого уровня эталонной модели OSI. По мере изучения главы читателю станут ясны базовые функции каждого уровня модели OSI, что послужит базой для последующего проектирования и построения сети, а также для устранения в ней ошибок.

В последней части главы описаны различные сетевые устройства, кабельная и логическая структуры сети.

Обратите внимание на относящиеся к данной главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Сетевая терминология

В этом разделе дается определение сети для передачи цифровых данных и описывается история таких сетей. В ней также описываются базовые функции сетей следующих типов:

- локальных сетей (Local-Area Networks — LAN);
- распределенных сетей (Wide-Area Networks — WAN);
- городских или региональных сетей (Metropolitan-Area Networks — MAN);
- сетей хранилищ данных (Storage-Area Networks — SAN);
- центров обработки данных (Data center);
- внутренних сетей (Intranet-сети);
- внешних сетей (Extranet-сети);
- виртуальных частных сетей (Virtual Private Networks — VPN).

Сети для передачи цифровых данных

Сети передачи данных появились и начали развиваться из-за того, что на коммерческих предприятиях и в правительственных организациях возникла потребность в обмене электронной информацией на больших расстояниях. В то время микрокомпьютеры не были соединены между собой, как терминалы мейнфрейма с центральным блоком, и вследствие этого отсутствовал эффективный способ совместного использования данных несколькими микрокомпьютерами. На рис. 2.1 показан пример компании, использующей большое количество микрокомпьютеров, которые не соединены в одну сеть.

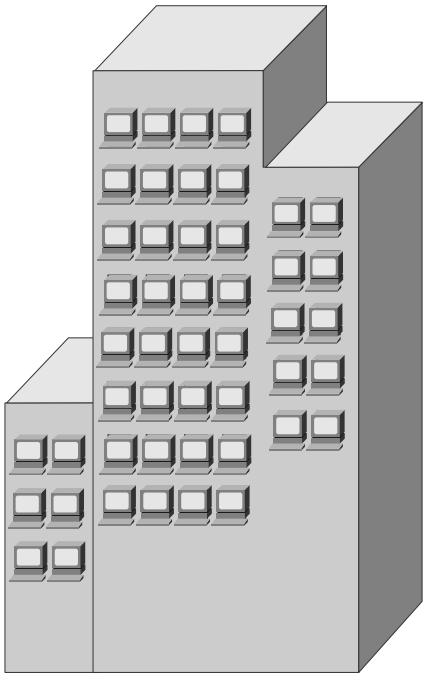


Рис. 2.1. Компания использует много отдельных изолированных компьютеров

ВНИМАНИЕ!

В те далекие годы, когда компьютерные технологии только-только начинали развиваться, компании вкладывали средства в компьютеры, которые были отдельными изолированными устройствами; к некоторым из них были подключены принтеры. Если сотруднику компании, работающему за компьютером без принтера, требовалось распечатать документ, то он копировал соответствующий файл на гибкий диск, переносил его к компьютеру, подсоединенному к принтеру, и распечатывал. Эта довольно примитивная версия сети была названа "флоппинет" (sneakernet[1]). Такая сеть показана на рис. 2.2.

С течением времени становилось очевидным, что совместное использование данных путем переноса их на гибких дисках является неэффективным и дорогостоящим способом работы. При изменении файла каждый раз требовалось произвести его обновление у всех остальных использующих его сотрудников. Если файл был изменен двумя сотрудниками и им требовалось в дальнейшем совместно его использовать, то один из наборов изменений неизбежно терялся. Предприятиям требовалось решить следующие вопросы:

[1] *Sneakernet (сленг) — в буквальном переводе обозначает сеть транспортировки данных "на своих двоих". Во многих странах ее называют* "флоппинет" *— по названию дисков (floppy), на которых переносят информацию. — Прим. ред.*

- как избежать дублирования оборудования и ресурсов?
- как осуществлять эффективную связь?
- как создать сеть и управлять ею?

Компании осознали, что применение сетевых технологий повысит производительность труда и позволит сэкономить средства. По мере появления новых сетевых технологий, аппаратных и программных продуктов, столь же стремительно появлялись новые сети и расширялись прежние. В начале 80-х годов XX века количество сетей резко увеличилось.

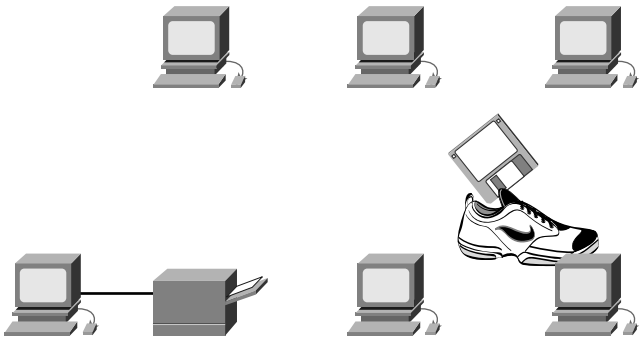


Рис. 2.2. Сеть "флоппинет"

В сетевых технологиях, которые появились в середине 80-х годов, использовалось самое разнообразное аппаратное и программное обеспечение. Каждая компания, разрабатывавшая аппаратное и программное обеспечение, использовала свои фирменные стандарты, что было вызвано жесткой конкуренцией с другими компаниями. Вследствие этого многие сетевые технологии оказались несовместимы друг с другом. В сетях, использующих разные спецификации, становилось все труднее осуществлять связь друг с другом; часто такая ситуация приводила к тому, что установка нового оборудования требовала полного удаления прежнего.

Одним из первых решений описанной выше проблемы стало создание стандартов *локальных сетей (Local-Area Network — LAN)*. Поскольку стандарты локальных сетей представляли собой открытый набор рекомендаций по созданию сетевого аппаратного и программного обеспечения, возможность использовать в одной сети оборудование разных производителей значительно увеличила устойчивость работы локальных сетей LAN. На рис. 2.3 показана несложная локальная сеть.

Однако по мере того, как компьютеры все больше использовались для работы в коммерческой сфере, становилось очевидным, что даже локальные сети не помогают решить все возникающие проблемы. В LAN-системе каждое подразделение компании представляет собой нечто вроде электронного острова, как показано на рис. 2.4.

Еще на ранних этапах создания LAN-сетей возникла потребность в быстрой и эффективной передаче информации не только в рамках одной компании, но и между

компаниями. Решением этой проблемы стало создание *городских* или *региональных сетей (Metropolitan-Area Network — MAN)* и *распределенных сетей (Wide-Area Network — WAN)*. Поскольку распределенные сети WAN соединяли пользователей, расположенных в обширной географической области, стало возможным осуществлять связь между компаниями, значительно удаленными друг от друга, как показано на рис. 2.5. Региональные сети позволяют установить связь в пределах некоторого региона, например, крупного города, нескольких населенных пунктов и т.д.

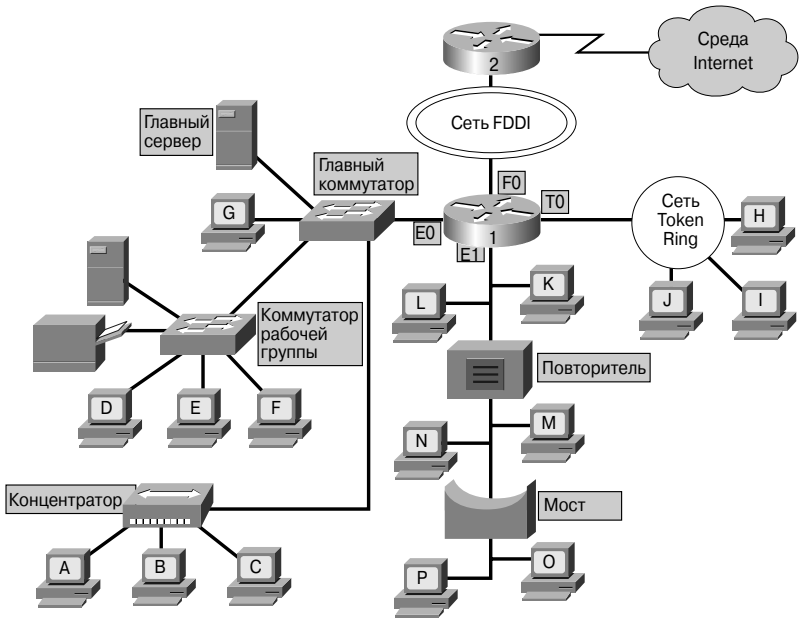


Рис. 2.3. Несложная локальная сеть

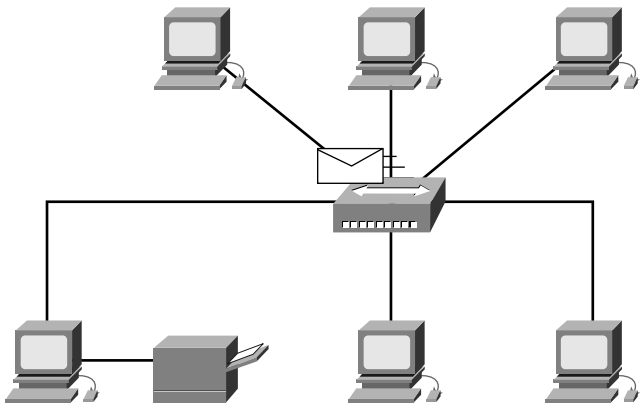


Рис. 2.4. Локальная сеть (LAN)

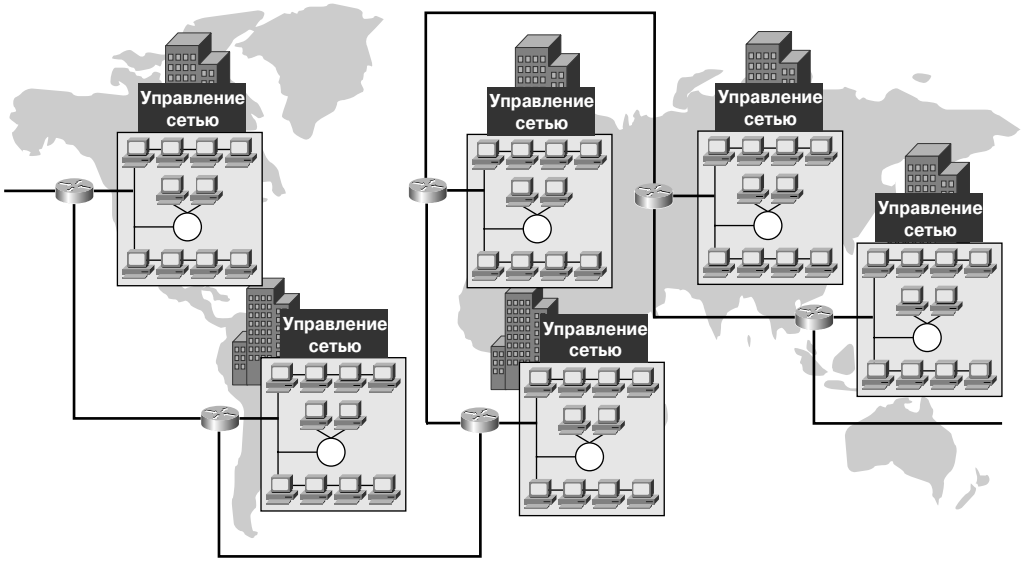


Рис. 2.5. Распределенная сеть (WAN)

История развития компьютерных сетей

История развития компьютерных сетей достаточно сложна; за прошедшие 35 лет в этом процессе приняли участие многие специалисты и пользователи сетей. В табл. 2.1 приведено краткое описание нескольких этапов эволюции компьютерных технологий сети Internet. Процесс создания и коммерческого применения новых типов сетей был значительно более сложным, однако целесообразно выделить его основные этапы.

В 40-х годах XX века компьютеры представляли собой большие электромагнитные устройства, подверженные частым сбоям. Создание в 1946 году полупроводникового транзистора открыло много новых возможностей для создания компактных и более надежных компьютеров. В 50-х годах крупные организации стали использовать компьютеры-мэйнфремы, которые выполняли программы, записанные на перфокартах. В конце 50-х годов были созданы первые интегральные микросхемы. Они включали в себя сначала несколько транзисторов, позднее количество транзисторов увеличивалось, а в настоящее время их количество в интегральной микросхеме достигает нескольких миллионов. На протяжении 60-х годов стало обычным использование мэйнфреймов с подключенными к ним терминалами, широко применялись интегральные микросхемы.

В конце 60-х годов — начале 70-х годов появились компьютеры меньшего размера, названные микрокомпьютерами (хотя по современным стандартам они имели довольно большие размеры). В 1977 году компания Apple Computer создала микрокомпьютер, названный персональным компьютером (Personal Computer — PC). В 1981 году корпорация IBM выпустила свой первый персональный компьютер PC.

Благодаря дружественному пользователю интерфейсу компьютера Apple Macintosh, открытой структуре IBM PC и дальнейшей микроминиатюризации интегральных схем PC стали широко применяться как в домашних условиях, так и на производствах.

Таблица 2.1. Развитие микрокомпьютерных технологий

Период времени	Этапы развития
Начало 40-х годов XX в.	Электромагнитные устройства больших размеров, подверженные частым сбоям
1947	Изобретение полупроводникового транзистора предоставило многочисленные возможности создания компактных и более надежных компьютеров
50-е годы	Изобретена интегральная микросхема. В ней на одном небольшом полупроводниковом кристалле объединялись несколько транзисторов, позднее их количество было увеличено (в настоящее время — миллионы)
60-е годы	Становится привычным использование мэйнфреймов с несколькими терминалами, широко применяются интегральные микросхемы
Конец 60-х годов и 70-е годы XX в.	Появляются небольшие компьютеры, которые стали называть миникомпьютерами
1977	Компания Apple Computer создает микрокомпьютер, названный персональным компьютером (Personal Computer — PC)
1981	Корпорация IBM создает свой первый персональный компьютер
Середина 80-х годов	Пользователи, работающие на отдельных, изолированных друг от друга компьютерах, начинают обмениваться данными (файлами) с помощью модема, подсоединенного к другому компьютеру. Этот способ связи получил название соединения “точка-точка”, или удаленного соединения

В середине 80-х годов пользователи, работающие на изолированных компьютерах, стали совместно использовать данные (файлы) с помощью модемов, подсоединенных к другому компьютеру. Такой вид связи назвали *соединением типа “точка-точка”*, или *соединением удаленного доступа*. Данный подход был впоследствии расширен путем использования специально выделенных компьютеров, которые служили центральными точками связи для соединений удаленного доступа. Такие компьютеры получили название *электронные доски объявлений*[2] *(bulletin board)*. Пользователи подсоединялись к доске объявлений, оставляли там свои сообщения, получали сообщения от других пользователей, загружали в систему файлы или переписывали на свой компьютер файлы из нее. Недостатком такой системы был очень низкий уровень

[2] *BBS — Bulletin Board System, система электронных досок объявлений, в которой через интерфейс терминального доступа можно пользоваться электронной почтой, перекачивать нужные файлы и (в последнее время) получать отдельные услуги Internet. На сегодняшний день такие системы мало распространены. — Прим. ред.*

прямых соединений пользователей друг с другом, а часто такое непосредственное соединение вообще отсутствовало. Кроме того, соединение можно было установить лишь с теми, кто знал о существовании доски объявлений. Другим существенным ограничением было то, что компьютер, выполняющий роль доски объявлений, требовал отдельного модема для каждого соединения с другим компьютером в сети. При одновременной работе пяти пользователей на доске объявлений требовались пять модемов, подсоединенных к пяти отдельным телефонным линиям. Можно себе представить, что бы произошло, если бы 500 пользователей захотели подсоединиться к доске объявлений одновременно!

С начала 60-х годов и вплоть до конца 90-х годов XX века Министерство обороны США (U.S. Department of Defense — DoD) разрабатывало крупные и надежные распределенные WAN-сети для военных и научных целей. Эта технология значительно отличалась от соединений типа "точка-точка", используемых в досках объявлений. Она позволяла соединять между собой большое количество компьютеров с использованием многих маршрутов. Сама сеть определяла, каким образом передавать данные от одного компьютера другому. При использовании такого типа связи стало возможным по одному соединению осуществлять связь со многими компьютерами, в отличие от прежней технологии, которая позволяла осуществлять только одно соединение. Сеть Министерства обороны постепенно превратилась в сеть Internet.

Сетевые устройства

Оборудование, непосредственно подсоединенное к сегменту сети, называется *сетевым устройством (device)*. Все устройства могут быть отнесены к одной из двух групп:

- **устройства конечного пользователя**. В эту группу входят компьютеры, принтеры, сканеры и другие устройства, которые выполняют функции, необходимые непосредственно пользователю сети;
- **сетевые устройства**. В эту группу входят устройства, подсоединенные к устройствам конечного пользователя и позволяющие им осуществлять связь друг с другом.

Устройства конечного пользователя, которые связывают его с сетью, также называются *оконечными узлами или станциями (host)*. На рис. 2.6 показано устройство конечного пользователя — рабочая станция.

Устройства данного типа позволяют пользователю создавать, получать и совместно с другими пользователями использовать информацию. Конечные устройства могут функционировать и без сети, но без нее их возможности в значительной степени ограничены. Эти устройства физически подсоединяются к сети с помощью *платы сетевого интерфейса (Network Interface Card — NIC)*, также называемой *сетевым адаптером*. Конечные устройства используют сетевое соединение для выполнения таких задач, как отправка сообщений по электронной почте, распечатка отчетов, переписывание рисунков и доступ к базам данных. Адаптер NIC представляет собой печатную плату, которая вставляется в гнездо расширения (слот) шины на

материнской плате компьютера или может быть отдельным периферийным устройством. У переносных портативных компьютеров адаптер NIC обычно имеет размеры карты PCMCIA.

Рис. 2.6. Устройство конечного пользователя — рабочая станция

Каждый адаптер NIC имеет уникальный код, называемый MAC-адресом. MAC-адреса мы рассмотрим несколько позже. Как указывает само название, карта сетевого интерфейса NIC управляет доступом рабочей станции к среде передачи. В сетевой сфере отсутствуют стандартные символы для устройств конечного пользователя. Чтобы их было проще распознать, конечные устройства обозначаются пиктограммами, похожими на реальное оборудование.

Сетевые устройства обеспечивают транспортировку данных, которые необходимо передавать между устройствами конечного пользователя. Они удлиняют и объединяют кабельные соединения, преобразуют данные из одного формата в другой и управляют передачей данных. Примерами устройств, выполняющих перечисленные функции, являются повторители, концентраторы, мосты, коммутаторы и маршрутизаторы. В последующих разделах приведен обзор некоторых типичных сетевых устройств.

Повторители

Повторители (repeater) представляют собой сетевые устройства, функционирующие на первом (физическом) уровне эталонной модели OSI. Для того чтобы понять работу повторителя, необходимо знать, что по мере того, как данные покидают устройство отправителя и выходят в сеть, они преобразуются в электрические или световые импульсы, которые после этого передаются по сетевой передающей среде. Такие импульсы называются *сигналами (signals)*. Когда сигналы покидают передающую станцию, они являются четкими и легко распознаваемыми. Однако чем больше длина кабеля, тем более слабым и менее различимым становится сигнал по мере прохождения по сетевой передающей среде. Целью использования повторителя является регенерация и ресинхронизация сетевых сигналов на битовом уровне, что позволяет передавать их по среде на большее расстояние. Термин *повторитель*

(repeater) первоначально означал отдельный порт "на входе" некоторого устройства и отдельный порт на его "выходе". В настоящее время используются также повторители с несколькими портами. В эталонной модели OSI повторители классифицируются как устройства первого уровня, поскольку они функционируют только на битовом уровне и не просматривают другую содержащуюся в пакете информацию.

Концентраторы

Использование *концентраторов (hub)* обусловлено необходимостью в регенерации и ресинхронизации сетевых сигналов. Характеристики концентратора аналогичны характеристикам повторителя. Как показано на рис. 2.7, концентратор является общей точкой для нескольких сетевых соединений. Концентраторы обычно соединяют между собой несколько сегментов локальной сети LAN. Концентратор имеет несколько портов. Когда на порт концентратора поступают пакеты, они копируются на все остальные порты и в результате могут быть просмотрены всеми сегментами LAN-сети.

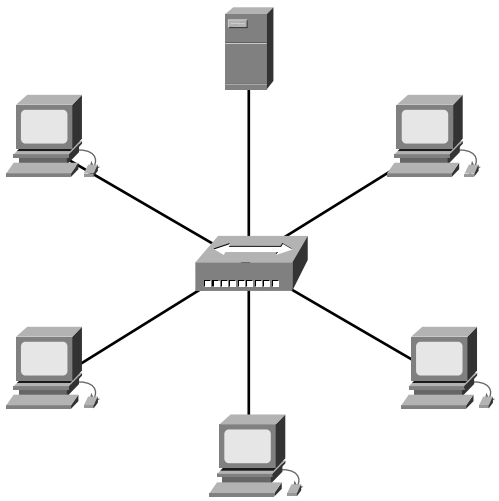


Рис. 2.7. Концентратор

Поскольку концентраторы и повторители имеют похожие характеристики, первые часто называют *многопортовыми повторителями (multiport repeater*). Разница между повторителем и концентратором состоит лишь в количестве кабелей, подсоединенных к устройству. В то время как повторитель имеет только два порта, концентратор обычно имеет от 4 до 20 и более портов, как показано на рис. 2.8.

Ниже приведены наиболее важные свойства устройств данного типа:

- концентраторы усиливают сигналы;
- концентраторы распространяют сигналы по сети;
- концентраторам не требуется фильтрация;

- концентраторам не требуется определение маршрутов и коммутации пакетов;
- концентраторы используются как точки объединения трафика в сети.

Рис. 2.8. Концентраторы имеют несколько портов

Как правило, концентраторы используются в сетях 10BASE-T или 100BASE-T (более подробно сети Ethernet описаны в главе 7, "Технологии Ethernet"). Концентраторы создают центральную точку соединений для кабельной среды. Они также повышают надежность сети, поскольку обрыв одного из кабелей не нарушает работу всей сети. Эта функция устройства отличает сети с концентраторами от сетей с шинной топологией, в которых обрыв одного из кабелей выводит из строя всю сеть (сетевые топологии обсуждаются ниже в настоящей главе). Концентраторы считаются устройствами первого уровня, поскольку они всего лишь регенерируют сигнал и повторяют его на всех своих портах (на выходных сетевых соединениях). В сетях Ethernet все рабочие станции подсоединены к одной и той же физической передающей среде. Сигналы, передаваемые по этой общей среде, принимаются другими устройствами сети. *Коллизия (collision)* представляет собой ситуацию, в которой два или более битов распространяются по одной и той же сети одновременно. Область сети, в которой создаваемые пакеты могут испытать коллизию, называется *доменом коллизий (collision domain*). Сеть с совместно используемой средой передачи данных является доменом коллизий, называемым также доменом разделяемой полосы пропускания (*bandwidth domain*). Более подробно домены коллизий рассмотрены в главе 6, "Основы технологии Ethernet".

Как уже говорилось, функция устройств первого уровня состоит лишь в содействии передаче сигнала по сети. Такие устройства не распознают ни информационные модели сигналов, ни адреса, ни данные. В случае, когда кабели соединены с помощью концентратора или повторителя, все их соединения являются частью коллизионного домена.

Сетевые карты

Платы (или карты) сетевых интерфейсов (Network Interface Card — NIC), коротко называемые *сетевыми картами*, рассматриваются как устройства второго уровня, поскольку все выпускаемые в мире адаптеры имеют уникальный код, называемый адресом *управления доступом к среде передачи* (*Media Access Control — MAC*), или MAC-адресом. Этот адрес управляет обменом данными между рабочей станцией и локальной сетью LAN. Адаптер NIC управляет доступом рабочей станции к среде передачи. На рис. 2.9 показан адаптер NIC.

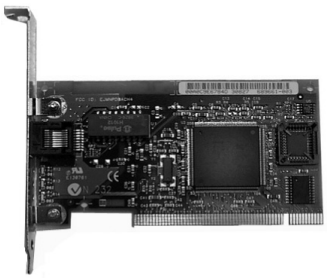


Рис. 2.9. Плата сетевого интерфейса

Мосты

Мост (bridge) представляет собой устройство второго уровня, предназначенное для создания двух или более сегментов локальной сети LAN, каждый из которых является отдельным коллизионным доменом. Иными словами, мосты предназначены для более рационального использования полосы пропускания. Целью моста является фильтрация потоков данных в LAN-сети с тем, чтобы локализовать внутрисегментную передачу данных и вместе с тем сохранить возможность связи с другими частями (сегментами) LAN-сети для перенаправления туда потоков данных. Каждое сетевое устройство имеет связанный с NIC-картой уникальный MAC-адрес. Мост собирает информацию о том, на какой его стороне (порте) находится конкретный MAC-адрес, и принимает решение о пересылке данных на основании соответствующего списка MAC-адресов. Мосты осуществляют фильтрацию потоков данных на основе только MAC-адресов узлов. По этой причине они могут быстро пересылать данные любых протоколов сетевого уровня. На решение о пересылке не влияет тип используемого протокола сетевого уровня, вследствие этого мосты принимают решение только о том, пересылать или не пересылать фрейм, и это решение основывается лишь на MAC-адресе получателя. Ниже приведены наиболее важные свойства мостов.

- Мосты являются более "интеллектуальными" устройствами, чем концентраторы. "Более интеллектуальные" в данном случае означает, что они могут анализировать входящие фреймы и пересылать их (или отбросить) на основе адресной информации.
- Мосты собирают и передают пакеты между двумя или более сегментами LAN-сети.
- Мосты увеличивают количество доменов коллизий[3], что позволяет нескольким устройствам передавать данные одновременно, не вызывая коллизий.
- Мосты поддерживают таблицы MAC-адресов.

На рис. 2.10 проиллюстрирован пример использования моста. Внешний вид мостов может значительно различаться в зависимости от типа и модели.

[3] *И уменьшают их размер за счет сегментации локальной сети. — Прим. ред.*

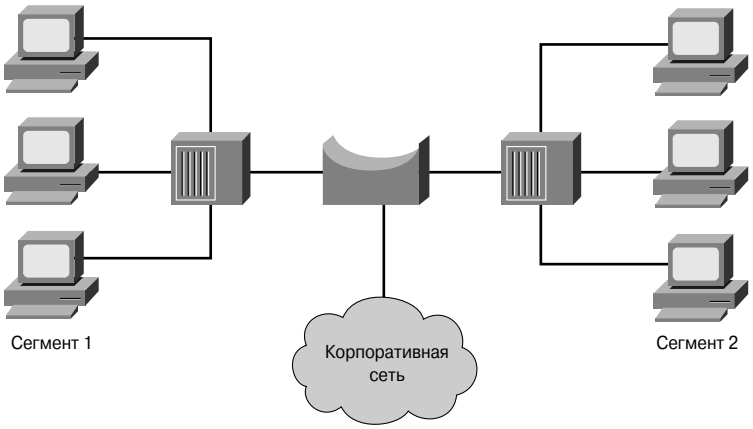


Рис. 2.10. Мост

Отличительными функциями моста являются фильтрация фреймов на втором уровне и используемый при этом способ обработки трафика. Для фильтрации или выборочной доставки данных мост создает таблицу всех MAC-адресов, расположенных в данном сетевом сегменте и в других известных ему сетях, и преобразует их в соответствующие номера портов. Этот процесс подробно описан ниже.

Этап 1. Если устройство пересылает фрейм данных впервые, мост ищет в нем MAC-адрес устройства-отправителя и записывает его в свою таблицу адресов.

Этап 2. Когда данные проходят по сетевой среде и поступают на порт моста, он сравнивает содержащийся в них MAC-адрес пункта назначения с MAC-адресами, находящимися в его адресных таблицах.

Этап 3. Если мост обнаруживает, что MAC-адрес получателя принадлежит тому же сетевому сегменту, в котором находится отправитель, то он не пересылает эти данные в другие сегменты сети. Этот процесс называется *фильтрацией (filtering)*. За счет такой фильтрации мосты могут значительно уменьшить объем передаваемых между сегментами данных, поскольку при этом исключается ненужная пересылка трафика.

Этап 4. Если мост определяет, что MAC-адрес получателя находится в сегменте, отличном от сегмента отправителя, он направляет данные только в соответствующий сегмент.

Этап 5. Если MAC-адрес получателя мосту неизвестен, он рассылает данные во все порты, за исключением того, из которого эти данные были получены. Такой процесс называется *лавинной рассылкой (flooding)*. Лавинная рассылка фреймов также используется в коммутаторах.

Этап 6. Мост строит свою таблицу адресов (зачастую ее называют мостовой таблицей или таблицей коммутации), изучая MAC-адреса отправителей во

фреймах. Если MAC-адрес отправителя блока данных, фрейма, отсутствует в таблице моста, то он вместе с номером интерфейса заносится в адресную таблицу. В коммутаторах, если рассматривать (в самом простейшем приближении) коммутатор как многопортовый мост, когда устройство обнаруживает, что MAC-адрес отправителя, который ему известен и вместе с номером порта занесен в адресную таблицу устройства, появляется на другом порту коммутатора, то он обновляет свою таблицу коммутации. Коммутатор предполагает, что сетевое устройство было физически перемещено из одного сегмента сети в другой.

ВНИМАНИЕ!

Коммутаторы используют те же концепции и этапы работы, которые характерны для мостов. В самом простом случае коммутатор можно назвать многопортовым мостом, но в некоторых случаях такое упрощение неправомерно.

Широковещательным (broadcast) называется пакет, который рассылается всем узлам сети. *Широковещательный домен (broadcast domain)* состоит из всех устройств, подсоединенных к сети, которые получают широковещательные пакеты, отправленные каким-либо узлом всем остальным узлам сети. Поскольку широковещательные пакеты (MAC-адрес таких пакетов равен FF.FF.FF.FF.FF.FF) должны быть получены всеми устройствами сети, мосты пересылают их в любом случае. Поэтому в сети, которая построена с использованием мостов, совокупность всех сегментов рассматривается как один широковещательный домен.

Точно так же, как концентратор является многопортовым повторителем, так и *коммутатор (switch*) выполняет функции моста, но может одновременно создавать несколько мостовых соединений и имеет много портов. Более подробно коммутаторы рассматриваются в следующем разделе.

Коммутаторы второго уровня

Коммутаторы второго уровня, также называемые коммутаторами локальных сетей (LAN), часто служат для замены совместно используемых концентраторов; они могут быть установлены в сеть с уже существующей кабельной инфраструктурой с минимальным нарушением работы сети. На рис. 2.11 приведен пример коммутатора.

Подобно мостам, коммутаторы соединяют между собой сегменты LAN-сетей, используют таблицы MAC-адресов для определения сегмента, в который следует направить фреймы, и уменьшают объем передаваемых данных. Однако коммутаторы работают со значительно бо́льшими скоростями, чем мосты.

Как и мосты, коммутаторы являются устройствами канального уровня и позволяют объединить несколько физических сегментов локальной сети в одну сеть большего размера. Как и мосты, коммутаторы пересылают данные или выполняют лавинную рассылку на основе MAC-адресов.

Рис. 2.11. Коммутатор

Поскольку коммутация осуществляется на аппаратном уровне, это происходит значительно быстрее, чем аналогичная функция, выполняемая мостом с помощью программного обеспечения[4]. Каждый порт коммутатора можно рассматривать как отдельный микромост. При этом каждый порт коммутатора предоставляет каждой рабочей станции всю полосу пропускания передающей среды. Такой процесс называется микросегментацией.

Микросегментация (microsegmentation) позволяет создавать частные, или выделенные сегменты, в которых имеется только одна рабочая станция. Каждая такая станция получает мгновенный доступ ко всей полосе пропускания, и ей не приходится конкурировать с другими станциями за право доступа к передающей среде. В дуплексных коммутаторах не происходит коллизий, поскольку к каждому порту коммутатора подсоединено только одно устройство.

Однако, как и мост, коммутатор пересылает широковещательные пакеты всем сегментам сети. Поэтому в сети, использующей коммутаторы, все сегменты должны рассматриваться как один широковещательный домен.

Некоторые коммутаторы, главным образом самые современные устройства и коммутаторы уровня предприятия, способны выполнять операции на нескольких уровнях. Например, устройства серий Cisco 6500 и 8500 выполняют некоторые функции третьего уровня. Показанный на рис. 2.12 коммутатор Cisco Catalyst 8500 представляет собой усовершенствованный ATM-коммутатор с функциями третьего уровня, который гармонично интегрирует функции ATM-коммутации и коммутации на третьем уровне, происходящей со скоростью передачи сигнала по проводу. Применение коммутаторов семейства Catalyst 8500 является эффективным решением в территориальных сетях (в сетях университетских городков, предприятий и т.п.) и в сетях городского масштаба MAN, поскольку эти коммутаторы обладают масштабируемой производительностью, стоят недорого и содержат функции Intranet-приложений, что обеспечивает их повышенную коммерческую эффективность. В отличие от прежних ATM-коммутаторов первого и второго поколений, которые вынуждали пользователя применять дорогие и малоэффективные многосистемные решения, коммутаторы Catalyst 8500 обеспечивают интеграцию технологий ATM и Gigabit Ethernet на одном шасси. Механизмы многоуровневой коммутации выходят за рамки данной книги и курса CCNA, поэтому основное внимание будет уделено только коммутаторам второго уровня.

[4] *Следует обратить внимание, что мост считается устройством с программной, коммутатор — с аппаратной коммутацией. — Прим. ред.*

Рис. 2.12. Коммутатор Catalyst 8500

Маршрутизаторы

Маршрутизаторы (router) представляют собой устройства объединенных сетей, которые пересылают пакеты между сетями на основе адресов третьего уровня (рис. 2.13). Маршрутизаторы способны выбирать наилучший путь в сети для передаваемых данных. Функционируя на третьем уровне, маршрутизатор может принимать решения на основе сетевых адресов вместо использования индивидуальных MAC-адресов второго уровня. Маршрутизаторы также способны соединять между собой сети с различными технологиями второго уровня, такими, как Ethernet, Token Ring и Fiber Distributed Data Interface (FDDI — распределенный интерфейс передачи данных по волоконно-оптическим каналам). Обычно маршрутизаторы также соединяют между собой сети, использующие технологию асинхронной передачи данных ATM (Asynchronous Transfer Mode — ATM) и последовательные соединения. Вследствие своей способности пересылать пакеты на основе информации третьего уровня, маршрутизаторы стали основной магистралью глобальной сети Internet и используют протокол IP.

Рис. 2.13. Маршрутизатор

Задачей маршрутизатора является инспектирование входящих пакетов (а именно, данных третьего уровня), выбор для них наилучшего пути по сети и их коммутация на соответствующий выходной порт. В крупных сетях маршрутизаторы являются главными устройствами, регулирующими перемещение по сети потоков данных. В принципе маршрутизаторы позволяют обмениваться информацией любым типам компьютеров.

Маршрутизаторы и механизмы третьего уровня эталонной модели взаимодействия открытых систем подробнее описаны в следующих главах.

Голосовые устройства, DSL-устройства, кабельные модемы и оптические устройства

Возникший в последнее время спрос на интеграцию голосовых и обычных данных и быструю передачу данных от конечных пользователей в сетевую магистраль привел к появлению следующих новых сетевых устройств:

- голосовых шлюзов, используемых для обработки интегрированного голосового трафика и обычных данных;
- мультиплексоров DSLAM, используемых в главных офисах провайдеров служб для концентрации соединений DSL-модемов от сотен индивидуальных домашних пользователей;
- терминальных систем кабельных модемов (Cable Modem Termination System — CMTS), используемых на стороне оператора кабельной связи или в головном офисе для концентрации соединений от многих подписчиков кабельных служб;
- оптических платформ для передачи и получения данных по оптоволоконному кабелю, обеспечивающих высокоскоростные соединения.

Подробнее перечисленные нами устройства и соответствующие технологии описаны во второй части книги.

Дополнительная информация: голосовые шлюзы

Под *шлюзом (gateway)* понимается устройство специального назначения, которое преобразует информацию из одного стека протоколов в другой. Универсальный сервер доступа серии Cisco AS5400 представляет собой высокоэффективную в финансовом отношении платформу для объединения функций маршрутизации, удаленного доступа, голосового шлюза, брандмауэра и блока цифровых модемов. На рис. 2.14 показан многофункциональный шлюз серии Cisco AS5400, предоставляющий на любом из своих портов универсальные службы передачи обычных данных, голосовых данных, средств беспроводной связи и передачи факсимильных данных.

Мультиплексоры DSLAM

Мультиплексор доступа к абонентским цифровым каналам (Digital Subscriber Line Access Multiplexer — DSLAM) представляет собой устройство, которое используется в ряде DSL-технологий. Мультиплексор DSLAM служит интерфейсом между оборудованием абонента и сетью оператора связи. На рис. 2.15 показан усовершенствованный мультиплексор доступа DSL серии Cisco 6100.

Рис. 2.14. Универсальный шлюз серии Cisco AS5400

Рис. 2.15. DSLAM-мультиплексор Cisco 6100

Системы CMTS

Операторы кабельной связи используют терминирующие системы кабельных модемов (Cable Modem Termination System — CMTS) в различных точках концентрации или в концентраторах кабельной сети для предоставления высокоскоростного доступа к сети Internet, голосовых и других сетевых служб индивидуальным пользователям и коммерческим предприятиям. Универсальный широкополосный маршрутизатор (Universal Broadband Router) CMTS серии uBR7100 предназначен для модулей MTU (multitenant units — блоков на большое количество абонентов), таких, как многоквартирные дома и отели. Модели высокой мощности, подобные маршрутизатору серии uBR10012, показанному на рис. 2.16, способны обрабатывать данные от тысяч потребителей.

Рис. 2.16. Система CMTS серии Cisco uBR1001

Оптические платформы

Для работы в оптических сетях, которые изначально являются магистральными и используют технологию распределенных сетей, созданы несколько оптических платформ. На рис. 2.17 показана оптическая сетевая система мультиплексирования высокой плотности по длине волны (Dense Wavelength Division Multiplexing — DWDM) Cisco ONS 15454. Эта система обеспечивает выполнение функций многих сетевых элементов на одной платформе.

Устройства для защиты сетей

В связи со значительным ростом числа Internet- и Extranet-соединений и по мере того, как все больше телеработников и мобильных пользователей хотят получать удаленный доступ к сети предприятия, возрастает важность обеспечения безопасности в сетях предприятий. Компонентами систем защиты сетей являются брандмауэры, AAA-серверы и VPN-концентраторы.

Брандмауэры

Термин *брандмауэр (firewall)* используется либо по отношению к программному обеспечению, работающему на маршрутизаторе или сервере, либо к отдельному аппаратному компоненту сети. Брандмауэр защищает ресурсы частной сети от несанкционированного доступа пользователей из других сетей. Работая в тесной связи с программным обеспечением маршрутизатора, брандмауэр исследует каждый сетевой пакет, чтобы определить, следует ли направлять

его получателю. Использование брандмауэра можно сравнить с работой сотрудника, который отвечает за то, чтобы только разрешенные данные поступали в сеть и выходили из нее. На рис. 2.18 показан брандмауэр Cisco PIX серии 535, представляющий собой специальное выделенное устройство для защиты сети.

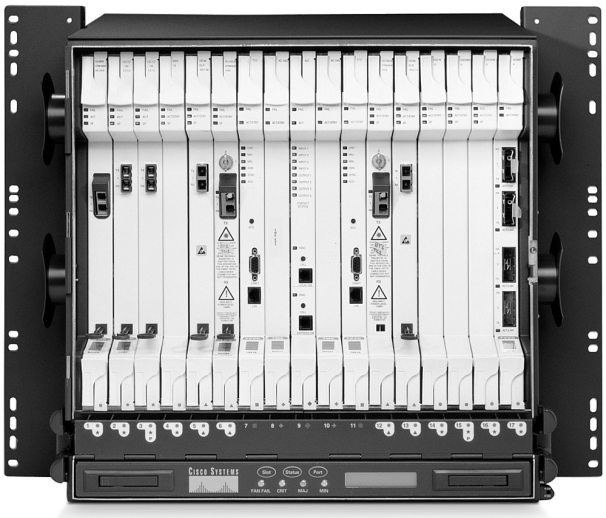


Рис. 2.17. Оптическая сетевая система Cisco ONS 15454 DWDM

Рис. 2.18. Брандмауэр Cisco PIX

Серверы AAA

Сервером AAA (AAA server) называется программа, которая обрабатывает запросы пользователя на доступ к компьютерным и сетевым ресурсам. Служба AAA обеспечивает для сети предприятия службы аутентификации, авторизации и учета. AAA-сервер гарантирует, что в сеть могут войти только пользователи, имеющие право доступа (служба аутентификации), что пользователи получают доступ только к тем ресурсам, которые им требуются (служба авторизации), а также записывает в журнал все действия пользователя после того, как ему разрешен вход в сеть (служба учета). Действия AAA-сервера аналогичны работе системы кредитных карт. Для того чтобы отнести какие-либо расходы на счет соответствующий кредитной карты, продавец должен сначала убедиться в том, что кредитная карта действительно принадлежит лицу, ее использующему (аутентификация). Он должен также проверить, что на счету имеется сумма, достаточная для оплаты покупки (авторизация), и после этого должен занести расходы на счет пользователя (учет). На рис. 2.19 приведен пример использования AAA-сервера.

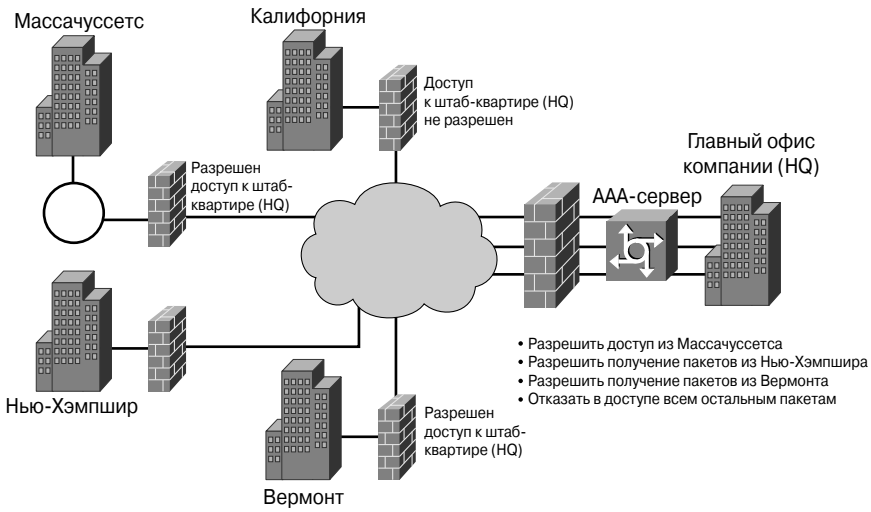


Рис. 2.19. AAA-сервер

Концентраторы виртуальных сетей VPN

Концентратор виртуальной частной сети (Virtual Private Network — VPN) обеспечивает удаленный доступ и связь между собой рабочих станций VPN-сети, простой в использовании интерфейс управления сетью и работу клиента VPN-сети. Серия концентраторов VPN-сетей Cisco 3000 представляет собой семейство специализированных VPN-платформ удаленного доступа и соответствующее программное обеспечение клиента, которые обеспечивают высокий уровень доступности, производительности и масштабируемости, а также самые современные способы шифрования и аутентификации, доступные на настоящий момент. На рис. 2.20 показан концентратор VPN-сети Cisco 3000.

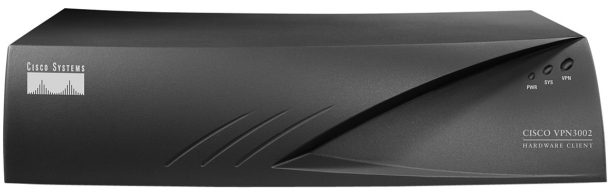


Рис. 2.20. Концентратор VPN-сети Cisco 3000

Беспроводные устройства

Беспроводная локальная сеть (Wireless LAN — WLAN) обеспечивает выполнение всех функций и сохранение всех преимуществ традиционных технологий локальных сетей LAN, таких, как Ethernet, без ограничений на длину провода или кабеля. Типичными устройствами беспроводной локальной сети являются беспроводные сетевые адаптеры NIC, беспроводные точки доступа и беспроводные мосты. Эти сетевые устройства кратко описаны в следующих разделах.

Беспроводные сетевые адаптеры

Каждому пользователю беспроводной сети требуется беспроводной сетевой адаптер NIC, называемый также адаптером клиента. Эти адаптеры доступны в виде плат PCMCIA или карт стандарта шины PCI и обеспечивают беспроводные соединения как для компактных переносных

компьютеров, так и для настольных рабочих станций. Переносные или компактные компьютеры PC с беспроводными адаптерами NIC могут свободно перемещаться в территориальной сети, поддерживая при этом непрерывную связь с сетью. Беспроводные адаптеры для шин PCI (Peripheral Component Interconnect — 32-разрядная системная шина для подключения периферийных устройств) и ISA (Industry-Standard Architecture — структура, соответствующая промышленному стандарту) для настольных рабочих станций позволяют добавлять к локальной сети LAN конечные станции легко, быстро и без особых материальных затрат. При этом не требуется прокладки дополнительных кабелей. Все адаптеры имеют антенну: карты PCMCIA обычно выпускаются со встроенной антенной, а PCI-карты комплектуются внешней антенной. Эти антенны обеспечивают зону приема, необходимую для передачи и приема данных. На рис. 2.21 показаны различные типы беспроводных адаптеров.

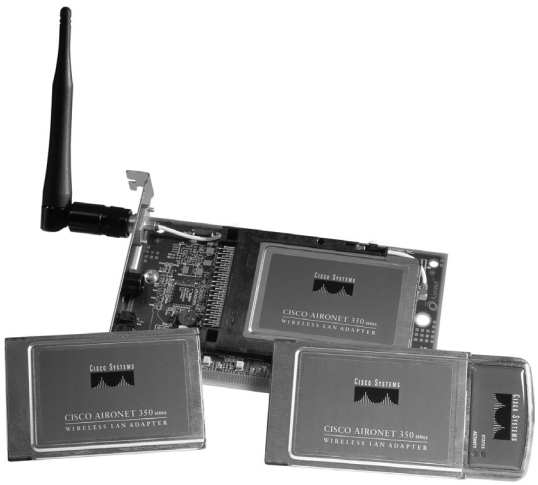


Рис. 2.21. Беспроводные адаптеры

Точки беспроводного доступа

Точка доступа (Access Point — AP), называемая также базовой станцией (рис. 2.22), представляет собой беспроводной приемопередатчик локальной сети LAN, который выполняет функции концентратора, т.е. центральной точки отдельной беспроводной сети, или функции моста — точки соединения проводной и беспроводной сетей. Использование нескольких точек AP позволяет обеспечить выполнение функций роуминга (roaming), что предоставляет пользователям беспроводного доступа свободный доступ в пределах некоторой области, поддерживая при этом непрерывную связь с сетью.

Беспроводные мосты

Беспроводной мост (рис. 2.23) обеспечивает высокоскоростные (11 Мбит/с) беспроводные соединения большой дальности в пределах видимости[5] (до 25 миль) между сетями Ethernet. В беспроводных сетях Cisco любая точка доступа может быть использована в качестве повторителя (точки расширения).

[5] *Здесь подразумевается видимость в радиотехническом понимании — зона покрытия антенны. — Прим. ред.*

Рис. 2.22. Точка беспроводного доступа

Рис. 2.23. Беспроводной мост

Презентация: концентратор Cisco 1503 Micro Hub.
В этой презентации показан внешний вид и особенности устройства Cisco 1503 Micro Hub.

Презентация: коммутатор Cisco Catalyst 1924.
В этой презентации показан внешний вид и особенности одного из наиболее распространенных коммутаторов рабочих групп корпорации Cisco.

Презентация: маршрутизатор Cisco 2621.
В этой презентации показан внешний вид и особенности маршрутизатора Cisco 2162.

Сетевые топологии

Сетевая топология определяет способ соединения в одну сеть таких устройств, как компьютеры, принтеры и другие. Иными словами, сетевая топология описывает расположение кабелей и устройств, а также маршруты, служащие для передачи данных. Топология сети в значительной степени определяет характер ее работы.

Сети имеют как физическую, так и логическую топологии. Термин *физическая топология* относится к физическому расположению устройств и соединениям передающей среды. Типичными физическими топологиями являются:

- шинная топология;
- кольцевая топология;
- звездообразная топология;
- расширенная звездообразная топология;
- иерархическая топология;
- полносвязная топология.

На рис. 2.24 проиллюстрированы различные физические топологии.

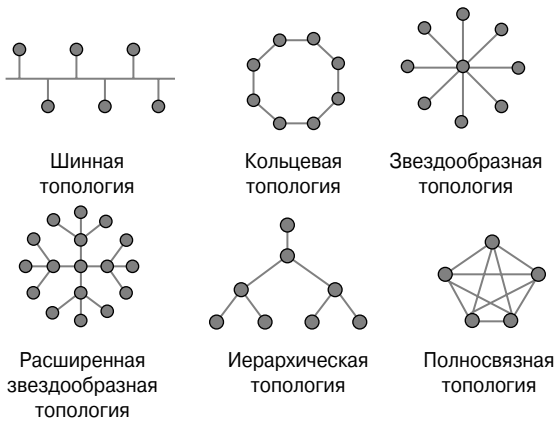


Рис. 2.24. Различные физические топологии

Логическая топология определяет, каким образом рабочие станции получают доступ к передающей среде для отправки данных. В следующих разделах описываются различные типы физических и логических топологий. На рис. 2.25 показаны несколько сетей с различными топологиями, которые соединены с разными традиционными сетевыми устройствами. На этом рисунке изображена сеть средней сложности, типичная для школы или малого предприятия.

В следующих разделах различные сетевые топологии рассматриваются более подробно.

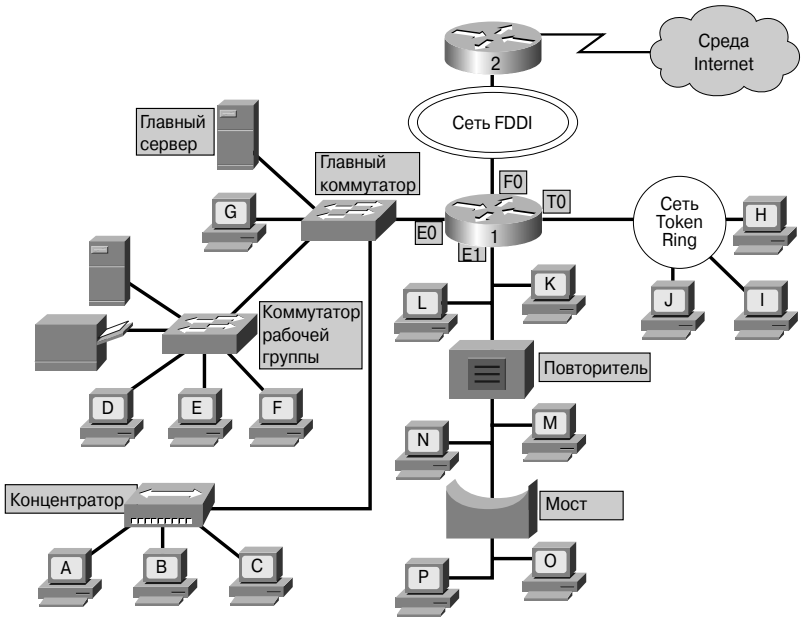


Рис. 2.25. Сетевые топологии

Шинная топология

Обычно называемая линейной шиной (linear bus) *шинная топология* (*bus topology*) подразумевает соединение всех устройств одним кабелем (рис. 2.26). Этот кабель проходит от одного компьютера к другому, подобно городскому автобусу, который движется от одной остановки к другой[6].

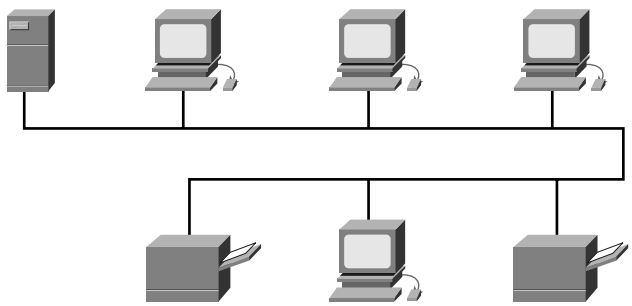


Рис. 2.26. Шинная топология

[6] *Эта аналогия объясняет английское название топологии* — bus topology — *шутливо дословно переводимое как* автобусная топология. — *Прим. пер.*

При использовании шинной топологии главный кабель сегмента должен заканчиваться специальным терминатором, который поглощает сигнал, когда последний достигает конца линии. Если бы терминатор отсутствовал, то представляющий данные электрический сигнал, отразившись на конце кабеля, вызвал бы наложение сигналов и ошибки в сети.

Звездообразная и расширенная звездообразная топологии

Звездообразная топология (star topology), показанная на рис. 2.27, представляет собой наиболее часто используемый тип сетевой топологии как в локальных Ethernet-структурах, так и в распределенных. После создания такой топологии сеть напоминает колесо велосипеда с расходящимися от оси спицами. Звездообразная топология состоит из центральной соединительной точки, которая может быть таким устройством, как концентратор, коммутатор или маршрутизатор, и расходящихся от нее сегментов кабелей.

Хотя звездообразная топология обходится дороже, чем физическая шинная топология, ее преимущества вполне оправдывают дополнительные затраты. Поскольку каждая рабочая станция подсоединена к центральному устройству отдельным кабелем, то при возникновении проблем с одним из таких кабелей сеть останется работоспособной. Такое свойство звездообразной топологии особенно важно, и этим объясняется тот факт, что практически все новые локальные сети LAN Ethernet имеют физическую звездообразную топологию. Центральная соединительная точка является усовершенствованием физической структуры сети из соображений безопасности или ограничения доступа, но вместе с тем она же является и основным уязвимым местом звездообразной топологии. Если выходит из строя центральное устройство, то вся сеть становится неработоспособной.

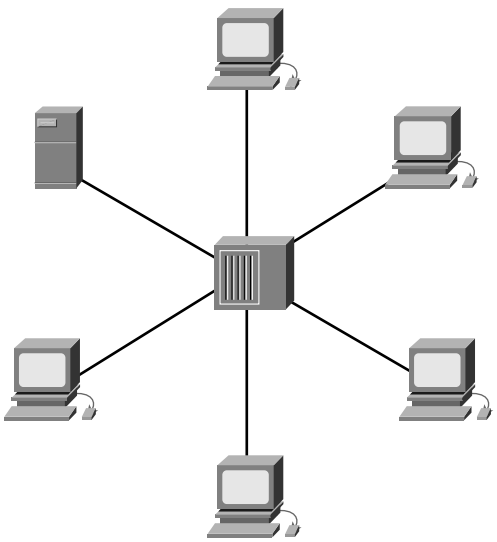


Рис. 2.27. Звездообразная топология

Если сеть со звездообразной топологией расширяется для включения дополнительных сетевых устройств, подсоединенных к главному сетевому устройству (центральной точке), то полученную топологию называют *расширенной звездообразной топологией (extended-star topology)*. Такая сеть показана на рис. 2.28.

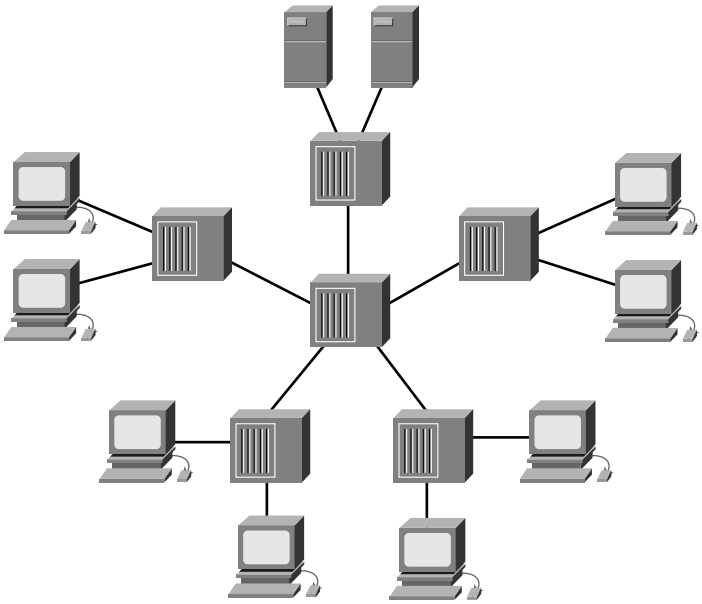


Рис. 2.28. Расширенная звездообразная топология

Звездообразная и расширенная звездообразная топологии подробно рассмотрены в следующих главах.

Кольцевая топология

Другой важной разновидностью топологии локальных сетей является *кольцевая топология (ring topology)*. Как видно из названия, в этой топологии рабочие станции соединены между собой так, что образуют непрерывное кольцо. В отличие от физической шинной топологии, сеть с кольцевой топологией не имеет начала и конца и не требует наличия терминатора. Способ передачи данных по сети с кольцевой топологией значительно отличается от того, который применяется в сети с шинной топологией. В такой сети специальный фрейм перемещается по кольцу, останавливаясь на каждом узле. Если какому-либо узлу требуется передать данные, то он может вставить в этот фрейм свои данные и адрес получателя. После этого фрейм перемещается по кольцу до тех пор, пока не дойдет до узла с адресом получателя, который извлекает данные из этого фрейма. Преимуществом такого способа передачи данных является невозможность коллизий.

Существуют два типа кольцевых топологий:

- одиночное кольцо;
- двойное кольцо.

В топологии одиночного кольца, показанной на рис. 2.29, все устройства сети вместе используют один кабель, а данные перемещаются только в одном направлении. Каждое устройство ожидает своей очереди для передачи данных по сети. Большинство сетей с топологией одиночного кольца в действительности имеют физические соединения, соответствующие звездообразной топологии.

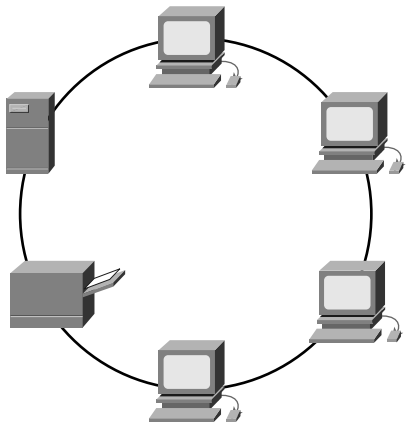


Рис. 2.29. Кольцевая топология

В сетях с топологией двойного кольца наличие двух колец позволяет посылать данные в обоих направлениях, как показано на рис. 2.30. Такая топология обеспечивает в сети избыточность, т.е. возможность в случае выхода из строя одного из кабелей передавать данные по другому кольцу. Еще одним преимуществом двойного кольца является возможность "сворачивания" (wrap) кольца, т.е. восстановления его работоспособности в случае обрыва.

Иерархическая топология

Иерархическая топология (hierarchical topology) создается аналогично расширенной звездообразной топологии. Основным отличием является отсутствие в такой сети центрального узла. Вместо этого используется магистральный узел (trunk node), от которого отходят ветви (branches) к другим узлам, как показано на рис. 2.31. Существуют два типа иерархической (древовидной) топологии: бинарное дерево — от каждого узла отходят два соединения; и магистральное дерево — магистральный узел имеет узлы-ветви, от которых отходят каналы к рабочим станциям.

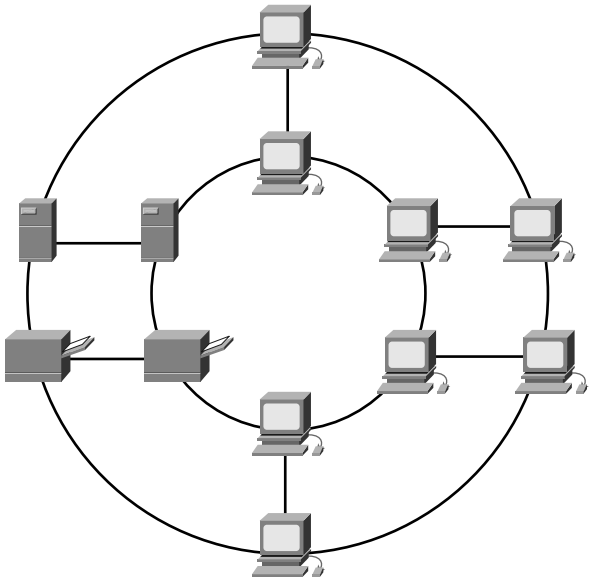


Рис. 2.30. Топология двойного кольца

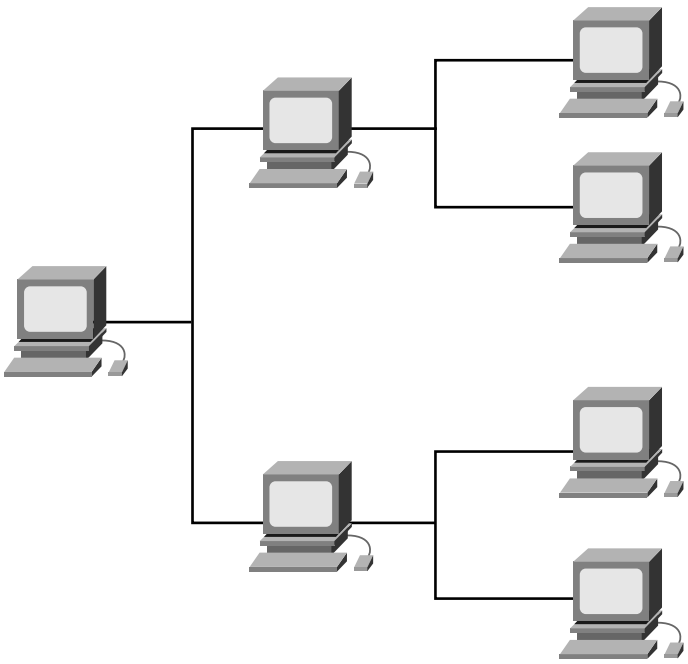


Рис. 2.31. Иерархическая топология

Полно- и неполносвязная топологии

В сети с *полносвязной топологией (full-mesh topology)* все устройства (узлы) соединены друг с другом, что обеспечивает избыточность (а в итоге — резервирование) и устойчивость к сбоям, как показано на рис. 2.32. Такое расположение кабелей сети имеет очевидные достоинства и недостатки. Достоинством такой структуры является то, что каждый узел физически соединен со всеми остальными, что обеспечивает высокую степень избыточности. Если какой-либо канал выходит из строя, то существует много других маршрутов, позволяющих передать данные в требуемый пункт назначения. Очевидным недостатком такой сети является то, что, за исключением случая очень небольшого количества узлов в сети, количество соединений становится чрезвычайно большим. В результате этого реализация сети, в которой используется полносвязная топология, становится крайне дорогостоящей и трудно реализуемой. Полносвязная топология обычно используется лишь в соединениях между собой маршрутизаторов распределенных сетей WAN.

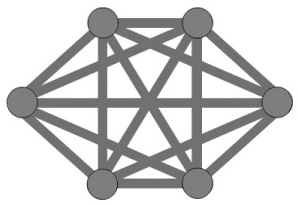


Рис. 2.32. Полносвязная топология

В сети с *неполносвязной топологией (partial-mesh topology)* (иногда называемой частично связной) по крайней мере одно устройство поддерживает несколько соединений с другими устройствами; при этом, однако, полносвязная топология не создается. Пример такой сети приведен на рис.2.33. Неполносвязная топология все же создает определенную степень избыточности за счет наличия нескольких альтернативных маршрутов. Если какой-либо из них не может быть использован, данные отправляются по другому маршруту, хотя он может оказаться и более протяженным. Неполносвязная топология используется во многих телекоммуникационных магистралях, а также в глобальной сети Internet.

Логическая топология сетей

Под логической топологией сети понимается способ коммуникации рабочих станций в сетевой передающей среде. Двумя основными типами логической топологии являются широковещательная топология и топология, использующая передачу маркера.

Использование широковещательной топологии означает всего лишь то, что каждая рабочая станция направляет по сетевой среде свои данные на конкретный адаптер NIC по адресу многоадресатной рассылки или по широковещательному адресу. Порядок передачи по сети данных отдельными станциями при этом не устанавливается. Как гласит известная поговорка, “первым пришел — первым обслужили”

(First come, first served). Далее мы покажем, что по такому же принципу работают все сети Ethernet.

Вторым типом логической топологии является топология с передачей маркера. Передача маркера управляет доступом к сети путем последовательного предоставления электронного маркера всем рабочим станциям. Когда станция получает маркер, она может отправить в сеть свои данные. Если у станции нет данных для передачи, она передает маркер другой, следующей за ней, станции, и процесс повторяется. Двумя примерами сетей, использующих передачу маркера, являются сети Token Ring и FDDI, которые могут рассматриваться как пример реализации технологии передачи маркера по сети с физической кольцевой топологией.

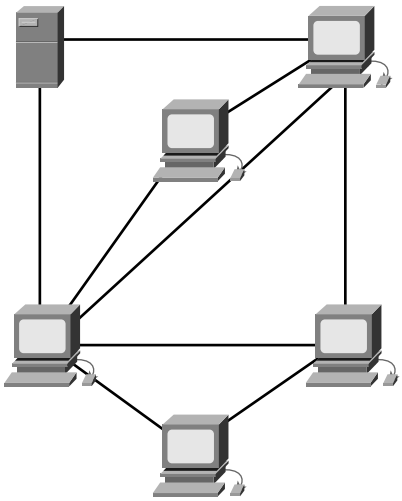


Рис.2.33. Неполносвязная топология

Сетевые протоколы

Стек протоколов — это набор протоколов, который позволяет одной рабочей станции осуществлять связь по сети с другой станцией. Под *протоколом* понимается формальное описание набора правил и соглашений, управляющих отдельными аспектами коммуникации устройств в сети. Протоколы определяют формат, синхронизацию, последовательность передачи данных и контроль ошибок. При отсутствии протоколов компьютер не смог бы создать или восстановить поток входящих битов от другого компьютера и преобразовать их в первоначальные данные.

Протоколы управляют всеми аспектами передачи данных. Они определяют способ физического построения сети, способы подсоединения к ней компьютеров, форматирование данных для передачи и сам метод их передачи. Правила работы в сети и протоколы разрабатываются и поддерживаются рядом организаций и комитетов:

- Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers — IEEE);

- Национальным институтом стандартизации США (American National Standards Institute — ANSI);
- Ассоциацией промышленности средств связи (Telecommunications Industry Association — TIA);
- Ассоциацией электронной промышленности (Electronic Industries Alliance — EIA);
- Международным союзом телекоммуникаций (International Telecommunications Union — ITU), ранее известным как Международный консультативный комитет по телеграфии и телефонии (Consultative Committee for International Telephone and Telegraphy — CCITT).

Локальные сети

Локальная сеть (Local-Area Network — LAN) состоит из компьютеров, сетевых адаптеров (network interface cards), периферийных устройств, среды передачи данных по сети и других сетевых устройств. На рис. 2.34 проиллюстрирована локальная сеть LAN.

Локальные сети позволяют компаниям применять различные компьютерные технологии для эффективного совместного использования файлов и принтеров, а также предоставляют возможность внутренней связи с помощью сообщений электронной почты. В локальной сети логически и физически объединены данные, локальная связь и вычислительное оборудование.

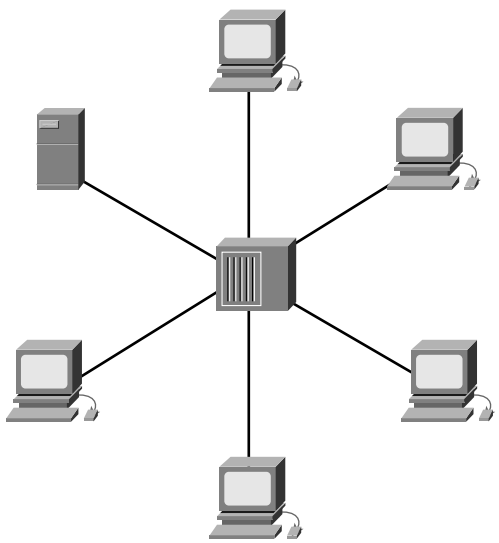


Рис. 2.34. Локальная сеть (LAN)

Локальная сеть создается для того, чтобы:

- функционировать в ограниченной географической области;
- обеспечить доступ многих пользователей к передающей среде с широкой полосой пропускания;
- обеспечить постоянную доступность удаленных ресурсов, подсоединенных к локальным службам;
- обеспечить физическое соединение смежных сетевых устройств.

Типичными технологиями локальных сетей являются следующие:

- Ethernet;
- Token Ring;
- FDDI.

Распределенные сети

Распределенные сети (Wide-Area Networks — WAN) соединяют между собой локальные сети LAN, что позволяет компьютерам LAN-сетей получать доступ к компьютерам и файловым серверам, находящимся в других локальных сетях. Поскольку WAN-сети соединяют пользователей, расположенных в обширной географической области, они делают возможным для предприятий осуществление связи на больших расстояниях (рис. 2.35).

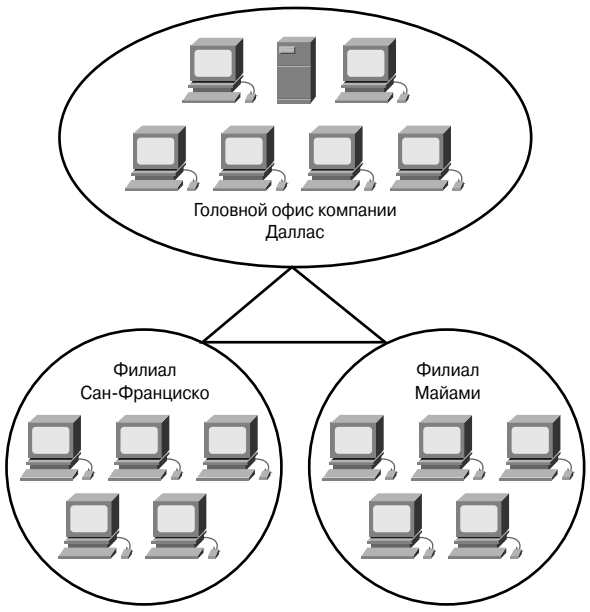


Рис. 2.35. Распределенная сеть (WAN)

Использование технологий распределенной сети позволяет компьютерам, принтерам и другим устройствам локальной сети LAN обмениваться данными с удаленными локальными сетями. Сети WAN обеспечивают практически мгновенную связь в пределах обширной географической области. Такая возможность посылать мгновенные сообщения (Instant Message — IM) любому адресату в любой точке земного шара обеспечивает пользователям те же возможности связи, какие имеются у пользователей, находящихся в одном офисе. Программное обеспечение для совместной работы в сети предоставляет доступ в реальном времени к информации и ресурсам, что дает возможность пользователям виртуально "встречаться" на большом расстоянии друг от друга. Создание распределенных сетей привело к появлению нового типа сотрудников — *телеработников (telecommuters)*, которые могут работать, вообще не покидая своего дома.

Распределенные сети WAN предназначены для выполнения следующих функций:

- осуществления связи в больших, географически разделенных областях;
- предоставления пользователям возможности коммуникации в реальном времени с другими пользователями;
- непрерывного обеспечения доступа к удаленным ресурсам через соединения с локальными службами;
- обеспечения службы электронной почты, World Wide Web, передачи файлов и средств электронной коммерции в сети Internet.

Типовые технологии распределенных сетей включают в себя:

- соединения через модемы;
- цифровую сеть с комплексным обслуживанием (Integrated Services Digital Network — ISDN);
- цифровые абонентские каналы (Digital Subscriber Line — DSL);
- технологию, основанную на использовании протокола Frame Relay;
- линии носителей T-типа (США) и E-типа (Европа) — T1, E1, T3, E3 и т.д.;
- синхронную оптическую сеть (Synchronous Optical Network — SONET) — синхронный транспортный сигнал 1-го уровня (STS-1) (оптический носитель [OC]-1), STS-3 (OC-3) и т.д.

Дополнительная информация: современные домашние сетевые приложения

В настоящее время многие люди превращают свое место проживания в Internet-дом, подключая свой домашний компьютер к локальной сети Ethernet. Такие пользователи интегрируют свои компьютеры с домашним телефоном, системой безопасности, с телевизором и видеослужбами, с отоплением и кондиционированием, с освещением и другими электронными компонентами для того, чтобы иметь возможность управлять ими с помощью щелчка мышью или даже голосовыми командами.

Провайдеры служб создали сотовые и спутниковые сети, которые предоставляют весьма сложные службы, такие, например, как беспроводной доступ к среде Internet. Местные телефонные компании (Local Exchange Carrier — LEC) реализуют высокоскоростные службы

передачи данных, такие, как подключение по линиям DSL с оплатой, приемлемой для домашних пользователей. Многие операторы кабельной связи в дополнение к кабельному телевидению в настоящее время предоставляют высокоскоростной доступ к сети Internet, который может совместно использоваться несколькими объединенными в сеть домашними компьютерами. Аппаратное и программное обеспечение корпорации Cisco поддерживает самые современные беспроводные и кабельные технологии, а также цифровые абонентские каналы DSL.

Пользователи также объединяют возможности персональных компьютеров, телефона и факса, что позволяет реализовать функции автоответчика, обеспечить хранение поступивших сообщений и их восстановление при помощи компьютера. Кроме того, телефонная связь через сеть Internet, которая основана на средах передачи данных и обеспечивает передачу голосовых данных по протоколу IP (Voice over IP — VoIP), позволяет пользователям полностью отказаться от использования телефонных линий и осуществлять междугородные переговоры путем соединения с сетью Internet по кабелю, по беспроводной связи и через другие среды передачи, и таким образом значительно экономить деньги.

Региональные сети

Под региональной или городской сетью (Metropolitan-Area Network — MAN) понимается сеть, охватывающая территорию крупного города, включая пригородные зоны. Сети MAN соединяют между собой локальные сети LAN, находящиеся на определенном расстоянии друг от друга, но в одной общей географической области, как показано на рис. 2.36. Например, MAN-сеть может использоваться банком, имеющим в городе несколько отделений. Обычно провайдер службы соединяет между собой две или более LAN-сетей, используя свои частные линии коммуникаций или оптические службы. MAN-сеть также может быть создана с использованием беспроводной мостовой технологии путем передачи сигналов через открытые телекоммуникационные инфраструктуры. Широкая полоса пропускания, предоставляемая доступными в настоящее время оптическими каналами, делает MAN-сети более функциональным и экономически доступным средством, чем раньше. MAN-сети отличаются от LAN- и WAN-сетей следующими функциями:

- MAN-сети соединяют друг с другом пользователей, находящихся в географической зоне или области большей, чем область LAN-сети, но меньшей, чем WAN-сети;
- MAN-сети соединяют сети города в одну сеть большего размера (которая может также обеспечивать эффективное соединение с WAN-сетью);
- MAN-сети также используются для соединения между собой нескольких локальных сетей LAN путем создания мостовых соединений через магистральные линии.

Дополнительная информация: специализированные сети, размещаемые внутри локальных сетей

Бывают случаи, когда необходимо разместить внутри локальной сети LAN специализированную сеть меньшего размера. Чаще всего такие специализированные сети используются для организации доступа к системам хранения данных, а также к системам и устройствам центров обработки данных. В число таких специализированных сетей также входят Intranet-сети и Extranet-сети, а также виртуальные частные сети VPN. В этом разделе описываются различные типы таких специализированных сетей.

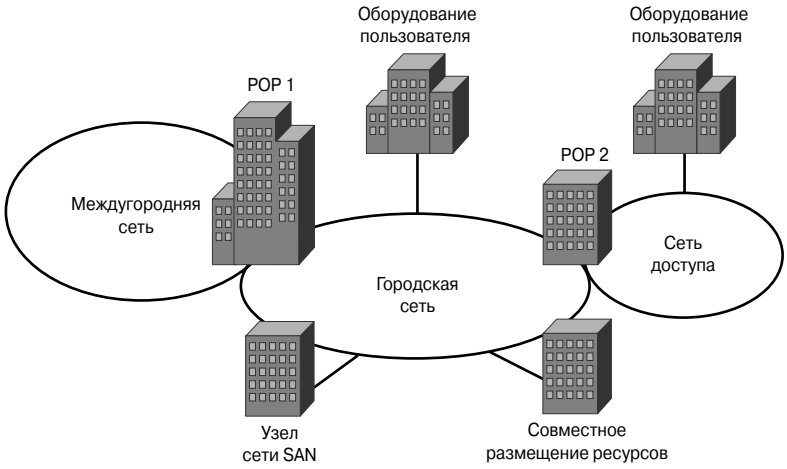


Рис. 2.36. Сеть масштаба города

Сети хранилищ данных

Сетями хранилищ данных (Storage-Area Network — SAN) называются специализированные выделенные высокоскоростные сети, которые перемещают данные между серверами и хранилищами ресурсов. Поскольку они являются отдельными выделенными сетями, конфликтов между потоками данных от серверов и их клиентов не возникает (рис. 2.37). SAN-технология позволяет осуществлять высокоскоростные соединения типа "сервер-хранилище", "хранилище-хранилище" и "сервер-сервер". При таком подходе используется отдельная сетевая инфраструктура, что устраняет все проблемы, связанные с наличием уже установленных в сети соединений. SAN-технология обеспечивает выполнение перечисленных ниже функций.

- **Высокая производительность при передаче данных**. SAN-сети позволяют осуществлять на конкурентной основе доступ к дисковым и ленточным накопителям двум и более серверам с высокой скоростью, что повышает эффективность работы сети.
- **Доступность**. SAN-сети обладают большей внутренней устойчивостью к стихийным бедствиям, поскольку при использовании технологии SAN данные могут быть продублированы на расстояниях вплоть до 10 км[7].
- **Масштабируемость**. Как и сети LAN/WAN, сети хранилищ SAN могут использовать различные технологии. Это позволяет легко переносить операции резервирования данных, перемещения файлов и дублирования данных из одной системы в другую.

[7] *6,2 мили. — Прим. пер.*

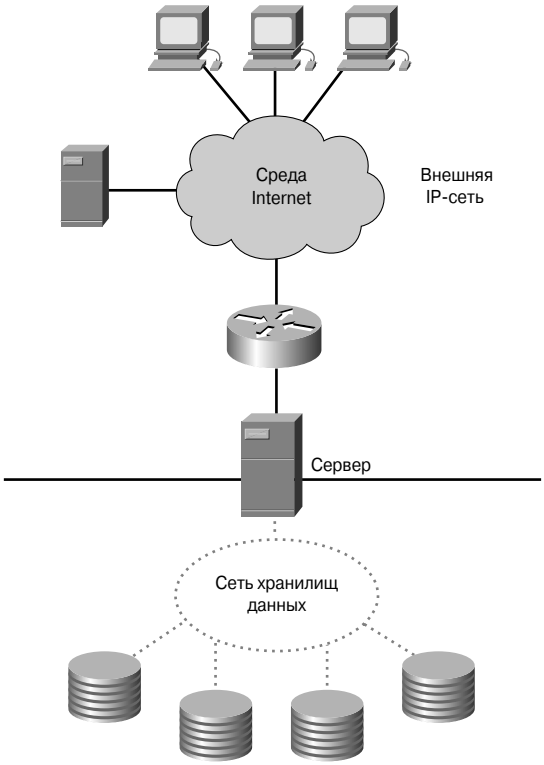


Рис. 2.37. Сеть хранилищ данных

Дополнительная информация: технологии центров обработки данных

Как показано на рис. 2.38, *центр обработки данных (data center)* представляет собой глобально координируемую сеть, состоящую из устройств, предназначенных для ускорения доставки информации по инфраструктуре Internet. Используя преимущества служб базовой IP-сети предприятия, провайдеры служб могут ускорить доставку и улучшить использование разнообразной информации, такой, как широкополосное потоковое видео. Структура с использованием центра обработки данных повышает производительность сети и избавляет от необходимости передавать потоковое видео по инфраструктуре локальной сети.

Центр обработки данных исключает потенциальные источники переполнения в сети путем распределения нагрузки между несколькими устройствами сбора и обработки информации, расположенными близко к получателям информации и данных.
Разнообразная Web- и мультимедиаинформация копируется в устройства–хранилища, а для пользователей создаются маршруты к оптимально расположенным устройствам.

Например, при загрузке видеофильма от Internet-провайдера (Internet Service Provider — ISP) вместо того, чтобы часами ожидать окончания загрузки соответствующего большого файла, тот же фильм может быть загружен за несколько минут, если Internet-провайдер использует технологию центров хранения или обработки данных, поскольку последний может значительно ускорить доставку информации.

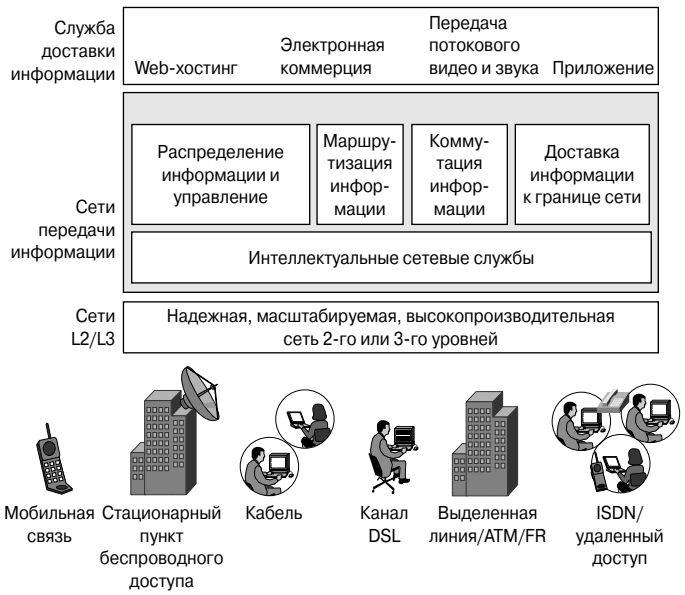


Рис. 2.38. Центр обработки данных

Виртуальные частные сети

Виртуальной частной сетью (Virtual Private Network — VPN) называется частная сеть, которая создается в инфраструктуре открытой сети, такой, например, как глобальная сеть Internet. Используя VPN-сеть, телеработник может получить доступ к сети головного офиса компании через сеть Internet путем создания безопасного туннеля между компьютером телеработника и VPN-маршрутизатором в головном офисе.

Аппаратное и программное обеспечение корпорации Cisco поддерживает самые современные VPN-технологии. Виртуальная частная сеть представляет собой службу, предоставляющую безопасное и надежное соединение через совместно используемую инфраструктуру открытой сети, такой, как Internet. В сетях VPN обеспечиваются такой же уровень безопасности и такие же политики управления, как и в обычной частной сети. Они представляют собой наиболее экономичный способ создания соединения типа "точка-точка" между удаленными пользователями и сетью предприятия.

Существуют три типа VPN-сетей, они показаны на рис. 2.39.

- *VPN-сети доступа (Access VPN)* обеспечивают удаленный доступ мобильным сотрудникам и малым/домашним офисам (Small Office/Home Office — SOHO) к внутренней или внешней сети (Intranet или Extranet) головного офиса по совместно используемой инфраструктуре. VPN-сети доступа используют аналоговый удаленный доступ, технологии ISDN, DSL, протокол мобильных IP-соединений и кабельные технологии для создания безопасных соединений

между сотрудниками головного офиса, телеработниками и филиалами компании.

- *VPN-сети Intranet (внутренние виртуальные частные сети)* связывают между собой региональные и удаленные офисы с головным офисом компании в совместно используемую инфраструктуру с помощью выделенных линий. Внутренние VPN-сети (Intranet) отличаются от внешних VPN-сетей (Extranet) тем, что они разрешают доступ только сотрудникам компании.
- *VPN-сети Extranet (внешние виртуальные частные сети)* соединяют коммерческих партнеров компании с сетью головного офиса через совместно используемую инфраструктуру с помощью выделенных линий. Внешние VPN-сети (Extranet) отличаются от внутренних VPN-сетей (Intranet) тем, что они разрешают доступ некоторым пользователям, не являющимся сотрудниками компании.

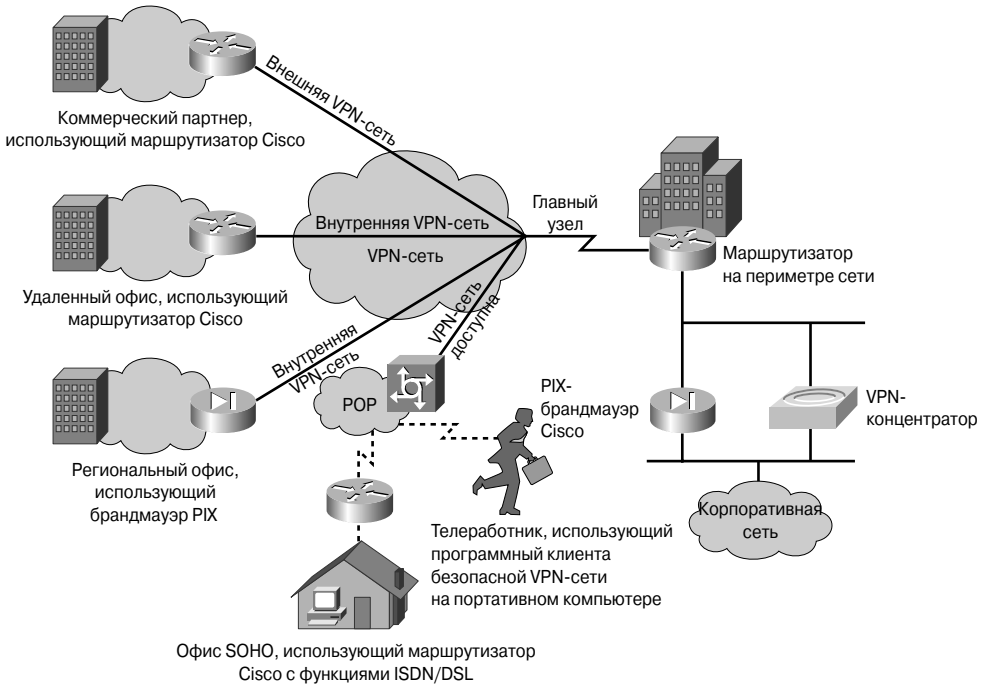


Рис. 2.39. Технологии VPN-сетей

VPN-сети обладают следующими преимуществами:

- единая VPN-технология обеспечивает конфиденциальность нескольким приложениям протокола TCP/IP. Это особенно важно в ситуациях, когда требуется обеспечить безопасный доступ партнерам или телеработникам;

- службы шифрования могут быть обеспечены всем соединениям TCP/IP между авторизованным пользователем и VPN-сервером. Преимуществом такого подхода является его прозрачность для конечного пользователя. Поскольку включен режим шифрования, сервер может повысить уровень шифрования;
- VPN-сети обеспечивают мобильность сотрудникам компании и позволяют им получать безопасный доступ к корпоративной сети.

Внутренние и внешние сети предприятия

Одной из типичных конфигураций LAN-сетей является *сеть Intranet* (*внутренняя сеть*). Web-серверы внутренней сети (Intranet) отличаются от открытых Web-серверов тем, что посторонние лица не имеют доступа к Intranet-сети организации без соответствующего разрешения и пароля. Внутренние сети (Intranet) спроектированы таким образом, что доступ к ним может быть получен только пользователем, имеющим право привилегированного доступа к внутренней локальной сети организации. Во внутренних сетях Web-серверы находятся внутри сети, а использование браузера является основным средством получения доступа к финансовым данным, а также к графическим и текстовым данным, хранящимся на этих серверах.

Сетью *Extranet (внешняя сеть*) называют внутреннюю сеть (Intranet), частичный доступ к которой имеют и авторизованные внешние пользователи. В то время как внутренняя сеть (Intranet) находится за брандмауэром и доступна только сотрудникам компании или организации, сеть Extranet обеспечивает различные уровни доступа для посторонних внешних пользователей. Пользователь может получить доступ к внешней сети (Extranet) только в том случае, если у него есть зарегистрированные в этой сети имя и пароль; идентификационные данные пользователя определяют уровень разрешенного ему доступа и доступные для просмотра области внешней сети (Extranet). Внешние сети (Extranet) помогают расширить сферу действия приложений и служб, которые базируются на Intranet-сети предприятия, но используют расширенный безопасный доступ ко внешним пользователям и предприятиям. Такой доступ обычно осуществляется с помощью паролей, идентификаторов (ID) пользователей и других средств обеспечения безопасности на уровне приложений. Соответственно, внешнюю сеть (Extranet) можно рассматривать как расширение стратегий двух или более внутренних сетей (Intranet) с безопасным взаимодействием участвующих предприятий и их соответствующих внутренних сетей (Intranet). Внешние сети (Extranet) поддерживают управление доступом ко внутренним сетям (Intranet) отдельных предприятий. Как правило, они используются для поддержки соединений потребителей, поставщиков, коммерческих партнеров и сообществ по интересам с корпоративной внутренней сетью (Intranet) по совместно используемой инфраструктуре с использованием выделенных линий. На рис. 2.40 показаны внешняя и внутренняя сети (Intranet и Extranet).

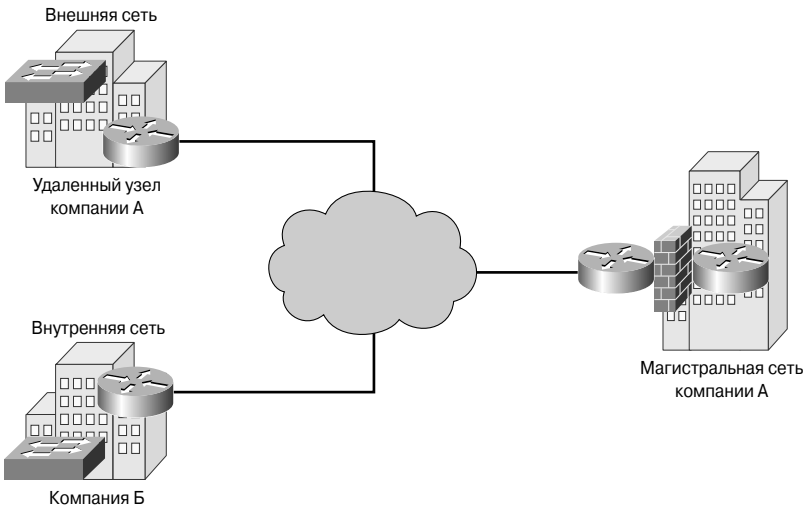


Рис. 2.40. Сети Intranet и Extranet

Полоса пропускания

Технологии локальных сетей LAN и распределенных сетей WAN всегда имели одну общую черту — для описания их возможностей применялся и применяется термин *ширина полосы пропускания* (часто для краткости просто *полоса пропускания* — *bandwidth*). Этот термин является весьма существенным для специалиста, который работает с компьютерными сетями, однако сначала он может показаться трудным для понимания. В последующих разделах подробно описан смысл этого понятия. Целесообразно сначала рассмотреть простые термины, перед тем как перейти к более сложным вопросам, связанным с работой сетей.

Важность ширины полосы пропускания

Полоса пропускания (bandwidth) определяется как объем информации, который может быть передан по сетевому соединению за определенный период времени. Такое определение может показаться простым, однако требуется глубокое понимание его смысла перед изучением других связанных с сетями вопросов. Почему так важна полоса пропускания?

- **Ширина полосы пропускания конечна**. Независимо от типа среды передачи, используемой для построения сети, существуют пределы, ограничивающие возможность сети передавать информацию. Полоса пропускания ограничена как физическими законами, так и технологиями, используемыми для передачи информации в сетевой среде. Например, полоса пропускания обычного модема ограничена скоростью около 56 Кбит/с, что определяется как физическими свойствами телефонных проводов типа витой пары, так и технологией аналогового модема для голосовых линий. Технология цифровых абонентских

каналов DSL также использует телефонные провода типа витой пары, однако каналы DSL обеспечивают значительно бо́льшую полосу пропускания, чем обычные модемы. Диапазон частот (полоса пропускания), используемый в технологии DSL, значительно шире, чем диапазон частот голосовых данных (используемый модемом обычной телефонной сети). Этим объясняется то, что по каналу DSL можно передавать большее количество битов в секунду. Оптоволоконный кабель обладает физическим потенциалом для создания практически неограниченной полосы пропускания. Однако потенциальная полоса пропускания оптоволоконного кабеля не может быть полностью реализована до тех пор, пока не будут разработаны технологии, позволяющие это сделать.

- **Полоса пропускания не бесплатна**. Для локальной сети LAN можно постепенно закупать дополнительное оборудование, которое с течением времени обеспечит практически неограниченную полосу пропускания. Для WAN-соединений полосу пропускания практически всегда требуется арендовать у провайдера службы. В любом случае понимание сущности полосы пропускания и изменений потребности организации в полосе пропускания может обеспечить значительную экономию средств как отдельному пользователю, так и коммерческому предприятию. Сетевому менеджеру требуется принимать оптимальные решения относительно закупаемого оборудования и подписки на сетевые службы провайдеров.
- **Ширина полосы пропускания является ключевым фактором при анализе эффективности работы сети, при проектировании новой сети и для понимания работы сети Internet**. Сетевой профессионал должен понимать огромное влияние ширины полосы пропускания на производительность сети и на проектирование телекоммуникационной инфраструктуры. Информационные потоки можно рассматривать как строку битов, перемещающихся от одного компьютера к другому по всем миру. В сети Internet перемещаются триллионы триллионов битов, представляющих огромное количество информации, перетекающей из одной точки земного шара в другую за считанные секунды. В определенном смысле можно сказать, что сеть Internet — это полоса пропускания.
- **Потребность в полосе пропускания постоянно возрастает**. Как только появляются новые сетевые технологии и инфраструктуры, предоставляющие бо́льшую ширину полосы пропускания, создаются новые приложения, которые используют ее преимущества. Передача по сети разнообразной медиа-информации, включая потоковое видео- и аудио-, требует огромной ширины полосы пропускания. В настоящее время вместо традиционных телефонных систем часто устанавливаются системы IP-телефонии, что дополнительно увеличивает потребность в полосе пропускания. Успешный сетевой профессионал должен уметь предсказать потребность в увеличенной полосе пропускания и планировать свои действия соответствующим образом.

Аналогии для описания полосы пропускания цифрового канала

Концепция передачи (“перетекания”) информационных потоков позволяет привести две наглядные аналогии, помогающие лучше представить себе роль полосы пропускания в работе сети. Поскольку в разговоре о перекачке воды и движении автотранспорта также говорят о *потоках*, рассмотрим приведенные ниже иллюстрации.

- **Ширину полосы пропускания можно сравнить с диаметром трубы, используемой при перекачке воды (рис. 2.41).** Приведенная на рисунке водопроводная сеть образована трубами различного диаметра. Главный водопровод города может использовать трубы диаметром до 2 метров, в то время как труба кухонного крана может иметь диаметр всего лишь 2 сантиметра. Диаметр трубы определяет возможности трубы при перекачке воды. Таким образом, воду можно сравнить с передаваемыми данными, а диаметр трубы играет такую же роль, как и полоса пропускания. Многие сетевые эксперты говорят, что им нужно “расширить трубу” (“put in bigger pipes”), когда им требуется увеличить возможности сети по передаче данных.

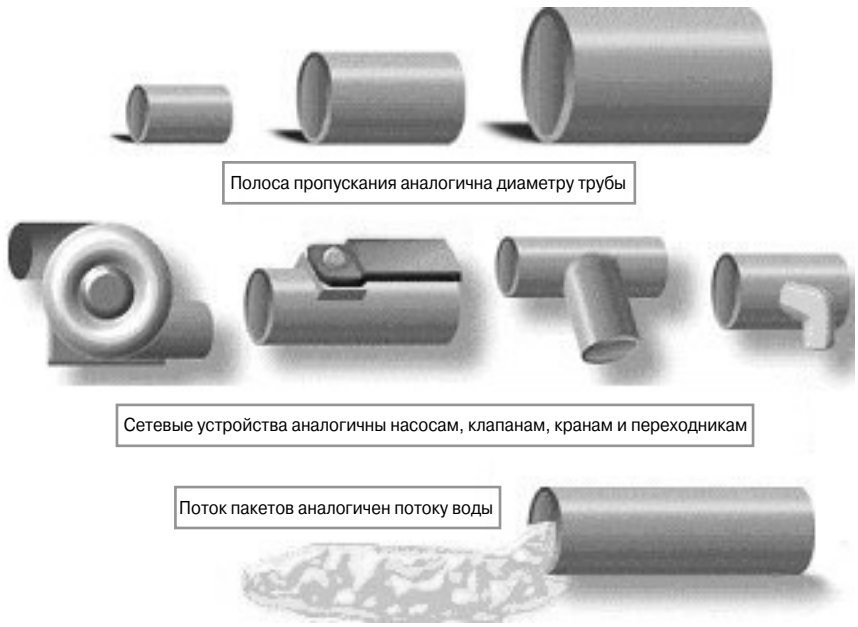


Рис. 2.41. Сравнение полосы пропускания с водопроводной трубой

- **Ширину полосы пропускания можно сравнить с количеством полос на автотрассе (рис. 2.42)**. Каждый город имеет целую сеть автомобильных дорог. В широкие автотрассы (хайвэи — highways) вливаются дороги меньшего масштаба, имеющие

меньшее количество полос. Эти дороги ведут к еще меньшим и более узким дорогам, заканчиваясь в конечном итоге подъездами к домам и офисам. Когда на дороге меньше автомобилей, каждый из них имеет бо́льшую свободу для передвижения и маневров. По мере того как поток машин увеличивается, каждая из них движется все медленнее, особенно на дорогах, на которых меньше полос для движения. В конечном итоге, по мере того как число машин на трассе увеличивается, даже дороги с большим количеством полос становятся перегруженными, и движение на них замедляется. Сеть данных ведет себя во многом аналогично транспортной системе; при этом пакеты играют роль автомобилей, а полоса пропускания сходна с количеством полос на дороге. Рассматривая сеть данных как систему дорог, легко понять, как соединения с узкой полосой пропускания могут вызвать переполнение в сети (иногда называемое затором).

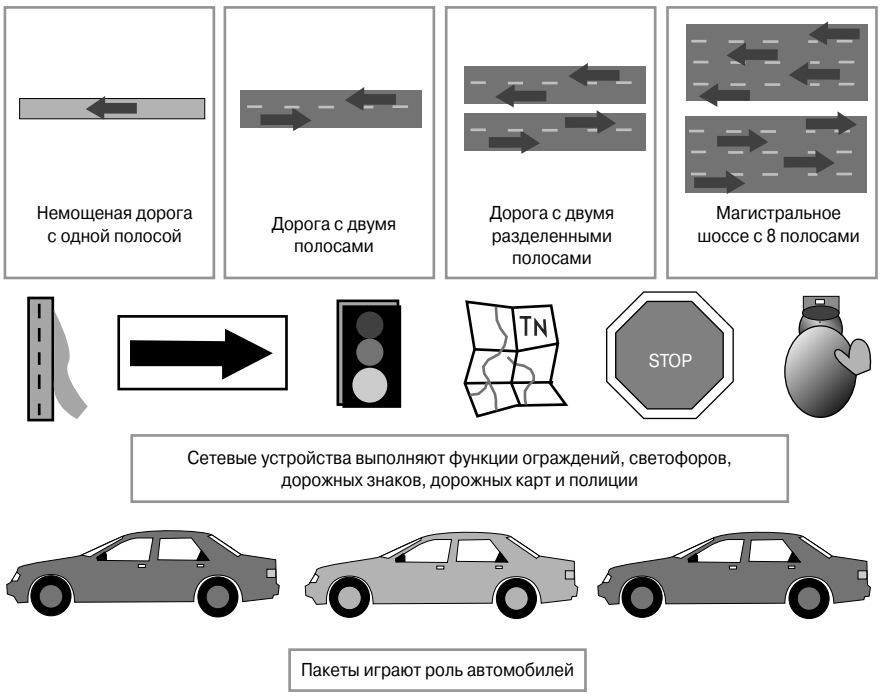


Рис. 2.42. Транспортная аналогия полосы пропускания сети

Следует учитывать, что действительным значением полосы пропускания в данном контексте является максимальное количество битов, которое теоретически может пройти по определенной зоне или области сети за некоторый промежуток времени при конкретных условиях. Приведенные выше аналогии использованы лишь для того, чтобы читателю было легче понять значение термина “ширина полосы пропускания”.

Измерение цифровой полосы пропускания

В цифровых системах базовой единицей при измерении полосы пропускания является количество битов в секунду. Полоса пропускания является мерой того, какой объем информации или какое количество битов может быть передано из одной точки сети в другую за определенный промежуток времени, выражаемый в секундах. Хотя ширина полосы пропускания может быть выражена непосредственно в битах в секунду, обычно используются более крупные единицы. Иными словами, ширина полосы пропускания обычно описывается в тысячах битов в секунду, миллионах битов в секунду или даже миллиардах.

Хотя термины *ширина полосы пропускания* и *скорость передачи* часто употребляются как синонимы, их смысл не полностью совпадает. Например, можно сказать, что линия T3 с полосой пропускания 45 Мбит/с работает с большей скоростью, чем линия T1 с полосой 1,544 Мбит/с. Однако если используется лишь небольшая часть потенциальной способности канала по передаче данных, то эти каналы передают данные примерно с одинаковой скоростью, подобно тому, как небольшое количество воды будет протекать через широкую трубу с такой же скоростью, как и через узкую. Поэтому будет более точным сказать, что соединение T3 имеет бо́льшую ширину полосы пропускания, чем линия T1.

В табл. 2.2 приведены различные единицы измерения полосы пропускания.

Таблица 2.2. Единицы измерения ширины полосы пропускания

Единица измерения ширины полосы пропускания	Аббревиатура	Эквивалент в битах в секунду
Битов в секунду	бит/с	1 бит/с — базовая единица измерения ширины полосы пропускания
Килобитов в секунду	Кбит/с	1 Кбит/с = 1000 бит/с = 10^3 бит/с
Мегабитов в секунду	Мбит/с	1 Мбит/с = 1 000 000 бит/с = 10^6 бит/с
Гигабитов в секунду	Гбит/с	1 Гбит/с = 1 000 000 000 бит/с = 10^9 бит/с

Ограничения полосы пропускания

Доступная ширина полосы пропускания зависит как от типа используемой среды передачи, так и от технологии локальной сети LAN или распределенной сети WAN. Некоторые различия объясняются физическими свойствами среды передачи. Физические различия среды при прохождении сигнала по витой паре из медного провода, по коаксиальному кабелю, по оптоволоконному кабелю или даже в атмосфере приводят к фундаментальным ограничениям на передающую способность конкретной среды передачи. Однако реальная пропускная способность сети определяется комбинацией свойств физической среды и технологией, выбранной для передачи и обнаружения сетевых сигналов. Например, при современном уровне понимания физических процессов, происходящих в кабеле медной витой пары (Unshielded Twisted-Pair — UTP), устанавливается теоретический предел ширины полосы пропускания, равный 1 Гбит/с, однако на практике ширина полосы пропускания определяется

конкретной используемой технологией, такой, как 10BASE-T, 100BASE-TX или 1000BASE-TX Ethernet. Полоса пропускания также определяется другими изменяющимися факторами, такими, как количество пользователей в сети, используемое оборудование, характер приложений, объем широковещания и т.д. Иными словами, реальная полоса пропускания определяется, как правило, не ограничениями передающей среды, а методами сигнализации, типом сетевых адаптеров NIC и другими компонентами используемого сетевого оборудования.

В табл. 2.3 перечислены некоторые типовые передающие среды, а также их ограничения на максимальную дальность передачи и на ширину полосы пропускания.

Таблица 2.3. Максимальная полоса пропускания и ограничения на дальность передачи

Среда передачи	Максимальная ширина полосы пропускания (Мбит/с)	Максимальное физическое расстояние (м)
Коаксиальный кабель 50 Ом (10BASE2 Ethernet, Thinnet)	10	185
Коаксиальный кабель 50 Ом (10BASE5 Ethernet, Thicknet)	10	500
Витая пара UTP 5-й категории (10BASE-T Ethernet)	10	100
Витая пара UTP 5-й категории (100BASE-TX Ethernet)	100	100
Витая пара UTP 5-й категории (1000BASE-TX Ethernet)	1000	100
Многомодовый оптоволоконный кабель (62.5/125 мкм) (100BASE-FX Ethernet)	100	2000
Многомодовый оптоволоконный кабель (62.5/125 мкм) (1000BASE-SX Ethernet)	1000	220
Многомодовый оптоволоконный кабель (50/125 мкм) (1000BASE-SX Ethernet)	1000	550
Одномодовый оптоволоконный кабель (9/125 мкм) (1000BASE-LX Ethernet)	1000	5000

В табл. 2.4 описаны типовые службы распределенных сетей WAN и их полосы пропускания.

Таблица 2.4. Службы распределенных сетей WAN и соответствующие полосы пропускания

Служба WAN-сети	Типичный потребитель	Ширина полосы пропускания
Модемное соединение	Индивидуальные пользователи	56 Кбит/с = 0,056 Мбит/с
DSL	Индивидуальные пользователи, телеработники, малые предприятия	От 12 Кбит/с до 6,1 Мбит/с = от 0,128 Кбит/с до 6,1 Мбит/с
ISDN	Телеработники, малые предприятия	128 Кбит/с = 0,128 Мбит/с
Frame Relay	Небольшие учреждения (школы) и средние предприятия	От 56 Кбит/с до 44,736 Мбит/с (США) или 34,368 Мбит/с (Европа) = 0,056 Мбит/с до 44,736 Мбит/с (США) до 34,368 Мбит/с (Европа)
Линия T1	Более крупные учреждения и предприятия	1,544 Мбит/с
Линия T3	Более крупные учреждения и предприятия	44,736 Мбит/с
Канал STS-1 (OC-1)	Телефонные компании, магистрали телекоммуникационных компаний	51,840 Мбит/с
Канал STS-3 (OC-3)	Телефонные компании, магистрали телекоммуникационных компаний	155,251 Мбит/с
Канал STS-48 (OC-48)	Телефонные компании, магистрали телекоммуникационных компаний	2,488 Гбит/с

Пропускная способность сети передачи данных

Полоса пропускания является мерой объема информации, которая может быть передана по сети за определенный период времени. Поэтому величина доступной полосы пропускания является критически важной характеристикой сетевой спецификации.

Типичная сеть LAN может быть спроектирована и реализована таким образом, чтобы каждая рабочая станция получала полосу пропускания 100 Мбит/с, однако это не означает, что каждый пользователь действительно сможет за одну секунду передавать данные объемом 100 Мбит/с. Такое может быть только в идеальной ситуации. Понятие пропускной способности сети объясняет, почему так происходит.

Под *пропускной способностью* (throughput) понимается реальная полоса пропускания, измеренная в определенное время рабочего дня с использованием специальных Internet-маршрутов во время передачи по сети специального набора данных. К сожалению, по многим причинам пропускная способность сети часто оказывается

значительно меньшей, чем максимально возможная цифровая полоса пропускания используемой передающей среды. Вот факторы, определяющие реальную полосу пропускания или пропускную способность сети:

- наличие в сети других устройств;
- тип передаваемых данных;
- топология сети;
- количество пользователей в сети;
- характеристики компьютера пользователя;
- характеристики компьютера, выполняющего функции сервера;
- характеристики используемого источника питания;
- возможность переполнения.

Вместе с тем теоретически возможная полоса пропускания является важным фактором, который необходимо учитывать при проектировании сети, поскольку полоса пропускания сети никогда не может выйти за пределы ограничений, налагаемых выбранной передающей средой и используемой сетевой технологией. На рис. 2.43 приведен список некоторых переменных величин, оказывающих влияние на пропускную способность сети. Проектировщику сети и сетевому администратору столь же важно учитывать факторы, которые могут повлиять на реальную пропускную способность сети. Регулярно измеряя пропускную способность сети, сетевой администратор может постоянно иметь точную картину изменений производительности сети и потребности пользователей сети. В этом случае сеть может быть соответствующим образом откорректирована.

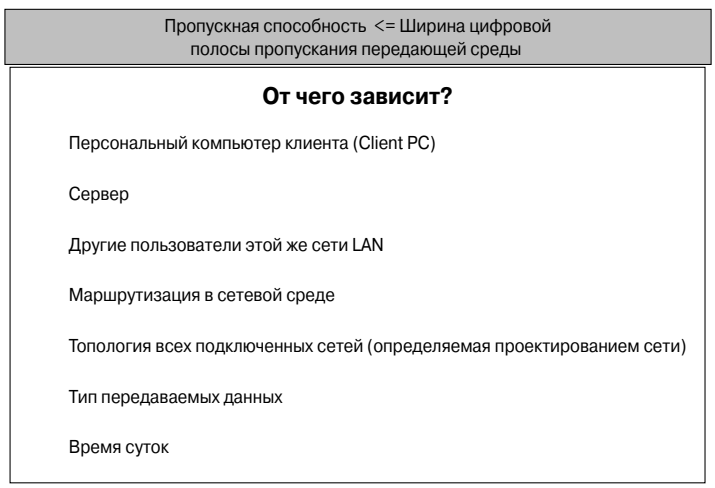


Рис. 2.43. Факторы, влияющие на пропускную способность

Расчет скорости передачи данных

Сетевых проектировщиков и администраторов часто приглашают для того, чтобы принять решение, касающееся полосы пропускания в конкретной сети. Следует ли увеличивать полосу пропускания WAN-соединения для того, чтобы подключиться к новой базе данных? Достаточна ли полоса пропускания магистрали LAN для работы с программой обучения в режиме реального времени? Ответить на эти вопросы не всегда легко, но исходной точкой может служить простой расчет скорости передачи данных.

Используя формулу T = S/BW (время передачи = размер файла /ширина полосы-пропускания), сетевой администратор может оценить некоторые важные параметры, влияющие на производительность сети. Если типичный для данного приложения размер файла известен, то, разделив размер файла на ширину полосы пропускания, можно получить оценку кратчайшего времени, за которое может быть принят или передан такой файл.

При расчетах производительности необходимо учесть два важных аспекта:

- результат вычисления представляет собой лишь предварительную оценку, поскольку в размер файла не включен объем служебных данных, которые буду добавлены в процессе подготовки к передаче данных по сети. Этот процесс называется инкапсуляцией. Инкапсуляция более подробно рассмотрена в следующих разделах;
- результат, вероятно, будет оценкой лишь для самого благоприятного случая, поскольку доступная полоса пропускания почти никогда не достигает максимального для данного конкретного типа сети значения (более точная оценка можно получить, если в приведенное выше уравнение подставить значение пропускной способности сети).

Хотя вычисление времени передачи данных согласно указанному выше уравнению достаточно просто, результат может оказаться неверным, если в этом вычислении будут использованы разные единицы измерения. Иными словами, если полоса пропускания измерена в Мбит/с, то размер файла также должен быть выражен в мегабитах (Мбит), а не в мегабайтах (Мбайт). Поскольку размер файла обычно выражается в мегабайтах, для преобразования в мегабиты необходимо умножить его на 8.

Попытайтесь, используя формулу T = S/BW, ответить на следующий вопрос (следует внимательно следить за единицами измерения и при необходимости преобразовать их): “Потребует ли передача содержимого полностью заполненной дискеты (гибкого диска объемом 1,44 Мбайта) по каналу ISDN меньше времени, чем передача содержимого полностью заполненного жесткого диска объемом 10 Гбайтов по каналу OC-48?”

На рис. 2.44 показана простая формула для вычисления времени передачи файла.

Типичное время загрузки T=S/P	Типичное время загрузки T=S/P
BW =	Максимальная (теоретически возможная) полоса пропускания “самого медленного канала” между рабочими станциями отправителя и получателя (в битах в секунду)
P =	Реальная пропускная способность в момент передачи (в битах в секунду)
T =	Время передачи файла (в битах в секунду)
S =	Размер файла в битах

Рис. 2.44. Расчет времени передачи файла

Сравнение цифровой и аналоговой полос пропускания

До недавнего времени радио-, теле- и телефонные сигналы передавались по воздушной среде или по проводам с использованием электромагнитных волн. Эти волны называются *аналоговыми*, поскольку они имеют ту же форму, что и световые и звуковые волны, генерируемые передатчиками. При изменении амплитуды и формы световых и звуковых сигналов электрические сигналы, переносящие информацию, изменяются пропорционально. Иными словами, электромагнитные волны *аналогичны* световым и звуковым волнам.

Ширина аналоговой полосы пропускания зависит от ширины диапазона электромагнитного спектра, занимаемого каждым сигналом. Базовой единицей измерения аналоговой полосы пропускания является герц (Гц — Hz), или количество циклов сигнала в секунду. Чаще для аналоговой полосы пропускания, как и для цифровой, используются более крупные единицы. Обычными единицами измерения являются килогерц (кГц), мегагерц (мГц) и гигагерц (гГц). Последние две единицы широко используются для описания полосы пропускания мобильных и беспроводных телефонов (как правило, работающих в диапазоне от 900 мГц до 2,4 гГц). Беспроводные сети спецификаций 802.11a и 802.11b в основном работают на частотах 5 гГц и 2,4 гГц.

Хотя аналоговые сигналы могут переносить различные виды информации, они обладают серьезными недостатками по сравнению с цифровой передачей. При использовании цифровых сигналов аналоговый видеосигнал, требующий для передачи широкого диапазона частот, не может быть сжат до узкой полосы. Следовательно, если обеспечить необходимую ширину полосы пропускания не удается, передача сигнала оказывается невозможной. То же относится и к цифровой полосе пропускания, однако в цифровом варианте такая недостаточность полосы пропускания случается гораздо реже, поскольку полоса пропускания в этом случае значительно шире. При использовании цифровой сигнализации вся информация посылается в виде битов, независимо от ее типа.

При подготовке к передаче по цифровой среде голосовые, видео и обычные данные превращаются в потоки битов, что дает цифровой технологии значительные

преимущества по сравнению с аналоговой. По цифровому каналу с очень узкой полосой пропускания могут быть переданы практически неограниченные объемы информации, хотя это может потребовать значительного времени. Переданную цифровую информацию после ее поступления в пункт назначения можно просмотреть, прослушать, прочитать или преобразовать в ее первоначальную форму.

Необходимо отчетливо понимать общие черты и различия между цифровой и аналоговой полосами пропускания. Оба типа полосы пропускания постоянно встречаются в информационных технологиях. Однако поскольку в настоящем курсе в основном рассматриваются цифровые сети, в дальнейшем под *полосой пропускания (bandwidth)* мы будем понимать цифровую полосу пропускания.

Сетевые модели

Изучить вопросы, связанные с функционированием сетей, легче, если начать с изучения первичных понятий и теоретических положений, а затем перейти к конкретным аспектам реализации сети. Читателю, который хочет стать сетевым профессионалом, необходимо изучить основные теоретические положения, перед тем как приступить к проектированию, построению и поддержке сети. Изучение принципов работы сети на разных уровнях поможет понять, что происходит при передаче информации с одного компьютера на другой. В данном разделе описана концепция использования уровней для понимания работы сети и показано, как она применяется в коммуникационных моделях. В нем описаны две конкретные модели сети — OSI и TCP/IP, а также одноранговая связь и инкапсуляция.

Использование уровней для анализа проблем передачи данных

Концепция использования уровней для анализа работы сети помогает лучше понять, что происходит при передаче информации от одного компьютера другому. Приведенные ниже вопросы касаются перемещения некоторых объектов, таких, например, как потоки автомобилей или потоки данных в электронном виде.

- Что такое поток?
- Каковы различные формы объектов, перемещающихся в виде потока?
- Что управляет потоком?
- Где происходит перемещение потоков?

Перемещение многих однотипных объектов, физических или логических, называется *потоком* (*flow*). Использование уровней помогает описать детали этого процесса. Примерами систем, в которых перемещаются потоки объектов, могут служить городская система водоснабжения, автострады и движение автомобилей по дорогам, почтовая система и телефонная сеть.

Рассмотрим данные, приведенные в табл. 2.5. Какие сети при этом исследуются? Какие объекты перемещаются в виде потока? Каковы различные формы этих перемещающихся объектов? Каковы правила управления потоком? Где происходит

перемещение потоков? Приведенные в таблице ситуации аналогичны перемещению данных по компьютерной сети и позволят читателю лучше понять ее функционирование.

Таблица 2.5. Сравнение принципа работы сети с другими примерами перемещения объектов в виде потоков

Сеть	Что перемещается	Различные формы	Правила	Где
Водопровод	Вода	Горячая, холодная, питьевая вода, сточные воды/канализация	Правила использования труб: необходимо закрывать краны, периодически их прочищать, нельзя допускать попадания в трубы посторонних предметов	Водопроводные трубы
Сеть автодорог	Средства передвижения	Грузовые, легковые, велосипеды	Дорожные правила и общепринятые меры вежливости	Дороги и автотрассы
Почтовая служба	Почтовые отправления	Письма (информация в письменном виде), посылки и бандероли	Правила упаковки и указания адреса получателя	Почтовые ящики, почтовые отделения, машины для перевозки почты, почтовые самолеты и сотрудники, доставляющие почту
Телефонная сеть	Голосовая информация	Разговорный язык	Правила вызова абонента и общепринятые нормы вежливости	Провода телефонной сети, электромагнитны е волны и т.д.

Процесс сетевой коммуникации достаточно сложен. Данные, передаваемые в форме электронных сигналов, должны пройти по передающей среде к требуемому компьютеру-получателю и вновь быть преобразованы в первоначальную форму для прочтения их получателем. Этот процесс включает в себя несколько этапов, поэтому наиболее эффективным способом реализовать сетевую коммуникацию является разделение процесса на различные уровни. В таком случае каждый уровень выполняет свои конкретные задачи независимо от других.

В следующих разделах показано, как с помощью многоуровневой модели сети процесс сетевой коммуникации подразделяется на отдельные уровни. Также описан процесс пересылки данных по сети и достижения ими пункта назначения. По мере

изучения процесса коммуникации в сети важно понять его различные этапы, компоненты и используемые протоколы. Такое понимание даст читателю информацию, необходимую для устранения ошибок в сети в том случае, если в реализации сетевого проекта возникнут трудности.

Использование уровней для описания процесса обмена данными в сети

Трудность реализации сетевого проекта состоит в том, что это достаточно сложный процесс. Он становится особенно трудным, если смотреть на него как на единое целое. Решение этой проблемы состоит в разделении всей системы сетевой коммуникации на ряд уровней. При этом каждый уровень отвечает за определенную часть процесса коммуникации и взаимодействует только с уровнем, находящимся непосредственно под ним, и с уровнем над ним. Такое взаимодействие строго определяет назначение каждого уровня. Двумя основными сетевыми моделями, использующими уровни, являются эталонная модель взаимодействия открытых систем (Open System Interconnection — OSI) и сетевая модель протоколов TCP/IP.

ВНИМАНИЕ!

На первый взгляд может показаться, что запомнить названия и функции уровней очень сложно. По мере дальнейшего изучения материала как первого, так и второго тома данной книги, вы будете все больше и больше узнавать об устройствах, которые работают на разных уровнях обеих обсуждаемых моделей. В следующих главах основные функции каждого уровня, применимые к ним технологии и отличия между уровнями эталонной модели взаимодействия открытых систем (OSI) неоднократно будут обсуждаться. Если после прочтения текущего раздела концепции модели OSI и всех ее семи уровней не совсем четко ясны, не стоит надолго задерживаться на этой теме, поскольку многие вопросы прояснятся по ходу чтения остальных глав.

Эталонная модель OSI

Начальная стадия развития сетей LAN, MAN и WAN имела во многих отношениях хаотический характер. В начале 80-х годов XX века резко увеличились размеры сетей и их количество. По мере того как компании осознавали, что, используя сетевые технологии, они могут сэкономить значительные средства и повысить эффективность своей работы, они создавали новые сети и расширяли уже существовавшие с той же быстротой, с какой появлялись новые сетевые технологии и новое оборудование.

Однако к середине 80-х годов эти же компании стали испытывать трудности с расширением уже существующих сетей. Сетям, использовавшим различные спецификации и реализованным различными способами, стало все труднее осуществлять связь друг с другом. Компании, оказавшиеся в такой ситуации, первыми осознали, что необходимо отходить от использования *фирменных (proprietary)* сетевых систем. Под фирменными системами понимаются сети, которые разрабатывались каждой компанией отдельно, принадлежали только ей и управлялись только этой компанией.

В компьютерной сфере понятие фирменной системы является противоположностью понятию открытой системы. Если система является фирменной, то это означает, что использованием данной технологии управляет только одна компания или группа компаний. Наоборот, открытость системы означает, что получить доступ к ней и к соответствующим стандартам может любой желающий.

Для решения проблемы несовместимости сетей и их неспособности осуществлять связь друг с другом международная организация по стандартизации (International Organization for Standardization — ISO) разработала различные сетевые схемы, такие, как DECnet, системная сетевая архитектура (Systems Network Architecture — SNA) и стек протоколов TCP/IP. Целью создания таких схем была разработка некоторого общего для всех пользователей набора правил работы сетей. В результате этих исследований организация ISO разработала сетевую модель, которая смогла помочь производителям оборудования создавать сети, совместимые друг с другом и успешно взаимодействовавшие. Процесс подразделения сложной задачи сетевой коммуникации на отдельные более мелкие можно сравнить с процессом сборки автомобиля. Процесс проектирования, изготовления деталей и сборки автомобиля, если его рассматривать как единое целое, является весьма сложным. Маловероятно, что нашелся бы специалист, который смог бы решить все требуемые задачи при сборке автомобиля: собрать машину из случайным образом подобранных деталей или, скажем, при изготовлении конечного продукта непосредственно из железной руды. По этой причине проектированием автомобиля занимаются инженеры-проектировщики, инженеры-литейщики проектируют формы для литья деталей, а сборочные инженеры и техники занимаются сборкой узлов и автомобиля из готовых деталей.

Эталонная модель OSI (OSI reference model), обнародованная в 1984 году, была описательной схемой, созданной организацией ISO. Эта эталонная модель предоставила производителям оборудования набор стандартов, которые обеспечили бо́льшую совместимость и более эффективное взаимодействие различных сетевых технологий и оборудования, производимого многочисленными компаниями во всем мире.

Эталонная модель OSI является первичной моделью, используемой в качестве основы для сетевых коммуникаций.

Хотя существуют и другие модели, большинство производителей оборудования и программного обеспечения ориентируются на эталонную модель OSI, особенно когда желают обучить пользователей работе с их продуктами. Эталонная модель OSI в настоящее время считается наилучшим доступным средством обучения пользователей принципам работы сетей и механизмам отправки и получения данных по сети.

Эталонная модель OSI определяет сетевые функции, выполняемые каждым ее уровнем. Что еще более важно, она является базой для понимания того, как информация передается по сети. Кроме того, модель OSI описывает, каким образом информация или пакеты данных перемещается от программ-приложений (таких, как электронные таблицы или текстовые процессоры) по сетевой передающей среде (такой, как провода) к другим программам-приложениям, работающим на другом компьютере этой сети, даже если отправитель и получатель используют разные виды передающих сред.

Эталонная модель OSI содержит семь пронумерованных уровней, каждый из которых выполняет свои особые функции в сети.

- **Уровень 7 —** уровень приложений.
- **Уровень 6 —** уровень представления данных.
- **Уровень 5 —** сеансовый уровень.
- **Уровень 4 —** транспортный уровень.
- **Уровень 3 —** сетевой уровень.
- **Уровень 2 —** канальный уровень.
- **Уровень 1 —** физический уровень.

Такое разделение выполняемых сетью функций называется *делением на уровни*. Подразделение сети на семь уровней обеспечивает следующие преимущества:

- процесс сетевой коммуникации подразделяется на меньшие и более простые этапы;
- стандартизируются сетевые компоненты, что позволяет использовать и поддерживать в сети оборудование разных производителей;
- подразделение процесса обмена данными на уровни позволяет осуществлять связь между различными типами аппаратного и программного обеспечения;
- изменения на одном уровне не влияют на функционирование других уровней, что позволяет быстрее разрабатывать новые программные и аппаратные продукты;
- коммуникация в сети подразделяется на компоненты меньшего размера, что облегчает их изучение.

Рассматривая перемещение информации по различным уровням эталонной модели OSI, читатель сможет понять, каким образом пакеты данных перемещаются по сети и какие устройства работают на каждом уровне. В конечном итоге знание функций и особенностей уровней поможет устранять проблемы, если таковые возникнут при передаче данных по сети.

Интерактивная презентация. Преимущества модели OSI.
Данная интерактивная презентация, в которой необходимо выбрать преимущества эталонной модели взаимодействия открытых систем, поможет закрепить изученный материал.

Уровни эталонной модели OSI и их функции

Для передачи пакетов данных по сети от отправителя получателю каждый уровень модели OSI должен выполнить свой набор функций. В следующих разделах кратко описаны все уровни эталонной модели OSI.

Уровень 7: уровень приложений

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

Уровень 6: уровень представления данных

Задача *уровня представления данных (presentation layer*) состоит в том, чтобы информация уровня приложений, которую посылает одна система (отправитель), могла быть прочитана уровнем приложений другой системы (получателя). При необходимости уровень представления преобразует данные в один из многочисленных существующих форматов, который поддерживается обеими системами. Другой важной задачей этого уровня является шифрование и расшифровка данных. Типовыми графическими стандартами шестого уровня являются стандарты PICT, TIFF и JPEG. Примерами стандартов шестого уровня эталонной модели, описывающих формат представления звука и видео, являются стандарты MIDI и MPEG.

Уровень 5: сеансовый уровень

Как показывает само название этого уровня, *сеансовый уровень (session layer*) устанавливает сеанс связи между двумя рабочими станциями, управляет им и разрывает его. Сеансовый уровень предоставляет свои службы уровню представления данных. Он также синхронизирует диалог между уровнями представления двух систем и управляет обменом данными. Кроме своей основной постоянной функции — управления, уровень сеанса связи обеспечивает эффективную передачу данных, требуемый класс обслуживания и рассылку экстренных сообщений о наличии проблем на сеансовом уровне, уровне представления данных или уровне приложений. Примерами протоколов пятого уровня могут служить сетевая файловая система (Network File System — NFS), система X-Window и протокол сеанса AppleTalk (AppleTalk Session Protocol — ASP).

Уровень 4: транспортный уровень

Транспортный уровень (transport layer) сегментирует данные передающей станции и вновь собирает их в одно целое на принимающей стороне. Границу между транспортным уровнем и уровнем сеанса связи можно рассматривать как границу между протоколами приложений и протоколами передачи данных. В то время как уровни приложений, представления данных и сеанса связи занимаются аспектами коммуникаций, которые связаны с работой приложений, нижние четыре уровня решают

вопросы транспортировки данных по сети. Транспортный уровень пытается обеспечить службу передачи данных таким образом, чтобы скрыть от верхних уровней детали процесса передачи данных. В частности, задачей транспортного уровня является обеспечение надежности передачи данных между двумя рабочими станциями. При обеспечении службы связи транспортный уровень устанавливает, поддерживает и соответствующим образом ликвидирует виртуальные каналы. Для обеспечения надежности транспортной службы используются выявление ошибок при передаче и управление информационными потоками. Примерами протоколов четвертого уровня могут служить протокол управления передачей (Transmission Control Protocol — TCP), протокол пользовательских дейтаграмм (User Datagram Protocol — UDP) и протокол последовательного обмена пакетами (Sequenced Packet Exchange — SPX).

Уровень 3: сетевой уровень

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

Уровень 2: канальный уровень

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

Уровень 1: физический уровень

Физический уровень (*physical layer*) определяет электрические, процедурные и функциональные спецификации для активизации, поддержки и отключения физических каналов между конечными системами. Спецификациями физического уровня определяются уровни напряжений, синхронизация изменений напряжения, физическая скорость передачи данных, максимальная дальность передачи, физические соединения и другие аналогичные параметры.

Интерактивная презентация. Семь уровней эталонной модели.
В этой презентации необходимо совместить уровни модели OSI с соответствующими им функциями.

Одноранговая связь

Для того чтобы передать пакеты данных от отправителя получателю, необходимо, чтобы каждый уровень модели OSI станции-отправителя вступил в связь с аналогичным уровнем получателя. Такая форма коммуникации называется *одноранговой связью (peer-to-peer communication)*. Во время этого процесса протоколы одного и того же уровня обеих систем обмениваются информацией, называемой протокольными

единицами обмена (Protocol Data Unit — PDU). Каждый уровень коммуникации компьютера-отправителя создает соответствующий ему модуль PDU и вступает в связь с одноименным уровнем компьютера-получателя.

Рис. 2.45. Одноранговая связь

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

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

и единиц (в биты) для передачи по сетевой среде (обычно по медному проводу) на первом уровне.

Сетевые устройства, такие, как концентраторы, коммутаторы и маршрутизаторы, функционируют на трех нижних уровнях эталонной модели OSI. Концентраторы функционируют на первом уровне, коммутаторы — на втором, а маршрутизаторы — на третьем уровне модели OSI. Первым уровнем, который связан с процессом сквозной (end-to-end) передачи данных между конечными устройствами, является транспортный (четвертый).

Сетевая модель TCP/IP

Несмотря на то что эталонная модель OSI в настоящее время является общепризнанной, исторически и технически открытым стандартом сети Internet являются протокол управления передачей (Transmission Control Protocol — TCP) и Internet-протокол (IP), которые обычно рассматриваются как одно целое и обозначаются TCP/IP. Эталонная модель TCP/IP и стек протоколов TCP/IP позволяют организовать связь между двумя компьютерами, расположенными в любых точках земного шара, со скоростью, близкой к скорости света. Модель TCP/IP имеет также большое историческое значение, подобное тому, какое имели стандарты, которые привели к широчайшему распространению телефонной связи, электросетей, железных дорог, телевидения и видеозаписи.

Министерство обороны США (Department of Defence — DoD) создало почву для разработки эталонной модели TCP/IP, поскольку оно требовало, чтобы сеть продолжала функционировать в любых условиях, даже в случае ядерной войны. Для более наглядной иллюстрации представим себе мир, находящийся в состоянии ядерной войны, и пронизанный самыми разными типами соединений, включая проводные, микроволновые соединения, оптоволоконные кабели и спутниковую связь. Предположим далее, что требуется, чтобы информация и данные (в виде пакетов) надежно передавались по этой сети независимо от состояния любого конкретного узла этой сети или состояния другой сети (которая в данном случае может быть уничтожена в ходе военных действий). Министерство обороны требовало, чтобы в любых условиях его данные продолжали передаваться по сети между любыми точками. Эта весьма сложная задача проектирования устойчивой сети привела к созданию модели TCP/IP, которая с тех пор стала стандартом, на базе которого выросла глобальная сеть Internet. При изучении уровней модели TCP/IP следует помнить о первоначальных целях, которые ставились перед сетью Internet; это поможет понять некоторые, возможно, неясные аспекты проблемы.

Как показано на рис. 2.46, сетевая модель TCP/IP имеет четыре уровня:

- уровень приложений;
- транспортный уровень;
- Internet-уровень;
- уровень доступа к сети.

Модель OSI	Модель TCP/IP
Уровень приложений (7-й уровень)	Уровень приложений
Уровень представления данных (6-й уровень)	
Уровень сеанса связи (5-й уровень)	
Транспортный уровень (4-й уровень)	Транспортный уровень
Сетевой уровень (3-й уровень)	Уровень Internet
Канальный уровень (2-й уровень)	Уровень доступа к сети
Физический уровень (1-й уровень)	

Рис. 2.46. Сетевая модель TCP/IP

Необходимо отметить, что некоторые уровни модели TCP/IP имеют те же названия, что и у уровней эталонной модели OSI. Однако не следует отождествлять одноименные уровни этих двух моделей. Функции одноименных уровней обеих моделей могут совпадать, но могут и различаться.

Практическое задание. Эталонная модель OSI и модель TCP/IP
В этой лабораторной работе требуется описать и сравнить уровни моделей OSI и TCP/IP. Необходимо также назвать протоколы стека TCP/IP и утилиты, используемые на каждом уровне.

Подробное описание процесса инкапсуляции

Все соединения сети инициируются отправителем и заканчиваются в пункте назначения, т.е. на станции-получателе. Информация, пересылаемая по сети, называется данными, или пакетами данных. Если одному компьютеру (станции А) требуется переслать данные другому компьютеру (станции Б), то эти данные должны быть сначала упакованы с помощью процесса, называемого *инкапсуляцией*.

Инкапсуляция

Процесс *инкапсуляции (encapsulation*) заключается в добавлении к пакету перед его передачей необходимой протокольной информации. Соответственно, по мере движения данных вниз по уровням эталонной модели OSI на каждом уровне к данным добавляется заголовок (а также концевик на втором уровне) перед передачей этих данных на нижележащий уровень. Заголовки и концевики содержат управляющую информацию, необходимую сетевым устройствам и получателю для того, чтобы обеспечить доставку данных и возможность получателю правильно интерпретировать полученные данные. В качестве иллюстративной аналогии можно рассмотреть адрес на конверте. Он требуется для того, чтобы письмо, лежащее в конверте, могло быть доставлено требуемому получателю.

Для того чтобы увидеть, как происходит процесс инкапсуляции, рассмотрим передачу данных по уровням модели OSI, проиллюстрированную на рис. 2.47. После того как данные пересланы отправителем, они проходят через уровень приложений и далее вниз через все остальные уровни. Тип упаковки и характер их передачи

изменяются в процессе выполнения различными уровнями своих функций для доставки данных конечному пользователю.

ВНИМАНИЕ!

Термин *заголовок* означает, что информация добавляется в начало пакета, в то время как концевик добавляется в его конец. Кроме этого, важным элементом добавляемой информации является адрес соответствующего уровня.

Данные в форме электронных сигналов должны быть переданы по кабелю компьютеру, который является требуемым пунктом назначения, а затем преобразованы в свою первоначальную форму, чтобы их мог прочитать получатель. Как можно себе представить, этот процесс включает в себя несколько качественно различных этапов. По этой причине разработчики аппаратного и программного обеспечения, а также протоколов пришли к выводу, что наиболее эффективным способом реализовать сетевые коммуникации является подразделение процесса передачи информации на несколько уровней.

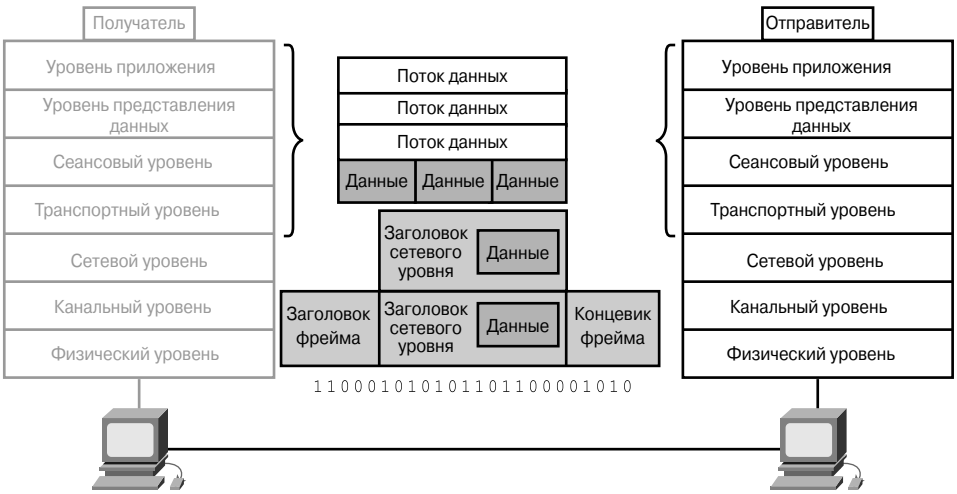


Рис. 2.47. Инкапсуляция

Как показано на рис. 2.48, для инкапсуляции данных в сети необходимо выполнить следующие пять этапов преобразования данных:

Этап 1. **Первоначальное формирование данных**. Когда пользователь отправляет сообщение по электронной почте, символы его письма преобразуются в данные, которые могут быть переданы по объединенной сети.

Этап 2. **Упаковка данных для сквозной передачи по сети**. На этом этапе данные упаковываются для передачи по сети. Используя сегменты, транспортная функция обеспечивает рабочим станции на обоих концах системы

электронной почты возможность осуществлять надежную связь.

Этап 3. **Добавление в заголовок сетевого адреса**. Данные помещаются в пакеты или дейтаграммы, содержащие сетевой заголовок, в котором расположены логические адреса источника и получателя. Эти адреса используются сетевыми устройствами для пересылки пакета по сети в соответствии с выбранным маршрутом.

Этап 4. **Добавление локального адреса в заголовок канального уровня**. Каждое сетевое устройство должно поместить пакет сетевого уровня во фрейм канального уровня. Преобразование пакета во фрейм позволяет осуществить соединение со следующим лежащим на данном маршруте непосредственно подсоединенным сетевым устройством. Каждому устройству на выбранном в сети маршруте необходимо выполнить такое преобразование пакета во фрейм для соединения со следующим устройством.

Этап 5. **Преобразование в биты для передачи по сети**. Функция синхронизации позволяет устройствам различать передаваемые биты при их передаче по сети. На протяжении используемого маршрута физическая среда объединенной сети может меняться. Например, электронное сообщение может исходить из локальной сети LAN, пересечь территориальную магистраль и выйти в канал распределенной сети WAN, перед тем как достичь пункта назначения или другой удаленной локальной сети. Заголовки и концевики добавляются по мере того, как данные перемещаются по уровням эталонной модели OSI.

Декапсуляция

Когда удаленное устройство получает последовательность битов, его физический уровень передает эти биты на канальный уровень для последующей обработки. Канальный уровень выполняет следующие действия:

Этап 1. Выполняется проверка, соответствует ли MAC-адрес пункта назначения адресу этой станции и не является ли он широковещательным адресом. Если ни одно из условий не выполняется, фрейм отбрасывается.

Этап 2. Если данные содержат ошибки, они могут быть отброшены; в этом случае канальный уровень может запросить повторную передачу данных.

Этап 3. Канальный уровень удаляет заголовок канального уровня и концевик, а затем передает оставшиеся данные на сетевой уровень, основываясь на управляющей информации, содержащейся в заголовке канального уровня.

Описанный выше процесс называется *декапсуляцией (de-encapsulation*). Каждый последующий уровень выполняет аналогичный процесс декапсуляции. Процесс декапсуляции можно сравнить с адресом на конверте: если письмо попало требуемому адресату, оно вынимается из конверта.

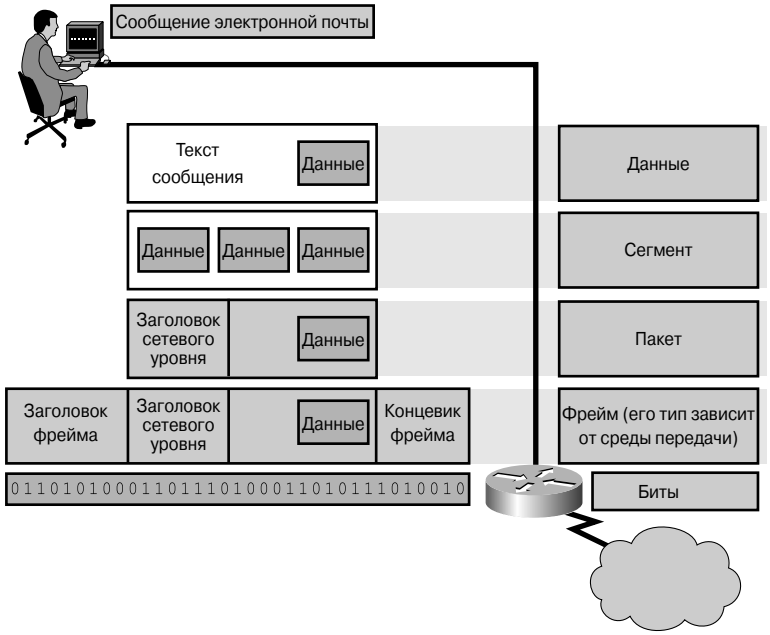


Рис. 2.48. Процесс инкапсуляции данных

Дополнительная информация: контроль с помощью циклического избыточного кода

Каждый пакет данных содержит информацию, которая добавляется к первоначальным содержательным данным в виде заголовков пакетов. Заголовки, в частности, содержат информацию об адресах, которая необходима для того, чтобы пакеты достигли требуемого пункта назначения. Они также содержат информацию о порядке следования пакетов, которая необходима для последующего восстановления первоначального порядка пакетов на компьютере-получателе. Информация заголовка размещается в начале пакета перед первоначальными данными. Пакеты могут также включать информацию концевика, который добавляется после пакета, за первоначальными данными. Находящийся в концевике компонент проверки наличия ошибок называется контролем с помощью циклического избыточного кода (Cyclical Redundancy Check — CRC), или CRC-проверкой. Механизм CRC-проверки выполняет над пакетом определенные вычисления перед тем, как он будет отправлен, и повторяет вычисления после того, как он будет принят получателем. Несовпадение результатов вычислений свидетельствует о том, что в процессе передачи данные были изменены. Это может произойти в результате искажения электрических сигналов, представляющих первоначальные данные в виде последовательности нулей и единиц. Если обнаружено такое несоответствие, то пакет может быть передан повторно.

Практическое задание 2.3.7. Характеристики разных уровней модели OSI и соответствующие устройства

В этой работе описаны характеристики, функции и термины, которые соответствуют разным уровням эталонной модели взаимодействия открытых систем.

Интерактивная презентация: процесс инкапсуляции данных
В этой презентации проиллюстрирован процесс инкапсуляции данных при переходе их с одного уровня эталонной модели OSI на другой.

Резюме

В настоящей главе были изложены следующие ключевые темы, касающиеся сетевых технологий:

- вкратце были описаны движущие мотивы исторического развития локальных сетей LAN и распределенных сетей WAN;
- сетевые устройства используются для соединения друг с другом отдельных сетей. Концентраторы, коммутаторы и маршрутизаторы соединяют между собой сегменты и устройства локальных сетей LAN, сетей городского масштаба MAN и распределенных сетей WAN. Сетевые устройства функционируют на различных уровнях эталонной модели OSI;
- физическая топология сети описывает структуру кабелей, соединяющих между собой физические устройства сети. Логическая топология описывает способ передачи информации по сети;
- в физической шинной топологии один кабель соединяет между собой все устройства сети;
- наиболее часто используемой структурой локальных сетей LAN Ethernet является физическая звездообразная топология. В сети со звездообразной топологией каждая рабочая станция подсоединена к центральному устройству своим собственным отрезком кабеля. Расширенную путем добавления дополнительных устройств, подсоединяемых к центральному устройству, звездообразную сеть называют расширенной звездообразной топологией;
- при использовании кольцевой топологии все рабочие станции соединены кабелем и образуют кольцо;
- в полносвязной топологии все устройства соединены друг с другом;
- локальная сеть LAN состоит из компьютеров, сетевых адаптеров NIC, периферийных устройств, передающей среды и сетевых устройств;
- распределенная сеть WAN состоит из двух или более локальных сетей LAN, охватывающих две или более географически отдаленных друг от друга области;
- сеть городского масштаба MAN обычно охватывает территорию крупного города, включая пригороды;
- сеть хранилищ данных (SAN) имеет повышенную производительность, допускает расширение и имеет встроенные механизмы защиты от стихийных бедствий;
- внутренние сети (Intranet) предназначены для доступа к ним пользователей, имеющих привилегированное право доступа к внутренней сети организации. Внешние сети (Extranet) предназначены для доставки данных приложений и

служб, базирующихся на принципах внутренней (Intranet) сети, однако также позволяющих получать к ним расширенный безопасный доступ внешним пользователям или компаниям;

- виртуальной частной сетью называется частная сеть, создаваемая в инфраструктуре общедоступной сети. Тремя типами VPN-сетей являются сети доступа, внутренние и внешние сети (Intranet и Extranet);
- ширина полосы пропускания и пропускная способность характеризуют производительность сети, т.е. скорость передачи по ней данных;
- пропускная способность сети измеряется в бит/с, Кбит/с, Мбит/с, Гбит/с;
- полоса пропускания ограничивается типом используемой среды, используемыми технологиями сетей LAN или WAN и производительностью сетевого оборудования;
- пропускная способность фактически описывает доступную полосу пропускания соединений и зависит от многих факторов: количества пользователей в сети, используемого сетевого оборудования, типа передаваемых данных, производительности рабочих станций и серверов;
- для расчета времени передачи данных используется следующая формула: T=S/BW (время = объем данных/полоса пропускания);
- аналоговая полоса пропускания указывает на то, какую часть электромагнитного спектра использует технология для передачи сигнала;
- в технологиях цифровой передачи данных вся информация пересылается в виде последовательностей битов независимо от ее природы;
- разделение большой задачи на ряд более мелких значительно облегчает понимание и процесс решения проблемы;
- осуществление связи в сети представляет собой большую задачу, которая может быть разбита на ряд более мелких задач, решаемых на отдельных уровнях. Это может быть сделано различным и способами;
- организация по стандартизации ISO создала и обнародовала эталонную модель OSI в 1984 году. Эталонная модель OSI представляет собой схему описания сети, стандарты которой обеспечивают совместимость и возможность совместной работы сетей, использующих различные сетевые технологии;
- каждый уровень модели OSI выполняет свои специфические функции и использует для этого соответствующие протоколы. Эталонная модель OSI имеет семь уровней: уровень приложений, уровень представления данных, уровень сеанса связи, транспортный уровень, сетевой, канальный и физический;
- каждый уровень в коммуникационном протоколе передающего устройства взаимодействует с аналогичным (одноранговым) уровнем принимающего устройства;

- модель TCP/IP имеет четыре уровня: уровень приложений, транспортный уровень, уровень Internet (межсетевого взаимодействия) и уровень доступа к сети;
- все соединения в сети инициируются станцией-отправителем и заканчиваются на станции-получателе. Перед передачей данных по сети на каждом уровне эталонной модели OSI происходит их инкапсуляция, т.е. добавление к ним необходимой протокольной информации;
- центром обработки данных называется глобально координируемая сеть, состоящая из устройств, предназначенных для ускорения передачи информации по инфраструктуре глобальной сети Internet;
- повторители регенерируют, усиливают и повторно синхронизируют сигналы перед отправкой их по сети;
- термин *концентратор (hub)* используется вместо термина *повторитель (repeater)* в том случае, когда такое устройство служит центральной точкой сети. Концентраторы (также называемые многопортовыми повторителями) функционируют только на первом уровне и не принимают решений о направлении пересылки данных. Сеть, в которой используются только концентраторы, является сетью с разделяемым доступом и в ней возможны коллизии. По мере того, как количество устройств в сети увеличивается, в ней происходит все больше коллизий и производительность сети резко падает;
- коммутаторы локальных сетей LAN функционируют на втором уровне и принимают некоторые решения о направлении пересылки данных на основании анализа аппаратных MAC-адресов. Коммутаторы в сетях Ethernet позволяют создавать выделенные LAN-соединения;
- работающие на втором, третьем и четвертом уровнях многоуровневые коммутаторы позволяют реализовать на третьем уровне эталонной модели механизмы качества обслуживания и функции обеспечения безопасности сети. Многоуровневые коммутаторы выполняют некоторые функции, обычно выполняемые маршрутизаторами, однако, в отличие от последних, делают это на уровне аппаратного обеспечения;
- маршрутизаторы способны принимать решения о наилучшем маршруте доставки данных по сети;
- для предоставления служб компьютерам и пользователям, получающим доступ к сети, используются различные типы серверов;
- брандмауэры, AAA-серверы и концентраторы VPN-сетей используются для обеспечения безопасности сети;
- типичными беспроводными сетевыми устройствами являются беспроводные сетевые адаптеры, беспроводные точки доступа и беспроводные мосты.

Обратите внимание на относящиеся к настоящей главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные

презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Ключевые термины

Адрес управления доступом к среде передачи, или MAC-адрес (Media Access Control — MAC) — аппаратный адрес, уникальным образом идентифицирующий каждый узел сети. Используется для управления сеансами связи данного устройства.

Брандмауэр (firewall) — маршрутизатор или сервер доступа, выполняющий роль буфера между подсоединенными общедоступными сетями и частной корпоративной сетью.

Виртуальная частная сеть (Virtual Private Network — VPN) — частная сеть, создаваемая в открытой сетевой инфраструктуре, такой, например, как глобальная сеть Internet.

Внешняя сеть (Extranet) — основанные на внутренней сети (Intranet) приложения и службы, позволяющие получать расширенный безопасный доступ к внутренней сети предприятия внешним пользователям или предприятиям.

Внутренняя сеть (Intranet) — обычная конфигурация локальной сети LAN. Intranet-сети предназначены для того, чтобы к ним получали доступ только пользователи, имеющие привилегированный доступ к внутренней локальной сети предприятия.

Декапсуляция (de-encapsulation) — освобождение данных от заголовка конкретного протокола.

Домен коллизий (collision domain): в сетях Ethernet — область сети, в которой распространяются столкнувшиеся и поврежденные фреймы. Повторители и концентраторы не отфильтровывают такие поврежденные фреймы, в то время как коммутаторы локальных сетей LAN, мосты и маршрутизаторы их не пропускают.

Звездообразная топология (star topology) — наиболее часто используемая физическая топология локальных сетей Ethernet. Сеть со звездообразной топологией имеет центральную точку соединений, которая может быть концентратором, коммутатором или маршрутизатором; в этой точке сходятся все кабельные сегменты.

Иерархическая топология (hierarchical topology) — эта топология создается аналогично расширенной звездообразной топологии. Основным отличием является отсутствие в ней центрального узла. Вместо него используется магистральный узел, от которого расходятся ветви к другим узлам.

Инкапсуляция (encapsulation) — упаковка данных в заголовок конкретного протокола.

Канальный уровень (data link layer) — второй уровень эталонной модели OSI. Обеспечивает передачу данных по физическому каналу. Канальный уровень отвечает за физическую адресацию, анализ сетевой топологии, контроль канала, уведомление об ошибках, упорядоченную доставку фреймов и управление потоками.

Коллизия (collision): в сетях Ethernet коллизия — столкновение фреймов, произошедшее вследствие попытки одновременной их передачи. В результате оба фрейма повреждаются при встрече в физической среде.

Кольцевая топология (ring topology) — тип сетевой топологии, при использовании которого рабочие станции объединяются в кольцо одним или двумя кабелями. В отличие от физической шинной топологии, в кольцевой нет начала и конца, поэтому необходимость в терминаторе отсутствует.

Коммутатор (switch) — устройство, соединяющее сегменты локальной сети LAN и использующее таблицу MAC-адресов для определения сегментов, в которые следует переслать фреймы. Такой принцип работы позволяет существенно уменьшить объем нецелесообразно рассылаемых данных. Коммутаторы работают с гораздо бо́льшими скоростями, чем мосты.

Концентратор (hub) — общая точка соединений устройств сети. Обычно концентраторы используются для подсоединения к локальной сети отдельных сегментов. Концентратор может иметь несколько портов. Когда на один из них поступает пакет, он копируется и направляется на все остальные порты концентратора, поэтому такой пакет поступает во все сегменты LAN-сети.

Лавинная рассылка (flooding) представляет собой способ передачи данных, применяемый коммутаторами и мостами, при использовании которого данные, полученные на некотором интерфейсе, рассылаются через все интерфейсы устройства, за исключением того, на котором они были первоначально получены.

Локальная сеть (local-area network — LAN) — высокоскоростная сеть передачи цифровых данных с низким уровнем ошибок, охватывающая относительно небольшую географическую область (до нескольких километров). Локальные сети включают в себя рабочие станции, периферийные устройства, терминалы и другие устройства, расположенные в одном здании или в другой географически ограниченной области.

Маршрутизатор (router) — это применяемое в объединенных сетях устройство, которое передает пакеты данных между сетями на основе адреса третьего уровня (сетевого адреса). Маршрутизатор может принимать решение о выборе наилучшего маршрута доставки данных по сети.

Микросегментация (microsegmentation) позволяет создавать в локальной сети частные или выделенные сегменты, в которых на каждый сегмент приходится только одна рабочая станция. В этом случае каждая станция получает мгновенный доступ ко всей полосе пропускания, и ей не приходится конкурировать с другими за доступ к доступной полосе пропускания.

Мост (bridge) — устройство второго уровня, предназначенное для создания двух или более сегментов локальной сети LAN, каждый из которых является отдельным доменом коллизий.

Неполносвязная топология (partial-mesh topology) — в сети с такой топологией, по крайней мере, одно устройство имеет несколько соединений с другими устройствами сети, однако при этом сеть не обладает полносвязной структурой. Вместе с тем

неполносвязная топология обеспечивает определенный уровень избыточности за счет наличия нескольких альтернативных маршрутов.

Одноранговая связь (peer-to-peer communication) — форма связи устройств в сети, в которой каждый уровень эталонной модели OSI источника вступает в связь с аналогичным уровнем получателя.

Пакет (packet) — логически сгруппированная информация, включающая в себя заголовок, содержащий управляющую информацию и (обычно) данные пользователя. Термин *пакет* чаще всего употребляется применительно к модулям данных сетевого уровня.

Передача маркера (token passing) — метод доступа, при использовании которого устройства сети получают доступ к физической среде передачи упорядоченным образом, на основе обладания небольшим фреймом, называемым маркером.

Плата сетевого интерфейса (Network Interface Card — NIC) — печатная плата, вставляемая в гнездо расширения на материнской плате компьютера. Также может быть отдельным периферийным устройством.

Повторитель (repeater) — сетевое устройство, функционирующее на первом (физическом) уровне эталонной модели OSI. Назначение повторителя состоит в регенерации и ресинхронизации сетевых сигналов на битовом уровне, что позволяет передавать их по передающей среде на большее расстояние.

Полносвязная топология (full-mesh topology) — разновидность сетевой топологии, в которой все устройства (узлы) соединены друг с другом, что обеспечивает высокий уровень избыточности и устойчивости при отказах отдельных каналов.

Пропускная способность сети (throughput) — объем информации, поступающей в конкретную точку сетевой системы или проходящей через нее.

Протокол (protocol) — формальное описание набора правил и соглашений, управляющих обменом информацией между устройствами сети.

Распределенная сеть (Wide-Area Network — WAN) — коммуникационная сеть, обслуживающая пользователей, расположенных в обширной географической области, в которой используются устройства передачи данных, предоставляемые операторами глобальной связи.

Расширенная звездообразная топология (extended-star topology) — сеть, в которой классическая звездообразная топология расширена и в нее включены дополнительные сетевые устройства, подсоединенные к главному сетевому устройству.

Региональная или городская сеть (Metropolitan-Area Network — MAN) —сеть, охватывающая область крупного города, включая пригороды. В целом MAN-сети, как правило, охватывают большую географическую область, чем локальные сети LAN, но меньшую, чем распределенные сети WAN.

Сеансовый уровень (session layer) — пятый уровень эталонной модели OSI. Устанавливает, поддерживает и прекращает сеансы связи между приложениями и управляет обменом данными между уровнями представления данных.

Сегмент (segment): в спецификации протокола TCP — логически сгруппированная информация на транспортном уровне эталонной модели OSI.

Сетевой уровень (network layer) — третий уровень эталонной модели OSI. Обеспечивает соединения и выбор маршрутов между конечными системами. На данном уровне происходит маршрутизация.

Сеть хранилищ данных (Storage-Area Network — SAN) — высокопроизводительная выделенная сеть, осуществляющая обмен данными между серверами и устройствами хранения данных.

Стек протоколов (protocol suite) — набор связанных между собой коммуникационных протоколов, функционирующих совместно и в качестве одного целого управляющих работой некоторых или всех семи уровней эталонной модели OSI. Не каждый стек протоколов охватывает все уровни эталонной модели; часто один протокол стека управляет коммуникацией сразу на нескольких уровнях. Типичным стеком протоколов является набор протоколов TCP/IP.

Транспортный уровень (transport layer) — четвертый уровень эталонной модели OSI. Он отвечает за надежность связи между конечными узлами. Транспортный уровень имеет механизмы установки, поддержки и отключения виртуальных каналов, обнаружения и устранения ошибок при передаче данных, а также управляет информационными потоками.

Уровень представления данных (presentation layer) — шестой уровень эталонной модели OSI. Он обеспечивает совместимость форматов (читабельность) данных разных систем.

Уровень приложений (application layer) — седьмой уровень эталонной модели OSI. Предоставляет службы процессам приложений (таким, как электронная почта, передача файлов или эмуляция терминала), находящимся вне эталонной модели OSI.

Физический уровень (physical layer) — первый уровень эталонной модели OSI. Определяет электрические, механические, процедурные и функциональные спецификации активизации, поддержки и отключения физических каналов между конечными системами.

Фрейм (frame) — логически сгруппированная информация, пересылаемая в виде блока данных канального уровня по среде сети.

Центр обработки данных (data center) — глобально координируемая сеть, состоящая из устройств, предназначенных для ускорения доставки данных по инфраструктуре сети Internet.

Шинная топология (bus topology) — топология, в которой все устройства соединены одним кабелем; часто называется линейной шиной. Этот кабель можно сравнить с автобусным маршрутом, проходящим от одной остановки к другой.

Ширина полосы пропускания (bandwidth) — объем информации, проходящей через сетевое соединение за определенный период времени.

Широковещание (broadcast) — процесс рассылки пакетов данных всем узлам сети. Широковещательные пакеты имеют специальный широковещательный адрес.

Широковещательный домен (broadcast domain) — совокупность устройств, получающих широковещательные фреймы от любого из них.

Эталонная модель взаимодействия открытых систем (Open System Interconnection — OSI reference model) — структурная модель сети, разработанная международной организацией по стандартизации (ISO). Эта модель включает в себя семь уровней, каждый из которых выполняет свои специфические функции, такие, как адресация, управление потоком, контроль ошибок, инкапсуляция и надежная передача сообщений. Эталонная модель OSI используется как универсальный метод обучения сетевых специалистов для понимания ими функций компьютерной сети.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. К какому типу относилась первая сеть, состоявшая из микрокомпьютеров?

а) MAN.

б) WAN.

в) LAN.

г) PAN.

2. Если для соединения компьютеров в сеть используются модемы, то сколько модемов требуется для соединения между собой десяти компьютеров?

а) Один.

б) Пять.

в) Десять.

г) Пятнадцать.

3. Какой код "прошивается" в постоянную память платы сетевого интерфейса?

а) NIC.

б) MAC-адрес.

в) Концентратор.

г) LAN-сеть.

4. В какой топологии все узлы подсоединены непосредственно к одной центральной точке и не имеют соединений с другими краевыми узлами?

а) В шинной топологии.

б) В кольцевой топологии.

в) В звездообразной топологии.

г) В полносвязной топологии.

5. Что означают аббревиатуры TIA и EIA?

а) Television Industry Association, Electronic Industries Association (Ассоциация телевизионной промышленности, Ассоциация электронной промышленности).

б) Telecommunications Industry Association, Electronic Industries Alliance (Ассоциация телекоммуникационной промышленности, Альянс электронной промышленности).

в) Telecommunications Industry Alliance, Electronic Industries Association (Альянс телекоммуникационной промышленности, Ассоциация электронной промышленности).

г) Téléphonique International Association, Elégraphique Industries Alliance (Международная телефонная ассоциация, Альянс телеграфной промышленности[8]).

6. Какие из перечисленных ниже функций должна выполнять локальная сеть LAN? (Следует выбрать все правильные ответы.)

а) Функционирование в географически ограниченной области.

б) Поддержка доступа многих пользователей к высокоскоростной широкополосной среде передачи.

в) Подсоединение к сети Internet.

г) Обеспечение постоянного подключения к локальным службам.

7. Какое из приведенных ниже утверждений наилучшим образом характеризует распределенную сеть WAN?

а) Эта сеть соединяет между собой локальные сети LAN, разделенные большими расстояниями в обширной географической области.

б) Эта сеть соединяет между собой рабочие станции, терминалы и другие устройства и объединяет их в сеть городского масштаба.

в) Эта сеть соединяет между собой несколько локальных сетей LAN в пределах одного большого здания.

г) Эта сеть соединяет между собой рабочие станции, терминалы и другие устройства, расположенные в одном здании.

8. Какое из приведенных ниже утверждений правильно описывает сеть городского масштаба MAN?

а) MAN представляет собой сеть, соединяющую между собой рабочие станции, периферийные устройства, терминалы и другие устройства, находящиеся в одном здании.

[8] *В данном варианте ответа расшифровки аббревиатур написаны на смеси ломаного французского и английского. — Прим. ред.*

б) MAN представляет собой сеть, которая обслуживает пользователей в обширной географической области. Часто она использует устройства передачи данных, предоставляемые операторами связи.

в) MAN представляет собой сеть, которая охватывает площадь крупного города, включая пригороды.

г) MAN представляет собой сеть, образованную соединенными между собой маршрутизаторами и другими устройствами и функционирующую как единая сеть.

9. Какая из перечисленных ниже функций *НЕ* является функцией сети SAN?

а) Сети SAN обеспечивают высокопроизводительный конкурентный доступ к дисковым или ленточным накопителям.

б) Сети SAN обеспечивают надежное восстановление сети в случае аварии.

в) Сети SAN обеспечивают масштабируемость.

г) Сети SAN сводят к минимуму доступность системы и данных.

10. Какие сети обеспечивают безопасные и надежные соединения по открытой сетевой инфраструктуре?

а) Сеть Internet.

б) Виртуальные частные сети.

в) Виртуальные открытые сети.

г) Распределенные сети WAN.

11. Какой тип каналов используется для связи между собой головного офиса компании, удаленных офисов и филиалов с помощью общей инфраструктуры?

а) VPN-сети доступа.

б) VPN-сети Intranet.

в) VPN-сети Extranet.

г) VPN-сети Internet.

12. Как называется часть локальной сети компании, которая доступна для связи с сотрудниками компании, клиентами и коммерческими партнерами?

а) Сеть Internet.

б) Сеть Extranet.

в) Сеть Intranet.

г) Локальная сеть LAN.

13. Как называется перемещение объектов по уровням эталонной модели?

а) Упаковка (wrapping).

б) Поток.

в) Путешествие.

г) Передача.

14. Сколько уровней имеет эталонная модель OSI?

а) Четыре.

б) Пять.

в) Шесть.

г) Семь.

15. Что представляет собой эталонная модель OSI?

а) Эталонная модель OSI представляет собой концептуальную схему, которая описывает перемещение информации по сети.

б) Эталонная модель OSI описывает перемещение данных по сети от одной программы-приложения к другой аналогичной программе.

в) Эталонная модель OSI представляет собой концептуальную схему, которая определяет, какие функции выполняются каждым уровнем модели.

г) Все вышеперечисленное.

16. Какой порядок уровней является правильным?

а) 1 — физический, 2 — канальный, 3 — транспортный, 4 — сетевой, 5 — уровень представления данных, 6 — сеансовый, 7 — уровень приложений.

б) 1 — физический, 2 — канальный, 3 — сетевой, 4 — транспортный, 5 — сеансовый, 6 — уровень представления данных, 7 — уровень приложений.

в) 1 — физический, 2 — канальный, 3 — сетевой, 4 — сеансовый, 5 — транспортный, 6 — уровень представления данных, 7 — уровень приложений.

г) 1 — физический, 2 — сетевой, 3 — сеансовый, 4 — канальный, 5 — транспортный, 6 — уровень приложений, 7 — уровень представления данных.

17. Какой уровень эталонной модели OSI отвечает за физическую адресацию, сетевую топологию, доступ к сети и управление потоками?

а) Физический уровень.

б) Канальный уровень.

в) Транспортный уровень.

г) Сетевой уровень.

18. Какая из приведенных ниже операций соответствует инкапсуляции?

а) Сегментация потока данных, для того чтобы при прохождении по сети не было его разрыва.

б) Сжатие данных для более быстрой их передачи.

в) Перемещение данных в группы для компактного совместного хранения.

г) Упаковка данных в отдельный заголовок протокола.

19. Сообщение по электронной почте отправляется рабочей станцией A рабочей станции B по локальной сети LAN. Перед отправкой этого сообщения данные должны быть инкапсулированы. Какое из приведенных ниже действий наилучшим образом описывает события, происходящие после создания пакета?

а) Пакет передается по среде.

б) Пакет помещается во фрейм.

в) Пакет сегментируется во фреймы.

г) Пакет преобразуется в двоичный формат.

20. Какой уровень в модели протоколов TCP/IP отвечает за надежность передачи, управление потоками и исправление ошибок при передаче?

а) Уровень приложений.

б) Транспортный уровень.

в) Уровень Internet.

г) Уровень доступа к сети.

21. Какая из приведенных ниже проблем легко может быть решена с помощью повторителя?

а) В сети слишком много различных типов не совместимого друг с другом оборудования.

б) В сети слишком большой объем передачи данных.

в) Скорость конвергенции протоколов слишком мала.

г) Слишком много узлов или недостаточно кабеля.

22. Какое из приведенных ниже утверждений справедливо для моста и принимаемых им решений о пересылке данных?

а) Мосты функционируют на втором уровне эталонной модели OSI и для принятия решений используют IP-адреса.

б) Мосты функционируют на третьем уровне эталонной модели OSI и для принятия решений используют IP-адреса.

в) Мосты функционируют на втором уровне эталонной модели OSI и для принятия решений используют MAC-адреса.

г) Мосты функционируют на третьем уровне эталонной модели OSI и для принятия решений используют MAC-адреса.

23. Какое из приведенных ниже утверждений справедливо для описания функций коммутатора?

а) Коммутаторы увеличивают количество доменов коллизий.

б) Коммутаторы объединяют в себе функции создания соединений концентратора и функцию регулирования потоков данных, присущую мосту.

в) Коммутаторы объединяют в себе функции создания соединений концентратора и функцию регулирования потоков данных, присущую маршрутизатору.

г) Коммутаторы осуществляют выбор маршрута на четвертом уровне.

24. Для каких объектов маршрутизатор выбирает маршрут?

а) Для битов первого уровня.

б) Для фреймов второго уровня.

в) Для пакетов третьего уровня.

г) Для сегментов четвертого уровня.

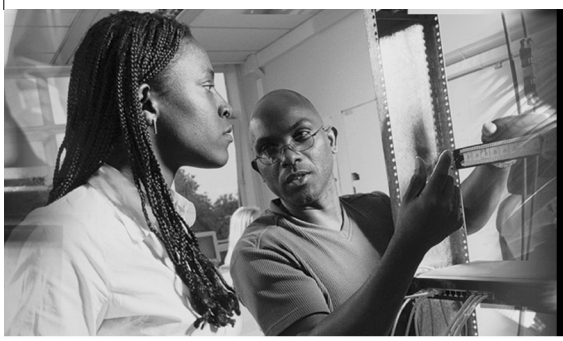
25. Какое из приведенных ниже утверждений справедливо?

а) Шлюз является устройством специального назначения, которое на уровне приложений преобразует информацию из одного стека протоколов в другой.

б) Универсальный шлюз серии AS5400 обеспечивает на всех своих портах постоянные универсальные службы, голосовую службу, службу беспроводного доступа и факсимильную связь.

в) Мультиплексор DSLAM служит точкой интерфейса между рядом помещений подписчиков и сетью оператора связи.

г) Справедливы все приведенные выше утверждения.



ГЛАВА 3

Сетевая среда передачи данных

В этой главе...

- описаны основные составляющие атома;
- рассказывается об основных измерительных характеристиках электричества;
- даны определения сопротивления и импеданса;
- объясняется, что такое ток и напряжение;
- описано, как устроена стандартная электрическая цепь;
- перечислены организации, которые разрабатывают стандарты для кабельных и беспроводных сетей;
- описаны основные типы кабеля витой пары и их использование;
- дано определение электромагнитного спектра;
- приводится описание основных разновидностей коаксиального кабеля и их использования;
- описана беспроводная среда передачи данных и применение беспроводной связи;
- рассказывается об электрических свойствах материи;
- рассматривается отражение и преломление света;
- описаны основные типы оптического кабеля и их использование, а также сигналы и шумы в стекловолокне;
- описаны различные методы беспроводного взаимодействия, их преимущества и недостатки;
- рассматриваются средства подключения и аутентификации узлов беспроводной сети;
- рассмотрены различные механизмы модуляции;
- описана радиочастотная модуляция;
- определены преимущества технологии расширения спектра;
- описаны технологии расширения спектра в прямой последовательности и со скачкообразным изменением частоты;
- говорится о важности шифрования и обеспечения безопасности в беспроводных сетях.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

коаксиальный кабель, с. 160,
сопротивление, с. 165,
импедансом, с. 165,
стандарт, с. 169,
институт инженеров по электротехнике и электронике, с. 169,
ассоциация промышленности средств связи, с. 169,
ассоциация электронной промышленности, с. 169,
толстый коаксиальный кабель, с. 173,
тонкий коаксиальный кабель, с. 174,
наводки, с. 176,
экранированная витая пара, с. 176,
неэкранированная витая пара, с. 177,
длина волны, с. 181,
электромагнитный спектр, с. 181,
отражение, с. 184,
преломление, с. 184,
оптоволоконные кабели, с. 188,
одномодовое волокно, с. 191,
многомодовое волокно, с. 191,
дисперсия мод, с. 191,
помеха, с. 197,
затухание, с. 197,
рассеивание, с. 198,
поглощение, с. 198,
дисперсия, с. 198,
децибел, с. 201,
амплитудная модуляция, с. 204,
частотная модуляция, с. 204,
фазовая модуляция, с. 204,
технология расширения частотного спектра, с. 206,
расширение спектра со скачкообразным изменением частоты, с. 207,
расширение спектра прямого преобразования, с. 207,
роуминг, с. 212,
протокол обеспечения безопасности для беспроводных сетей, с. 218.

Основные функции физического уровня заключаются в передаче данных от отправителя получателю по определенным электрическим, беспроводным либо оптическим средам передачи данных. После того как данные достигают распределительного оборудования в здании, они переносятся с помощью сигналов с низким напряжением к рабочим станциям, серверам и сетевым устройствам посредством кабелей, которые вмонтированы в стены либо размещены над подвесными потолками или под полом. Данные, которые могут состоять из текста, графических изображений, звука или видео, распространяются через кабельные системы, в которых они представляются как электрические импульсы в медных проводниках либо как световые импульсы в оптических волокнах.

В этой главе изложены основы теории электричества, необходимые для понимания работы сети на физическом уровне базовой модели OSI. В главе также обсуждаются различные типы сетевых сред передачи данных, которые используются на физическом уровне, включая экранированную витую пару, неэкранированную витую пару, коаксиальный кабель, оптоволоконный кабель, а также беспроводные механизмы передачи данных.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в данной главе.

Медные проводники как среда передачи данных

В этом разделе обсуждаются основы теории электричества, которые необходимы для понимания работы сети на физическом уровне (т.е. первом уровне) базовой эталонной модели OSI.

Медные проводники — наиболее распространенная среда передачи данных для передачи электрических сигналов. Они являются компонентами кабелей, по которым сигналы передаются от источника приемнику. Меди присущи несколько очень важных свойств, которые делают ее предпочтительной для прокладки соединительных кабелей.

- **Высокая электропроводность.** Медь хорошо известна своей способностью беспрепятственно пропускать электрический ток. Медь также превосходно проводит тепло. Последнее свойство сделало этот материал привлекательным для изготовления предметов кухонной утвари, радиаторов, рефрижераторов.
- **Устойчивость против коррозии.** Медь слабо окисляется и поэтому имеет надлежащую стойкость к коррозии; медь окисляется до оксида намного медленнее, чем другие металлы.
- **Эластичность.** Медь обладает большой эластичностью, свойством вытягиваться в тонкую проволоку, не разрываясь при этом. Например, медный прут толщиной 1 см может быть нагрет, раскатан и вытянут в проволоку толщиной меньше человеческого волоса.

- **Ковкость.** Чистая медь очень хорошо поддается ковке (приданию любой формы). Она не крошится при ковке, чеканке либо скручивании в необычные формы. Медь может обрабатываться как при низких, так и при высоких температурах.
- **Прочность.** Холоднокатаная медь имеет прочность на разрыв от 3500 до 4900 килограммов на квадратный сантиметр. Она сохраняет свою прочность даже при нагревании до температуры в 400 градусов по Фаренгейту (F) (204 градуса по Цельсию (C)).

В этом разделе речь пойдет о двух типах медных кабелей, которые используются для соединения сетевых устройств.

- **Витая пара (Twisted-Pair).** Кабель витой пары составлен из одной или более пар медных проводников. Большинство сетей передачи данных и голоса используют соединения кабелем витой пары.
- **Коаксиальный кабель (Coaxial cable).** Коаксиальный кабель состоит из центрального сплошного и сплетенного медных проводников. Коаксиальный кабель когда-то был выбран в качестве основного для прокладки локальных компьютерных сетей, но сейчас он преимущественно используется для соединения видеоаппаратуры, высокоскоростных соединений, таких, как линии T3 (либо E3), а также для кабельного телевидения.

Строение атома

Основными единицами, из которых состоят любые материалы во вселенной, являются атомы. Атомы состоят из более мелких частиц трех типов: протонов, нейтронов и электронов. Нейтроны и протоны сосредоточены в небольшой области и формируют ядро атома. Электроны находятся в свободном движении вокруг этого ядра. Когда частицы трех типов сближаются на определенное расстояние, они создают атомы. Периодическая таблица элементов, изображенная на рис. 3.1, содержит все известные химические элементы (атомы) и их свойства. Атомы состоят из трех простейших частиц:

- **протонов** — частиц, имеющих положительный электрический заряд;
- **нейтронов** — частиц, не имеющих электрического заряда;
- **электронов** — частиц, имеющих отрицательный электрический заряд.

В нормальном состоянии атом состоит из одинакового количества протонов и электронов. Поскольку положительный и отрицательный заряды одинаковы по величине, суммарный заряд атома равен нулю, либо, иными словами, отсутствует.

Нильс Бор (Niels Bohr), датский физик, разработал упрощенную модель для иллюстрации строения атомов, которая изображена на рис. 3.2. На рисунке изображена модель Бора для атома гелия, который состоит из двух протонов, двух нейтронов и двух электронов. Протоны и нейтроны формируют ядро атома в его центре, а электроны вращаются вокруг ядра по своим орбитам. На рисунке не соблюден масштаб, потому как если протоны и нейтроны этого атома представить размером с футбольные

мячи в центре футбольного поля, тогда электроны сравнимы по размеру с вишнями, и их орбиты будут расположены рядом с самыми отдаленными местами на стадионе. Электроны ничтожно малы по сравнению с ядром, а их орбиты намного больше размеров частиц; кроме того, сами атомы являются микроскопическими.

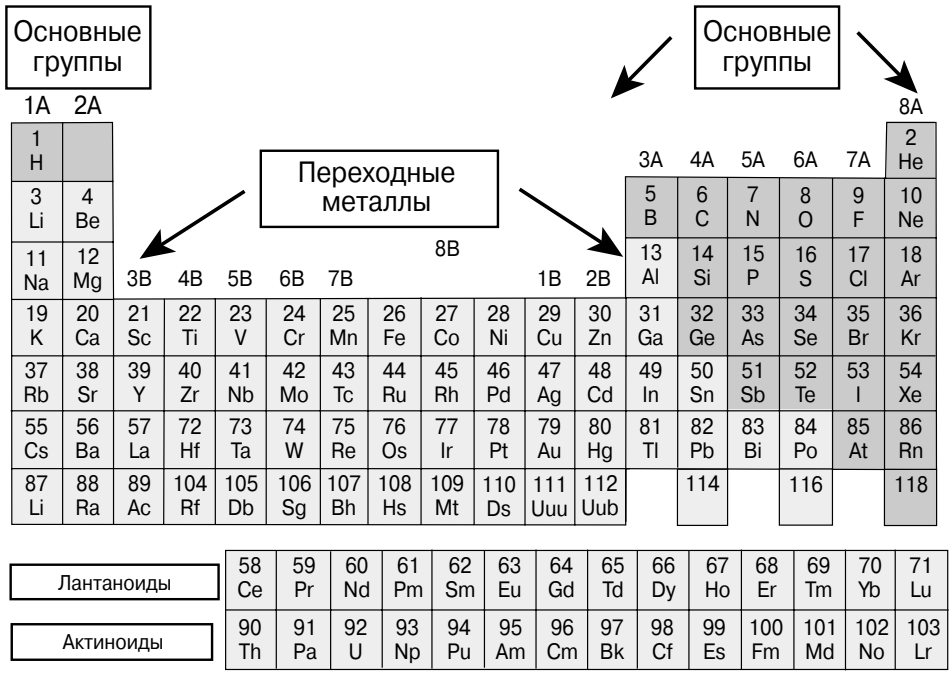


Рис. 3.1. Периодическая таблица элементов

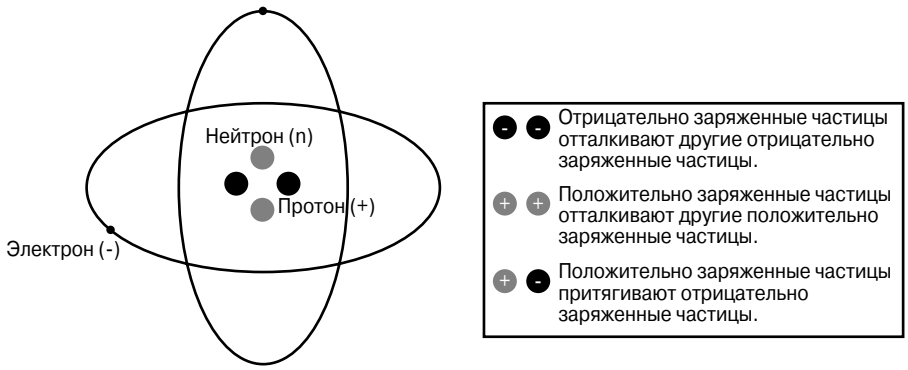


Рис. 3.2. Модель Бора для атома гелия

Атомы соединяются вместе в различных комбинациях и создают молекулы разнообразных материалов. Например, молекулы воды формируются за счет соединения атомов водорода и кислорода.

Электрические свойства материалов

Частицы в ядре атома удерживаются огромной силой. Электроны, вращающиеся по своим орбитам, удерживаются на них с намного меньшей силой. Электроны некоторых атомов могут отдаляться от своих орбит и переходить на орбиты близлежащих атомов. Такое передвижение электронов было названо электрическим током.

Если какой-либо атом потерял или приобрел электрон, то в таком случае количество электронов и протонов в атоме становится разным. Такие атомы называют ионами. Они имеют ненулевой результирующий электрический заряд вследствие разного количества протонов и электронов. Заряд иона вызывает силу, которая воздействует на соседние атомы, и может вынудить их к потере либо приобретению электронов. Таким образом, электроны соседних атомов приходят в движение и создают электрический ток через материал.

Атомы и молекулы могут быть отнесены к одной из трех групп, в зависимости от того, насколько легко электроны могут покидать свои орбиты. Такие три группы материалов называют изоляторами, проводниками и полупроводниками. В табл. 3.1 приведены примеры материалов, относящихся к указанным трем группам.

Электрические изоляторы

Изоляторы — материалы, состоящие из атомов либо молекул, в которых необходимо приложить очень большую силу, для того чтобы их электроны покинули свои орбиты. Примерами электрических изоляторов являются пластик, стекло, воздух, сухое дерево, бумага, резина и чистая вода (в которой атомы находятся в неионизированном состоянии).

Таблица 3.1. Три типа электрических материалов

Материал	Подвижность электронов	Примеры
Изоляторы	Поток электронов затруднен	Пластик, бумага, резина, сухое дерево, воздух, чистая вода и стекло
Проводники	Свободный поток электронов	Медь (Cu), серебро (Ag), золото (Au), олово, ионизированная вода и человеческое тело
Полупроводники	Поток электронов можно точно контролировать	Углерод (C), германий (Ge), арсенид галлия (GaAs) и кремний (Si)

Проводники

Проводники — материалы, состоящие из атомов или молекул, электроны которых очень слабо удерживаются ядрами и под действием небольшой силы легко покидают свои орбиты. Атомы в периодической таблице распределены по группам в соответствии с колонкой, в которой расположен данный элемент. Хорошо проводящие электрический ток материалы расположены в отдельной строке в табл. 3.1 и в отдельной колонке периодической таблицы элементов: медь (Cu), серебро (Ag)

и золото (Au). К другим проводникам относят переходные металлы, включая свинцовый припой, который является смесью свинца (Pb) и олова (Sn), а также воду, в которой присутствуют ионы. Поскольку человеческое тело состоит приблизительно на 70 % из ионизированной воды, оно также является неплохим проводником.

Полупроводники

Полупроводники — материалы, состоящие из атомов или молекул, движение электронов которых можно контролировать. Наиболее важным полупроводником является кремний (Si). Другие примеры полупроводниковых материалов из той же колонки периодической таблицы: углерод (C) и германий (Ge). Арсенид галлия (GaAs) состоит из молекул, которые являются химическим соединением атомов галлия (Ga) и мышьяка (As). Он также является распространенным полупроводником.

Кремний является широко распространенным в природе веществом и присутствует в песке, стекле и многих разновидностях скальных пород. Район города Сан-Хосе в Калифорнии называют "Кремниевой долиной" (Silicon Valley), поскольку компьютерная промышленность, в которой широко используются кремниевые микросхемы, зарождалась именно здесь. Логические элементы любого переключателя в микросхеме сделаны из кремния. В Кремниевой долине размещены офисы множества корпораций и фирм, которые имеют отношение к компьютерной и электронной промышленности.

Практическое задание 3.1.1. Правила электротехнической безопасности и работа с мультиметром

В этой лабораторной работе вы познакомитесь с устройством для измерения параметров электрических цепей — мультиметром и научитесь правильно им пользоваться.

Напряжение

Для того чтобы использовать электрические процессы, необходимо определить параметры, которые описывают свойства электрических процессов. Можно измерять множество параметров электрических процессов, но в следующих разделах речь пойдет об основных характеристиках электрических цепей: напряжении, электрическом токе, сопротивлении и импедансе.

Исходя из того, что электроны и протоны имеют противоположные по знаку заряды, они притягиваются друг к другу с силой, подобной той, которая возникает между северным и южным полюсами двух магнитов. Если такие заряды разнести в пространстве, то между ними возникнет сила притяжения. В пространстве между таким образом разнесенными зарядами возникает электрическое поле. Работа, произведенная при перемещении единичного заряда между двумя точками в пространстве в электрическом поле, и называется напряжением.

Напряжение, иногда называемое электродвижущей силой (э.д.с.), представляет собой электрическую силу или давление, которое возникает при разделении электронов и протонов. Возникающая сила толкает в направлении разноименных зарядов и в противоположную сторону от одноименных. Подобный процесс имеет место в электрической батарее, когда химическая реакция вызывает высвобождение

электронов на отрицательном полюсе и их перемещение к противоположному положительному полюсу. Разделение зарядов приводит к возникновению напряжения. Напряжение также может создаваться трением (статическое электричество), магнитным полем (электрический генератор) или светом (солнечная батарея).

Напряжение обозначается буквой *V* и иногда буквой *E* (от английского electromotive force — электродвижущая сила). Единицей измерения напряжения является вольт (В), который определяется как количество работы на единицу заряда, затрачиваемой на разделение зарядов (например, 12 V = 12 В = 12 Вольт).

Существуют две разновидности напряжения:

- **напряжение постоянного тока (Direct-Current voltage — DC voltage).** Примером источника постоянного тока являются обычные батарейки. Движение электронов в таком источнике всегда происходит в одном направлении, от негативного полюса к позитивному;
- **напряжение переменного тока (Alternate-Current voltage — AC voltage)** дает источник тока, в котором положительный и отрицательный полюса изменяются периодически с течением времени. Пример того, как изменяется напряжение на полюсах в зависимости от времени, приведен на рис. 3.3. Изменение знака полюсов источника напряжения приводит к изменению направления движения электронов с течением времени.

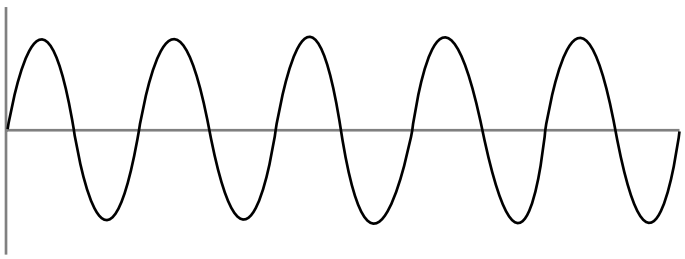


Рис. 3.3. Переменный ток

Практическое задание. Измерение напряжения
В данной лабораторной работе необходимо будет измерить напряжение с помощью мультиметра.

Сопротивление и импеданс

Атомы проводников обмениваются электронами довольно легко, поэтому не нужно прикладывать высокое напряжение, для того чтобы заставить их двигаться по проводнику. В то же время электроны в изолирующих материалах очень сильно удерживаются на своих атомарных орбитах, что препятствует их движению по объему изолятора. *Сопротивление* — это свойство материала, которое показывает, насколько сильно материал препятствует прохождению через него электрического тока. У проводящих материалов сопротивление невелико, а у изоляторов оно высоко.

Сопротивление обозначают латинской буквой *R*. Единицей измерения сопротивления является Ом, обозначается греческой буквой омега (*Ω*).

Термин *сопротивление* используется в основном применительно к электрическим цепям с постоянным током. Сопротивление движению электронов в цепях с переменным током называют полным сопротивлением, либо *импедансом*. Импеданс обозначается латинской буквой *Z*. Так же, как и сопротивление, единицей измерения импеданса является Ом, обозначается греческой буквой омега (*Ω*).

Практическое задание. Измерение сопротивления
В этой лабораторной работе читатель научится измерять сопротивление и продолжит свое знакомство с мультиметром.

Электрический ток

Электрический ток — это перемещение заряда, которое вызвано движением электронов. Если напряжение (электрическое поле) приложено к объекту и существует путь для электрического тока, электроны перемещаются от отрицательного полюса (который отталкивает их) вдоль существующего пути к положительному полюсу (который притягивает электроны).

Электрический ток обозначают латинской буквой *I*. Единицей измерения величины электрического тока служит Ампер, обозначается латинской буквой *A*, либо аббревиатурой *amp*. Электрический ток величиной один ампер — это такой поток электронов, в котором за одну секунду через проводник проходит единичный заряд. Эту величину можно представить как объем потока электронов, которые проходят по электрической цепи; чем большее количество электронов проходит через поперечное сечение проводника, тем больше величина электрического тока.

Электрический ток от источника постоянного тока (DC) всегда протекает в одном направлении, от негативного полюса к позитивному. Если же электрический ток получен от источника переменного напряжения (AC), то его направление периодически изменяется с течением времени.

Мощность

Если электрический ток можно представить как количество электронов, которые перемещаются через поперечное сечение проводника за единицу времени, а напряжение — как скорость перемещения потока электронов, тогда сочетание этих двух величин соответствует силе электронного потока либо мощности. Единицей измерения мощности служит Ватт (*W*). Мощность рассчитывается как произведение величины электрического тока на приложенное к цепи напряжение ($W = I \times V$). Электрические устройства, такие, как лампы накаливания, моторы и компьютерные блоки питания, всегда маркируются номинальной мощностью, которую они потребляют либо выделяют при работе. При прохождении электрического тока в электрической цепи он выполняет некоторую работу. Например, статическое электричество, имеющее высокое напряжение, может вызвать электрический разряд на расстоянии в дюйм и более. Несмотря на это, ток в таком разряде будет очень мал, он может вызвать шок, но не может нанести повреждения. Стартер автомобиля работает на относительно

невысоком напряжении в 12 Вольт, но при этом он требует больших электрических токов для того, чтобы создать необходимое количество энергии для старта двигателя. Молния представляет собой разряд высокого напряжения и высокого тока, поэтому может нанести большой вред или повреждение.

Электрические цепи

Электрическая цепь подразумевает существование потока электронов, который протекает в замкнутом проводящем контуре. Электрическая цепь должна содержать источник питания (его часто называют источником напряжения) и проводники, которые подключают такой источник к нагрузке. Разность потенциалов вызывает протекание электрического тока, в качестве нагрузки может выступать сопротивление — в нем электрический ток преобразовывается в тепловую энергию. Электрический ток протекает от отрицательного к положительному контакту через электрическую цепь. Знание этих простых фактов позволяет контролировать электрический ток.

Ток, согласно законам физики, протекает через среду с наименьшим сопротивлением. Это свойство используется, например, в заземлении, по которому безопасно стекает паразитный электрический заряд. Если человеческое тело имеет самое меньшее сопротивление из окружающих объектов, которые имеют контакт с заземлением, то разряд тока пройдет через него. Во избежание этого все современное оборудование комплектуется шнурами питания с вилками, которые имеют три штыря, один из них является контактом заземления. Правильно установленное заземление имеет минимальное сопротивление, и оно значительно меньше, чем сопротивление человеческого тела, поэтому с большой вероятностью гарантирует защиту от разряда электрического тока. Под *заземлением* зачастую понимают нулевой уровень напряжения (обычно такое подключение называют *занулением*, поскольку соответствующее значение можно получить при электроизмерениях). Следует помнить, что напряжение создается за счет разнесения электрических зарядов в пространстве, поэтому его измерение проводится посредством подключения измерительного прибора к двум точкам цепи.

Свободнее всего электроны перемещаются в проводниках. Несмотря на то что влажный воздух может выступать в роли проводящего материала для статического электричества, электроны не могут преодолеть воздушную прослойку между одним из полюсов гальванического элемента и недалеко расположенным медным проводником. Электрический ток, или направленное движение электронов, возникает только в цепях, формирующих замкнутую петлю. Такие электрические цепи называются замкнутыми.

На рис. 3.4 изображена простейшая электрическая цепь, которая обычно существует в карманных фонариках. Переключатель представляет собой два конца одного и того же провода, которые могут быть разорваны (ключ открыт) либо сомкнуты (ключ закрыт), для того что бы предотвратить либо разрешить протекание электрического тока в цепи.

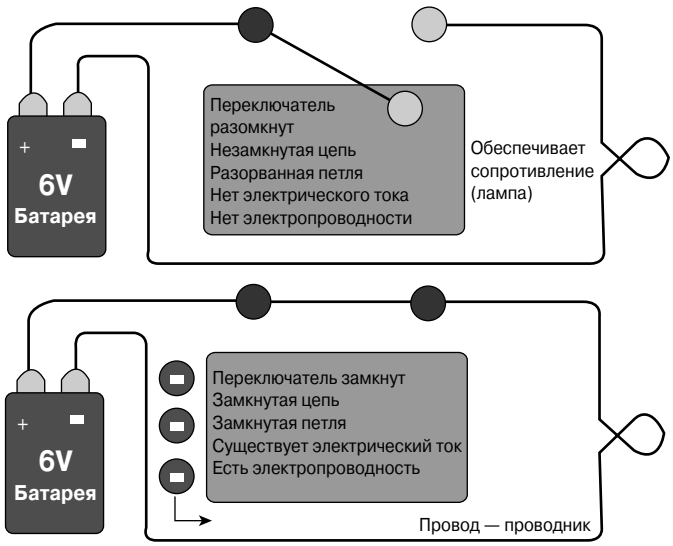


Рис. 3.4. Простейшая последовательная электрическая цепь — карманный фонарь

В верхней части рис. 3.4 схематически показан электрический фонарик, в котором переключатель находится в разомкнутом положении. Химические процессы в батарее вызывают разделение зарядов, что дает напряжение на ее полюсах. Несмотря на это, при разомкнутом ключе нет замкнутой петли для движения электронов, электрический ток не протекает и лампочка фонарика не светится.

В нижней части рис. 3.4 показан тот же фонарик, но уже с замкнутым ключом. В этом случае существует замкнутая цепь для движения электронов, и в цепи протекает электрический ток. Электрическая лампочка препятствует прохождению электронов, нагреваясь и вызывая тем самым выделение энергии в виде светового потока от нити накаливания.

Электрические цепи, участвующие в передаче сигналов по сетевым кабелям, основаны на тех же принципах, что и электрический фонарик, но они намного сложнее. При изучении новых тем, принципов и концепций для лучшего их понимания необходимо проводить параллели с другими схожими примерами. Рассмотренную выше электрическую цепь можно сравнить с потоком воды, который изображен на рис. 3.5. Вода в баке создает давление на уровне крана и заставляет воду вытекать через него. Кран можно представить как переключатель в предыдущем примере. Когда кран закрыт, он не дает воде вытекать из бака. Если же открыть кран, он даст возможность воде вытекать через него, а также будет служить препятствием (аналог сопротивления) для движения водного потока, поскольку чем меньше открыт кран, тем меньше поток воды, и наоборот. Кроме того, труба представляет собой "замкнутую цепь", через которую с помощью помпы воду закачивают обратно в резервуар.

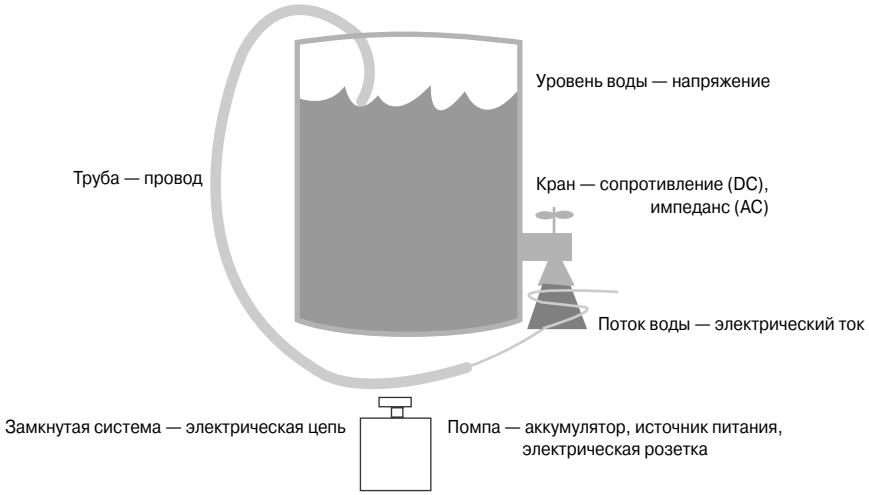


Рис. 3.5. Поток воды как аналог движения электронов

Три основные характеристики электрических цепей тесно взаимосвязаны друг с другом: напряжение (V) равно произведению тока (I) на сопротивление (R) электрической цепи. Формально это соотношение записывается в виде формулы $V = I \times R$[1], которая называется законом *Ома* — по имени ученого, который ее открыл.

Существуют две разновидности тока: переменный (AC — alternating current) и постоянный (DC — direct current). Когда в цепи используется переменный ток, это означает, что полярность источника питания плавно меняется по синусоидальному закону с течением времени, т.е. меняется направление протекания тока — сначала ток течет в одном направлении, потом плавно изменяет свое направление на противоположное, и так с определенной периодичностью.

Постоянный ток течет в одном направлении, и полярность источника питания (напряжения) всегда одинакова и с течением времени не изменяется. Один контакт всегда будет положительным, другой — отрицательным. В линиях питания электрическая энергия всегда передается в виде переменного тока, поскольку именно такой способ передачи электричества на дальние расстояния вызывает меньшие потери мощности и экономически более эффективен. Источники постоянного тока в виде батареек и аккумуляторов широко используются в бытовых целях (например, в карманных фонариках). Переменный ток с помощью выпрямителей в блоках питания преобразовывается в постоянный в бытовой и промышленной аппаратуре.

Практическое задание 3.1.5. Электрические цепи
В этой практической работе необходимо создать несколько электрических цепей и проанализировать их основные параметры.

[1] *В отечественной литературе принято обозначать напряжение латинской буквой U. — Прим. ред.*

Спецификации кабелей

Спецификации, либо *стандарты*, представляют собой набор повсеместно используемых правил и полезных общепринятых методов выполнения кабельных работ. Например, стандарт эталонной модели OSI помогает обеспечить совместимость сетевых устройств во всем мире и позволить им взаимодействовать друг с другом. Большинство стандартов построения кабельных систем помогают обеспечить взаимодействие между системами, их безопасность и высокую производительность.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers — IEEE) утверждает спецификации, или стандарты, построения кабельных систем локальных сетей. Спецификация IEEE 802.3 является стандартом для сетей Ethernet, а IEEE 802.5 — стандарт для построения сетей на основе технологии Token Ring. Лаборатория по технике безопасности (Underwriters Laboratories) разрабатывает стандарты, которые в первую очередь связаны с безопасностью телекоммуникационных структур.

Ассоциация промышленности средств связи (Telecommunications Industry Associastion — TIA) и *ассоциация электронной промышленности (Electronics Industries Association — EIA*) совместно разрабатывают стандарты для построения кабельных систем, семейство которых называется TIA/EIA. Ниже приведены примеры некоторых стандартов из набора TIA/EIA.

- **Спецификация TIA/EIA 568-A** представляет собой стандарт телекоммуникационной кабельной структуры офисного здания. Она описывает минимальные требования к кабельной системе, рекомендуемую топологию и ограничения по длине кабелей, указывает спецификации среды передачи данных и производительность каналов между сетевым аппаратным обеспечением, а также задает параметры используемых разъемов и правила их распайки.
- **Спецификация TIA/EIA 568-B** представляет собой общий стандарт кабельной системы. В этом стандарте указаны компоненты и передаточные характеристики сетевой среды. В стандарте TIA/EIA 568-B.1 описана “обобщенная” кабельная телекоммуникационная структура офисного здания, которая способна взаимодействовать с различным оборудованием разных производителей. Стандарт TIA/EIA 568-B.1.1 является приложением, в котором описано применение восьмипроводной неэкранированной витой пары (Unshielded Twisted-Pair — UTP) и экранированной витой пары (Screened Twisted-Pair — ScTP), а также указаны радиусы изгиба соединительного кабеля обоих типов. Â ñтандарте TIA/EIA 568-B.1.1 описаны компоненты кабельной системы, моделирование процессов передачи и кабельных систем и указаны измерительные процедуры, которые используются для проверки кабелей. Спецификация TIA/EIA 568-B.2.1 является приложением, в котором перечислены требования к кабельным системам на основе витой пары категории 6. В стандарте TIA/EIA 568-B.3. описаны компоненты и передаточные функции оптоволоконных кабельных систем.

- **Спецификация TIA/EIA 569-B** представляет собой стандарт, описывающий кабелепроводы и маршруты прокладки кабеля кабельной структуры офисного здания. Она описывает оборудование, принципы дизайна и методы построения опорных структур для прокладки кабеля как внутри, так и вне зданий.
- **Спецификация TIA/EIA 606-A** представляет собой стандарт управления телекоммуникационной кабельной структурой офисного здания и содержит правила маркировки кабелей. Именно в этом стандарте указано, что каждая конечная точка или порт оборудования должны быть промаркированы уникальным идентификатором. В этом стандарте также перечислены требования к документации по сети и описано, как поддерживать записи в административных журналах в актуальном состоянии.
- **Спецификация TIA/EIA 607** является стандартом, который описывает правила заземления кабельных оболочек или брони кабельной системы офисного здания. Она учитывает особенности различных типов оборудования многих производителей, в частности, указывает общепринятые методы безопасной установки устройств в серверной комнате потребителя. В этом стандарте четко описаны стандартные точки заземления в здании, конфигурации заземления телекоммуникационного оборудования и требования к стандартной оснастке офиса, которые позволят обеспечить стабильную и безопасную работу сетевых устройств.

Спецификации TIA/EIA организации оказывают большое влияние на стандарты сетевой среды передачи данных и включают в себя стандарты горизонтальной и опорной (так называемой вертикальной) кабельных систем, кабельных узлов и комнат с оборудованием, рабочих мест и точек присутствия операторов связи или провайдров услуг. Стандарты TIA/EIA позволяют разработчикам планировать локальную сеть и устанавливать сетевое оборудование независимо от типа устройств, необходимых для обеспечения ее работоспособности.

Стандарт TIA/EIA-568-B описывает правила построения горизонтальных кабельных систем, в которых кабели соединяют розетки рабочих мест с кабельными узлами. Существуют пять категорий кабеля (от CAT 1 до CAT 5), но, согласно стандарту TIA/EIA-568-B, для компьютерных сетей можно использовать только кабели трех категорий: CAT 3, CAT 4, CAT 5. Наиболее часто используется витая пара пятой категории (CAT 5). Новейшие стандарты разрабатываются для витой пары новых категорий CAT 5e и CAT 6; в процессе разработки находится новый стандарт для витой пары, CAT 7. Новые стандарты содержат некоторые полезные усовершенствования по сравнению со стандартами для кабеля пятой категории и должны вскоре стать общепринятыми.

Спецификация TIA/EIA-568-B предполагает укладку как минимум двух кабелей к каждой розетке в рабочей области:

- телефонный кабель для передачи голоса;
- кабель компьютерной сети для передачи данных.

Телефонный кабель должен быть двухпарным кабелем UTP с правильными соединителями либо разъемами. Сетевой кабель и его терминаторы должны удовлетворять одной из следующих спецификаций:

- двухпарный кабель STP с сопротивлением 150 Ом (локальные сети Token Ring);
- четырехпарный кабель UTP с сопротивлением 100 Ом (локальные сети Ethernet);
- оптический кабель 62,5/125 мкм (локальные сети Ethernet);
- коаксиальный кабель (очень редко используется для новых подключений и, вероятно, будет удален из этого списка при первом же обновлении стандарта).

Несмотря на то что коаксиальный кабель RG-6 с сопротивлением 75 Ом не входит в данный стандарт, он может быть использован для подключения кабельного телевидения, если такая необходимость существует.

Стандарт также описывает максимальную длину кабелей UTP, соединяющих розетку на рабочем месте и кабельный узел. В спецификации указана длина кабеля, которым компьютер должен быть соединен с розеткой (так называемый соединительный кабель, patch cord), она составляет 3 м. Максимальная длина кабеля, соединяющего розетку на рабочем месте и *коммутационную панель* телекоммуникационного узла, не должна превышать 90 м. Длина кабеля, соединяющего коммутационную панель и горизонтальную коммутационную систему в кабельном чулане, не должна превышать 6 метров[2]. Таким образом, стандарт гарантирует, что общая длина кабеля не будет превышать 100 м.

Спецификации кабелей технологии Ethernet включают в себя следующие стандарты:

- 10BASE-T;
- 10BASE5;
- 10BASE2.

Спецификация 10BASE-T описывает среду, которая работает на скорости 10 Мбит/с. Она описывает узкополосный принцип передачи (ключевое слово BASE в названии) и требует использования витой пары (символ T в названии означает “twisted” — витая).

Спецификация 10BASE5 также описывает среду, которая работает на скорости 10 Мбит/с и использует узкополосный метод передачи. Цифра “5” в названии свидетельствует о том, что кабель может переносить сигнал приблизительно на расстояние 500 м; если кабель превышает это ограничение, то сигнал необходимо усиливать, иначе он не будет правильно распознан приемником. Кабель стандарта 10BASE5 зачастую называют *толстым коаксиалом*, хотя в действительности это название применимо к определенному типу сети, а кабель называют согласно названию его стандарта.

---

[2] *Согласно самому новому стандарту, длина каждого из двух соединительных кабелей должна составлять 5 м, а не 3 и 6 м, как раньше. — Прим. ред.*

Спецификация 10BASE2, как и две предыдущих, указывает на то, что используется десятимегабитовая среда с узкополосной передачей сигналов. Цифра “2” в названии спецификации указывает на то, что сигнал может быть передан на расстояние до 200 м; если диаметр сети больше, то необходимо использовать повторители, чтобы усилить и очистить сигнал от шумов. Кабель стандарта 10BASE2 зачастую называют *тонким коаксиалом*, хотя в действительности так называется сеть, которая построена на основе такого кабеля, а кабель называют согласно названию его стандарта.

Коаксиальный кабель

Коаксиальный кабель, который показан на рис. 3.6, состоит из четырех основных компонентов:

- медного проводника;
- пластикового изолятора;
- переплетенного медного экрана;
- внешней оболочки.

В центре кабеля помещен толстый медный проводник; его окружает гибкий пластиковый изолятор, который, в свою очередь, завернут в металлическую фольгу либо оплетен медным экраном. Внешний экран либо фольга выступают в качестве второго проводника в кабеле. Они используются как экран для внутреннего проводника и защищают его от внешних помех. Весь кабель помещен во внешнюю оболочку, которая защищает его от механических повреждений. Разъем для соединения коаксиального кабеля называется BNC-разъемом (сокращение от British Naval Connector, либо Bayonet Neill Concelman — миниатюрный байонетный соединитель).

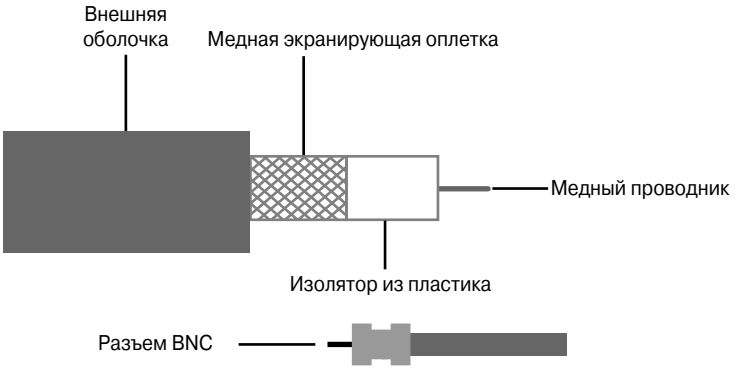


Рис. 3.6. Коаксиальный кабель

В прошлом коаксиальный кабель был наиболее популярен для построения локальных сетей (LAN), поскольку он предоставлял несколько существенных преимуществ разработчику сети. Такой кабель можно было использовать с меньшим

количеством повторителей на далекие расстояния между сетевыми устройствами, чем кабели STP и UTP. Коаксиальный кабель стоит дороже, чем неэкранированная витая пара, но он дешевле оптического кабеля. Технология на основе коаксиального кабеля очень хорошо изучена, т.к. она использовалась на протяжении многих лет в различных структурах для передачи данных. Например, коаксиальный кабель широко применяется для подсоединения к системам домашнего кабельного телевидения и высокоскоростного доступа в сеть Internet. Для кабельного телевидения внутри домов чаще всего используется кабель RG-59, диаметр центрального проводника которого равен 20 AWG. Кабель RG-6 используется для соединения домов с колодцами, потому как имеет более надежную защиту и диаметр центрального проводника 18 AWG. Для магистральных соединений колодцев в пределах города используют более жесткий кабель RG-11 с сечением центрального проводника 14 AWG.

Работая с кабелем, нужно принимать во внимание его размер. При увеличении диаметра центрального проводника увеличивается сложность работы с ним, поскольку кабель должен быть проложен через существующие колодцы и трубы, размер (или, как говорят специалисты по укладке кабеля, кабельная емкость) которых ограничен. Коаксиальный кабель бывает разных размеров. Наибольший диаметр (1 см) рекомендован для использования в *опорной сети* Ethernet, потому что он может быть использован для передачи данных на большие расстояния и менее чувствителен к внешним помехам, чем остальные типы кабеля. Этот тип обычно называют *толстым* коаксиальным кабелем; его внешний вид показан на рис. 3.7. Как следует из названия, толстый коаксиальный кабель очень жесткий и прост в установке в некоторых ситуациях именно из-за своей жесткости. Основное правило специалиста по разработке сетей гласит, что чем труднее укладывать кабель, тем дороже будет стоить его прокладка. Коаксиальный кабель дороже с точки зрения его прокладки, чем витая пара. Толстый коаксиальный кабель на сегодняшний день практически не используется, за исключением некоторых специфических случаев.

Рис. 3.7. Толстый коаксиальный кабель

Коаксиальный кабель, диаметр центрального проводника которого равен 0,35 см, иногда называемый *тонким* коаксиальным кабелем, также широко используется в сетях, работающих на основе технологии Ethernet. Тонкий коаксиальный кабель, который показан на рис. 3.8, весьма пригоден для построения кабельных систем, в которых часто встречаются изгибы и повороты кабелепроводов. Поскольку кабель очень легко устанавливать, его укладка достаточно дешева. Поэтому такой кабель иногда называют *дешевым коаксиальным кабелем*.

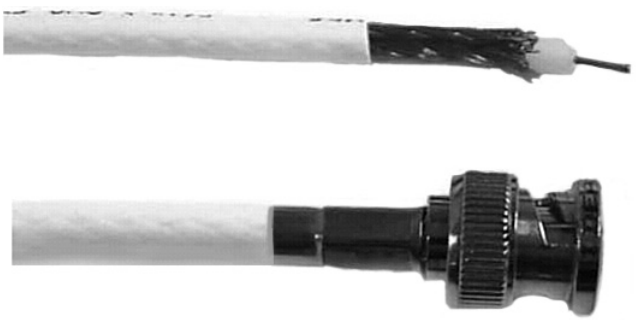


Рис. 3.8. Тонкий коаксиальный кабель

Несмотря на все, что было сказано выше, в обоих типах коаксиального кабеля внешний проводник должен быть тщательно и правильно заземлен, что несколько усложняет его использование. Из-за такого недостатка коаксиальный кабель практически не используется на сегодняшний день в сетях на основе технологии Ethernet.

Несмотря на указанный выше недостаток, в большинстве сетевых топологий с общей шиной во всем мире широко используется коаксиальный кабель. Организация IEEE не рекомендует использовать этот кабель либо соответствующую топологию как стандарт для сетей Ethernet. Почти все новые локальные сети построены на основе топологии расширенной звезды Ethernet и комбинируют кабель UTP и оптическое волокно.

Основные свойства коаксиального кабеля:

- **пропускная способность** составляет от 10 до 100 Мбит/с;
- **средняя стоимость узла** невысока;
- **размеры кабеля и контактных разъемов** средние;
- **максимальная длина кабеля** не должна превышать 500 м (средний показатель максимальной длины).

Дополнительная информация: огнеупорный кабель

Огнеупорный кабель предназначен для прокладки в вентиляционных структурах здания. При возведении здания создаются вентиляционные пространства, которые являются отдельными выделенными пространствами, используемыми для нагревания, вентиляции и кондиционирования воздуха. Обычно вентиляционное пространство расположено между стационарными перекрытиями и подвесными потолками зданий. В зданиях, где установлены компьютеры, вентиляционное пространство часто используется для прокладки различных кабельных систем. Исходя из того, что обычный кабель выделяет токсичные вещества при возгорании, для построения кабельных систем в вентиляционных нишах необходимо использовать специальный огнеупорный кабель.

Обшивка огнеупорного кабеля сделана из специализированного материала, тефлона (Teflon), и такой кабель стоит дороже, чем обычный. Этот материал очень плохо горит и при воздействии на него огня выделяет намного меньше дыма, чем оболочка обычного кабеля. Оба типа кабеля, коаксиальный и витая пара, встречаются в огнеупорном варианте.

Дополнительная информация: американская система оценки проводов (AWG)

Диаметр проводов или проводников в кабелях измеряется с использованием Американской системы оценки проводов (American Wire Gauge System — AWG). Система AWG является предпочтительным стандартом для измерения диаметра медных и алюминиевых проводников. Диаметр проводников в кабелях, разведенных по жилым домам, равен 12 либо 14 AWG. Диаметр проводников, из которых состоит неэкранированная витая пара (UTP), использующаяся в большинстве абонентских каналов (от точки присутствия до дома или офиса), находится в пределах от 19 до 26 AWG. Диаметр более новых телефонных линий лежит в пределах от 22 до 26 AWG, но самыми распространенными являются проводники диаметром 24 AWG. Меньшее значение AWG соответствует более толстому проводнику. Утолщенные провода имеют меньшее сопротивление и могут пропускать большие электрические токи, и, как следствие, их использование позволяет получить лучшее качество сигнала на больших расстояниях. Проводу размером 24 AWG соответствует диаметр в 1/24 дюйма.

Витая пара

Типичным кабелем, использующимся в телефонных сетях и современных сетях Ethernet, является витая пара. Пара проводников формирует электрическую цепь, по которой передаются данные. В этом кабеле проводники одной пары переплетены и перекручены, для того чтобы обеспечить защиту от *наводок* — помех, создаваемых соседними парами.

Проводники в паре переплетены по двум причинам. Первая из них заключается в том, что когда по проводнику протекает электрический ток, он создает вокруг проводника магнитное поле, которое может накладываться на сигнал, который проходит по соседней паре (наводки). Для того чтобы избавиться от такого рода помех, проводники, которые переносят сигналы в разных направлениях, и, соответственно, создают магнитные поля разных знаков, переплетаются. Результатом такого переплетения является взаимная компенсация магнитного поля. Такой эффект обычно называют *гашением* либо *компенсацией*. Переплетение пары позволяет проводникам одной пары всегда оставаться вместе, а также добиться компенсации полей по всей длине кабеля.

Вторая причина заключается в том, что по витой паре данные передаются с использованием двух проводников. Сигналу, который передается по одному из проводников, соответствует "зеркальный" сигнал, передаваемый по второму проводнику. Такие сигналы называются *разностными*. Если же проводники переплетены, тогда помехи и в одном, и во втором проводниках будут одинаковы. Когда приемник получит оба сигнала, один из них инвертируется (вместе с шумом), и результат сравнивается. Таким образом, получатель может отфильтровать помехи, поскольку они компенсируют друг друга.

Наиболее распространены два типа витой пары: экранированная (Shielded Twisted-Pair — STP) и неэкранированная (Unshielded Twisted-Pair — UTP). Рассмотрим детально оба типа витой пары.

Экранированая витая пара (STP)

Экранированная витая пара (STP) состоит из четырех пар тонких медных проводников, покрытых изолятором соответствующих цветов и перекрученных между собой. Каждая пара экранирована металлической фольгой, и все четыре пары также оплетены металлической нитью либо фольгой. Такой кабель, как и все другие, поверх общего экрана покрыт внешней оболочкой из пластика. Кабель витой пары показан на рис. 3.9.

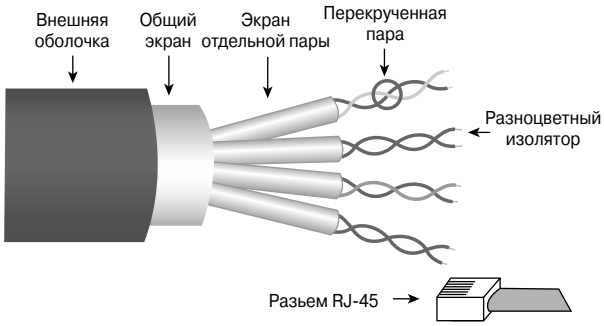


Рис. 3.9. Кабель экранированной витой пары

Защищенная витая пара (Screened twisted-pair — ScTP) является одной из разновидностей кабеля STP. По своему строению она идентична экранированной витой паре, за исключением того момента, что в ней отсутствуют экраны для отдельных пар, как показано на рис. 3.10. Экраны в обоих типах витой пары (STP и ScTP) уменьшают внешние электрические помехи. Это обеспечивает преимущество экранированной витой пары перед неэкранированным кабелем.

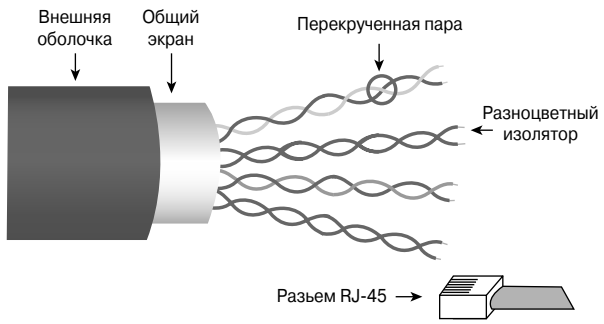


Рис. 3.10. Защищенная витая пара (ScTP)

Тем не менее, экранированный кабель более сложен в использовании, чем неэкранированный, потому как его экран должен быть заземлен. Неправильно используемый кабель защищенной витой пары очень чувствителен к помехам, поскольку его экран в таком случае выступает в роли антенны, которая улавливает нежелательные

сигналы и помехи. Кабели STP и ScTP не могут использоваться для передачи сигналов на такие большие расстояния, как коаксиальный либо оптический кабель, без применения повторителя. Изоляция и экранирование значительно увеличивают размеры, вес и стоимость кабеля. Несмотря на перечисленные недостатки, экранированный медный кабель широко используется для построения структурированных кабельных сетей в Европе.

Основные свойства экранированной витой пары:

- **пропускная способность** составляет от 10 до 100 Мбит/с;
- **средняя стоимость из расчета на одно рабочее место** — умеренная;
- **размеры кабеля и разъема для соединения** средние;
- **максимальная длина кабеля** — 100 м (относительно невелика).

Неэкранированная витая пара

Неэкранированная витая пара (Unshielded Twisted-Pair — UTP) — наиболее распространенный кабель для построения сетей. Он состоит из четырех пар тонких медных проводников, покрытых изолятором соответствующих цветов и переплетенных между собой, как показано на рис. 3.11. Витые пары завернуты в пластиковый кожух. Разъем, использующийся для соединения неэкранированной витой пары, носит название зарегистрированного разъема 45 (Registered Jack 45 — RJ-45). Внешний вид такого разъема приведен на рис. 3.12.

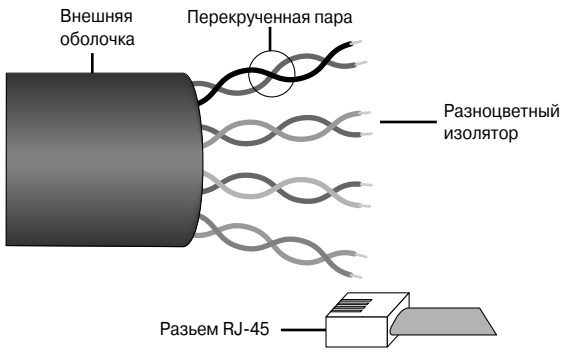


Рис. 3.11. Неэкранированная витая пара

Неэкранированная витая пара (UTP) имеет множество преимуществ. Она довольно тонка и не требует заземления, что упрощает ее укладку и установку. Небольшие размеры этой витой пары позволяют уместить большее количество кабелей UTP в ограниченном пространстве, чем любого другого медного кабеля. Неэкранированная витая пара является наиболее дешевой разновидностью сетевой среды передачи данных, и ее соединительные разъемы очень легки в установке. Она поддерживает те же скорости передачи данных, что и остальные типы медных кабелей.

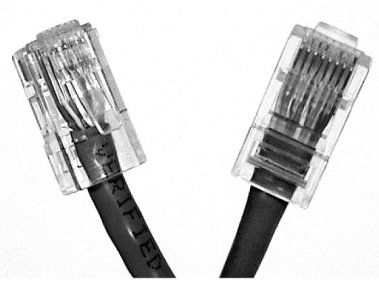


Рис. 3.12. Разъем RJ-45

Основным недостатком неэкранированной витой пары (UTP), в сравнении с другими сетевыми средами передачи данных, является ее восприимчивость к электрическим помехам и наложению сигналов. Т.к. кабель UTP лишен экрана, уменьшения помех в этом типе кабеля можно добиться только за счет эффекта погашения (компенсации) и использования разностных сигналов. Второй недостаток UTP заключается в малой максимальной длине кабеля, которая меньше, чем у коаксиального либо оптического кабелей.

Несмотря на то что ранее кабель UTP использовался для построения низкоскоростных сетей передачи данных, в настоящее время он широко применятся для построения высокоскоростных сетей на основе медных проводников.

Основные свойства неэкранированной витой пары:

- **пропускная способность** составляет от 10 до 1000 Мбит/с;
- **средняя стоимость из расчета на одно рабочее место** — минимальная;
- **размеры кабеля и разъема для соединения** — малые;
- **максимальная длина кабеля** — 100 м (относительно невелика).

Широко используются следующие разновидности кабелей UTP:

- **кабель категории 1 (Category 1 — CAT 1)** используется для телефонных коммуникаций, непригоден для построения сетей передачи данных;
- **кабель категории 2 (Category 2 — CAT 2)** обеспечивает максимальную скорость передачи данных — до 4 Мбит/с;
- **кабель категории 3 (Category 3 — CAT 3)** используется в сетях 10BASET Ethernet. Обеспечивает передачу данных на скоростях вплоть до 10 Мбит/с;
- **кабель категории 4 (Category 4 — CAT 4)** используется в сетях Token Ring. Обеспечивает передачу данных на скоростях до 16 Мбит/с;
- **кабель категории 5 (Category 5 — CAT 5)** поддерживает скорость передачи данных до 100 Мбит/с. Используется в сетях, построенных на базе технологии Fast Ethernet;

- **кабель категории 5e (Category 5e — CAT 5e)** используется для построения сетей на основе технологии Gigabit Ethernet (GigE). Максимальная скорость передачи данных в таком кабеле составляет до 1000 Мбит/с (1 Гбит/с);
- **кабель категории 6 (Category 6 — CAT 6).** Спецификация витой пары данной категории выпущена 3 февраля 2003 г. и является достаточно новой. Кабель 6-й категории используется для построения сетей на основе технологии Gigabit Ethernet (GigE).

Кабели категории 5 и выше содержат в себе четыре пары многожильных медных проводников с сечением 24 AWG. Более старые сети передачи данных используют кабели категории 3 для передачи голоса и категории 5 — для передачи данных. Более новые сети используют минимум категорию 5e для передачи голоса и данных. Несмотря на то что стоимость витой пары последнего типа немного выше, кабель этой категории может быть использован для создания более длинных соединений.

Для сравнения кабелей UTP и STP следует учитывать следующие их особенности:

- скорость передачи данных по обоим типам кабелей достаточна для построения локальных сетей (LAN);
- кабель UTP менее дорогой, чем STP. Кабель UTP является самым дешевым из своих аналогов для построения сетей передачи данных, и в целом витая пара — недорогое решение для локальной сети;
- поскольку в большинстве строений уже присутствует развитая инфраструктура кабелей UTP, было адаптировано много стандартов передачи данных для использования существующей проводки, чтобы не заменять ее альтернативным кабелем. Следует помнить тот факт, что уровень категории соответствует максимальной пропускной способности кабеля. Например, в здании, в котором проложена витая пара категории 3, не может быть использована технология Fast Ethernet, для которой необходим кабель как минимум категории 5.

Практическое задание 3.1.9a. Простые цепи
В этом задании необходимо создать простые электрические цепи и изучить их свойства.

Практическое задание 3.1.9b. Тестирование кабелей с помощью тестера Fluke 620
Выполнив эту лабораторную работу, вы научитесь пользоваться простым кабельным тестером для проверки прямого либо перекрестного кабеля на работоспособность. Вы также научитесь пользоваться тестером Fluke 620 с расширенными возможностями для определения длины кабелей и для проверки правильности распайки пар на разных концах кабеля.

Практическое задание 3.1.9c. Создание прямого кабеля
Выполнив эту лабораторную работу, вы научитесь создавать кабели для соединения сетевых устройств Ethernet на основе витой пары категории 5 или 5e. Вы также протестируете полученный кабель на наличие обрывов и определите правильность распайки пар на разных его концах.

Практическое задание 3.1.9d. Создание консольного кабеля
Выполнив эту лабораторную работу, вы научитесь создавать консольный кабель на основе витой пары категории 5 или 5e. Вы также протестируете полученный кабель на наличие обрывов и определите правильность распайки пар на разных его концах.

Практическое задание 3.1.9e. Создание перекрестного кабеля
Выполнив эту лабораторную работу, вы научитесь создавать перекрестный кабель для соединения устройств Ethernet на основе витой пары категории 5 или 5e согласно стандартам TIA-568-B и TIA-568-A. Вы также протестируете полученный кабель на наличие обрывов и определите правильность распайки пар на разных его концах.

Практическое задание 3.1.9f. Выбор и приобретение кабеля UTP
Выполнив эту лабораторную работу, вы ознакомитесь с различными типами кабелей и связанными с ними компонентами, а также с их ценами на рынке. В этой лабораторной работе прежде всего рассмотрены бухты кабеля и соединительные кабели.

Оптическая среда передачи данных

Оптоволоконный кабель широко распространен и используется для передачи данных с высокой скоростью между двумя точками на довольно большие расстояния, например, в магистралях локальных сетей, а также в распределенных сетях (Wide-Area Network — WAN).

Основные причины использования оптоволоконных кабелей:

- оптическое волокно не чувствительно к разрядам молний, не подвержено электромагнитным помехам или перекрестным наводкам. Оно также не создает электромагнитного излучения;
- пропускная способность оптоволоконных каналов больше, чем любых других сред передачи данных;
- используя оптоволоконные каналы, можно передавать данные на достаточно большие расстояния и при этом получать хорошее качество сигнала за счет его очень малого затухания;
- передача данных по оптоволоконным каналам связи наиболее безопасна по той причине, что очень трудно вклиниться в существующий оптоволоконный канал и очень легко обнаружить вторжение в него;
- существующие приемники и передатчики можно заменить на более совершенные недавно разработанные устройства и достичь большей пропускной способности уже существующих оптоволоконных соединений без замены оптического волокна;
- оптоволоконные соединения дешевле медных, если использовать их для передачи данных на большие расстояния;
- оптические волокна изготавливаются из песка, недорогого материала, широко распространенного на Земле;

- оптоволоконные каналы не требуют заземления, в отличие от электрических каналов связи;
- оптические волокна имеют очень маленькую массу и просты в установке;
- оптические волокна более стойки к окружающим факторам, например, к воздействию влаги, в отличие от медных проводников;
- длина оптоволоконных соединений может быть легко увеличена для передачи данных на достаточно большие расстояния.

Если необходима большая пропускная способность канала на расстояния больше 100 м, рекомендуется использовать оптоволоконный канал передачи данных.

В этом разделе рассмотрены основные принципы работы *оптоволоконного кабеля*. Далее мы расскажем о том, каким образом волокно переносит световой сигнал на большие расстояния, а также опишем, какие типы кабеля используются, каким образом они монтируются, какие разъемы и оборудование используется совместно с оптоволокном и как проверяют работоспособность оптических соединений.

Спектр электромагнитных волн

Лучи света, которые используются в оптоволоконных кабелях, — это разновидность электромагнитной энергии. Электрические заряды, которые движутся с ускорением, либо их колебания приводят к выделению энергии в виде электромагнитного излучения. Электромагнитная энергия в виде световых волн может распространяться через вакуум, воздух и некоторые материалы, такие, как, например, стекло. Важной характеристикой электромагнитных волн является их *длина волны* (рис. 3.13).

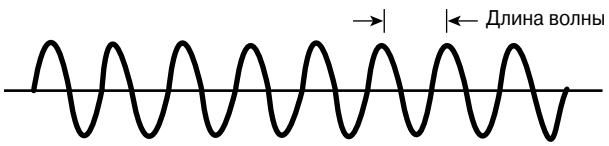


Рис. 3.13. Длина волны

Радио-, микроволны, радар, видимый свет, рентгеновские и гамма лучи кажутся совершенно разными вещами, но на самом деле это все лишь различные типы электромагнитной энергии. Если все формы электромагнитной энергии расположить в порядке убывания длины волны, мы получим *электромагнитный спектр*, который показан на рис. 3.14.

Длина волны электромагнитного излучения определяется частотой колебаний электрического заряда, который излучает эти волны. Например, если колебания заряда происходят медленно, то такой заряд излучает длинные волны. Визуально движение электрических зарядов и излучаемые волны можно представить себе как движение палки в водоеме. Если медленно двигать палкой вперед и назад, на воде возникнут волны с большим расстоянием между их вершинами. Если же палкой двигать в более быстром темпе, тогда расстояние между вершинами волн уменьшится.

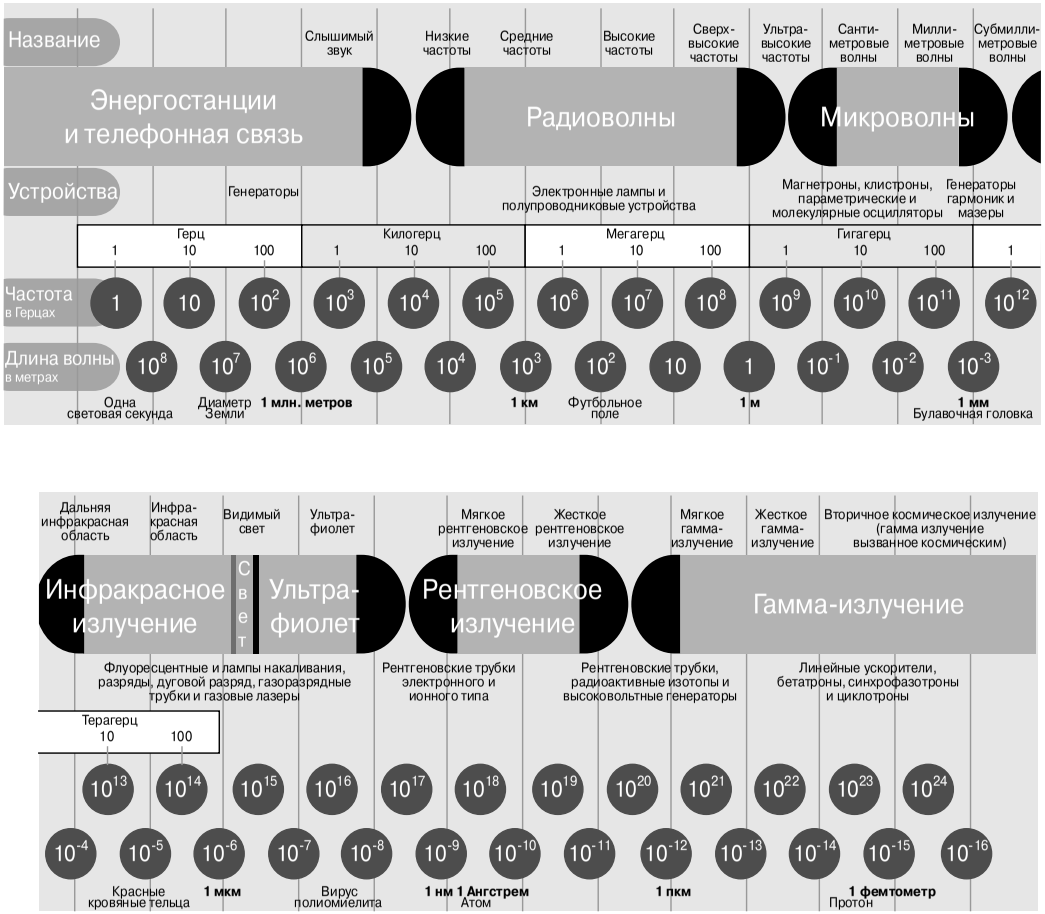


Рис. 3.14. Электромагнитный спектр

Все электромагнитные волны излучаются единым образом, поэтому все они имеют одинаковые свойства. Например, скорость распространения любых электромагнитных волн в вакууме равна 300 000 км/с, либо 186 000 миль/с. Такую скорость называют скоростью света.

Человеческий глаз способен воспринимать электромагнитную энергию с длиной волны в диапазоне от 700 до 400 нанометров. Нанометр равен одной миллиардной части метра (0,000000001 м), обычно его обозначают как нм. Электромагнитное излучение, длина волны которого находится в пределах между 700 нм и 400 нм, называют *видимым светом*. Излучение, длина волны которого находится в районе 700 нм и выше, имеет красный цвет. А излучение с длиной волны 400 нм и меньше имеет фиолетовую окраску. В средней части видимого электромагнитного спектра цвета распределены точно так же, как в радуге.

Для передачи данных через оптические волокна используются длины волн, которые невидимы для человеческого глаза. Длина этих волн немного превосходит длину волны видимого света. Такие волны называются *инфракрасным излучением*. Инфракрасные волны часто используются в бытовой технике, например, пультах дистанционного управления. Основные значения длин волн, используемых для передачи данных по оптоволоконным каналам:

- 850 нм;
- 1310 нм;
- 1550 нм.

Эти длины волн выбраны потому, что они лучше распространяются через оптоволоконные каналы, чем остальные.

Лучевая модель света

Электромагнитное излучение, в том числе и видимый свет, излучаемое некоторым источником, распространяется по прямым линиям. Такие линии называются *световыми лучами*.

Представьте себе узкий пучок света, такой, как создает лазер. В вакууме свет распространяется прямолинейно со скоростью 300 000 км/с. В любых других физических средах и материалах, таких, как воздух, вода или стекло, скорость распространения световых лучей меньше, чем в вакууме. Если световой луч (который называют *падающим лучом*) пересекает границу перехода из одного вещества (например, воздуха) в другое (например, стекло), небольшое количество энергии светового луча отражается в обратном направлении. По этой причине можно увидеть свое отражение в воде или в зеркале. Световой луч, отраженный от границы двух материалов, называется *отраженным*.

Энергия светового луча, которая не была отражена, проникает в стекло. Входящий луч обычно проникает в стекло под углом к его предыдущему направлению. Такой луч называется *преломленным*. Насколько сильно световой луч преломляется, зависит от двух факторов:

- угла, под которым падающий луч падает на поверхность стекла;
- соотношения скоростей распространения света в двух субстанциях (в рассматриваемом примере: воздух и стекло).

Эффект преломления световых лучей на границе двух сред позволяет им проходить по оптоволоконному кабелю, даже если такой кабель скручен в кольцо.

Насколько сильно световой луч преломляется при проникновении в стекло, определяется оптической плотностью стекла. Оптическая плотность — это параметр, который показывает, насколько медленно свет распространяется в материале. Материал с более высокой оптической плотностью имеет меньшую скорость распространения светового луча. Соотношение скорости света в вакууме к скорости света в материале называют коэффициентом преломления (Index of Refraction — IR) и записывают как:

IR = (скорость света в вакууме)/(скорость света в материале).

Следовательно, мерой оптической плотности является коэффициент преломления материала. Чем больше значение коэффициента преломления материала, тем больше его оптическая плотность и тем меньше скорость распространения света в нем, по отношению к материалу с меньшим коэффициентом преломления.

В табл. 3.2 перечислены коэффициенты преломления для воздуха, стекла, алмаза и воды.

Таблица 3.2. Коэффициенты преломления

Материал	Коэффициент преломления
Воздух	1,000
Стекло	1,523
Алмаз	2,419
Вода	1,333

Для таких материалов, как стекло, коэффициент преломления можно увеличить, если при изготовлении материала добавлять в него различные химические вещества, которые называют примесями. Коэффициент также можно уменьшить, уменьшая количество примесей.

В следующих двух разделах подробно описано *отражение* и *преломление* света, для того чтобы в дальнейшем было легче разобраться в принципах построения и работы оптических устройств и волокон.

Закон отражения света

При падении светового луча на границу раздела двух сред, например, из воздуха на стекло, существуют два луча — отраженный и преломленный, как показано на рис. 3.15. Наличие или отсутствие таких двух лучей зависит от угла, под которым свет падает на границу двух веществ. Угол между падающим лучом и перпендикуляром к поверхности стекла в точке падения называется *углом падения*. Если значение угла падения достигает некоторой величины, называемой критическим углом, то из

двух вышеупомянутых лучей будет существовать только отраженный, как показано на рис. 3.16. Иными словами, вся энергия светового луча отражается от раздела двух сред.

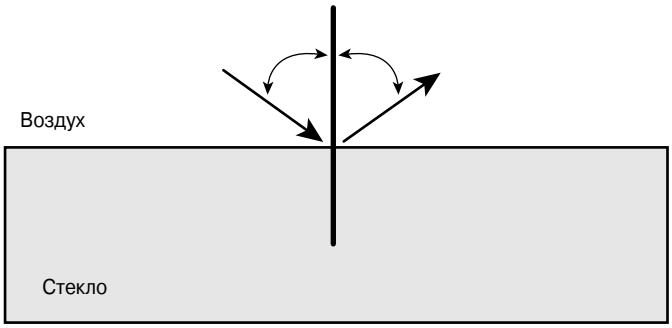


Рис. 3.15. Отражение света

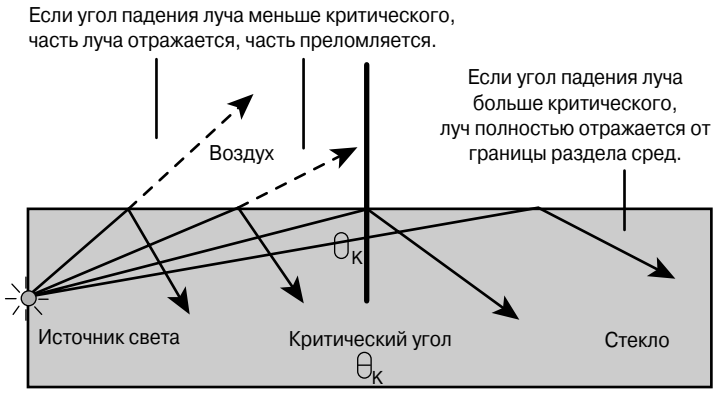


Рис. 3.16. Критический угол

Перпендикуляр к поверхности вещества называется *нормалью*. Нормаль не является световым лучом, она просто помогает измерять углы. Угол между отраженным лучом и нормалью называется *углом отражения* светового луча и равен углу падения. Иными словами, угол, под которым луч света падает на отражающую поверхность, определяет угол, под которым луч будет отражен от поверхности.

Закон преломления света

Когда свет падает на границу раздела двух прозрачных материалов, например, воздуха и стекла, световой луч разделяется на две части. Одна из частей отражается обратно в первый материал (воздух) под углом, называемым углом отражения, который всегда равен углу падения. Оставшаяся часть энергии светового луча пересекает границу раздела материалов и проникает во второй материал (стекло).

Если световой луч падает на поверхность стекла под углом, равным 90 градусам, то он практически полностью проникает в стекло и не преломляется. Если же угол падения не соответствует 90 градусам, тогда луч света, проникший в стекло, отклоняется от своего направления в воздухе. Такое отклонение проникших лучей называется *преломлением*. Насколько сильно отклонится луч, пересекший границу раздела двух материалов, зависит от коэффициентов преломления этих материалов. Если луч света пересекает границу между менее оптически плотным материалом и более оптически плотным , угол преломления будет меньше угла падения (преломленный луч будет приближаться к нормали). Если же луч света будет пересекать эту же границу в обратном направлении, он будет отдаляться от нормали (угол преломления больше угла падения). Преломление светового луча проиллюстрировано на рис. 3.17.

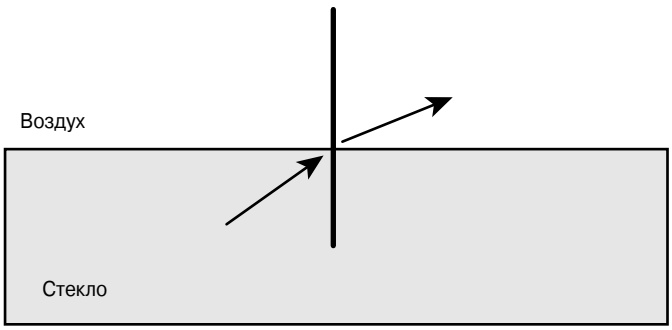


Рис. 3.17. Преломление света

Чтобы лучше понять, как световые лучи проходят границу раздела двух сред под углами, не равными 90 градусам, рассмотрим луч, который по очереди пересекает границу между стеклом и алмазом, а потом между алмазом и воздухом, как показано на рис. 3.18. Коэффициенты преломления стекла и алмаза соответственно равны 1,523 и 2,419. Поэтому преломленный луч в алмазе будет распространяться ближе к нормали (под меньшим углом). После прохождения границы между алмазом и воздухом преломленный луч будет распространяться под бо́льшим углом к нормали, чем в алмазе. Причиной этому будет меньший коэффициент преломления воздуха, который равен 1,000.

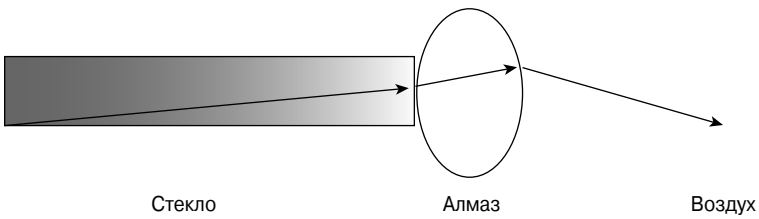


Рис. 3.18. Преломление светового луча на границе раздела двух сред

Полное внутреннее отражение

Передача данных по оптоволоконным каналам происходит путем преобразования единиц и нулей двоичного сигнала в наличие или отсутствие светового потока (сигнала). Такой световой поток должен оставаться внутри оптического волокна, пока не достигнет его второго конца, и не должен проникать в оболочку оптического волокна. Проникновение света в оболочку будет вызывать потерю мощности, а значит, и затухание сигнала. При изготовлении оптических волокон внешнюю поверхность делают близкой по характеристикам к зеркалу, чтобы распространяющиеся в нем световые лучи отражались. Если любой луч, который падает на границу оптического волокна, полностью отражается по направлению к другому концу волокна, то волокно будет хорошим "проводником" или, как обычно говорят, *волноводом* для передачи световых волн (рис. 3.19).

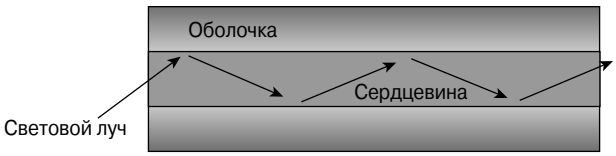


Рис. 3.19. Полное внутреннее отражение

Законы отражения и преломления позволяют изготавливать оптическое волокно для передачи световых лучей с минимальными потерями энергии. Необходимо придерживаться двух требований для полного отражения лучей в оптическом волокне без потерь из-за преломления и выхода сигнала в оболочку:

- сердцевина оптического волокна должна иметь больший коэффициент преломления, чем материал, который окружает ее. Окружающий сердцевину материал называют оболочкой;
- угол падения световых лучей на границу между сердцевиной и оболочкой должен быть больше критического угла.

Если оба требования соблюдены, все падающие лучи света будут отражены внутрь оптического волокна. Этот эффект называется *полным внутренним отражением* и является основой, на которой базируется производство оптических волокон. Эффект полного внутреннего отражения вынуждает световые лучи в оптических волокнах отражаться от границы с сердцевиной и продолжать свой путь ко второму концу волокна. Таким образом, световые лучи, проходя "зигзагообразный" путь в сердцевине волокна, достигают его конца.

Оптические волокна, отвечающие первому условию (коэффициент преломления оболочки меньше, чем у сердцевины), очень просты в изготовлении. Можно контролировать угол падения световых лучей, вводимых в сердцевину. Угол падения ограничен двумя факторами:

- числовой апертурой волокна — набором углов падающих световых лучей, при которых будет наблюдаться эффект полного внутреннего отражения, как показано на рис. 3.20;
- максимальным количеством путей (называемых модами), по которым световые лучи могут распространяться в оптических волокнах.

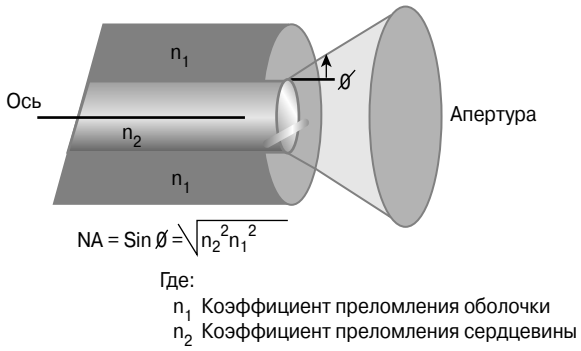


Рис. 3.20. Числовая апертура

Учитывая и контролируя оба указанных фактора, производители выпускают оптические волокна с полным внутренним отражением, которые могут быть использованы для передачи данных на большие расстояния (рис. 3.21).

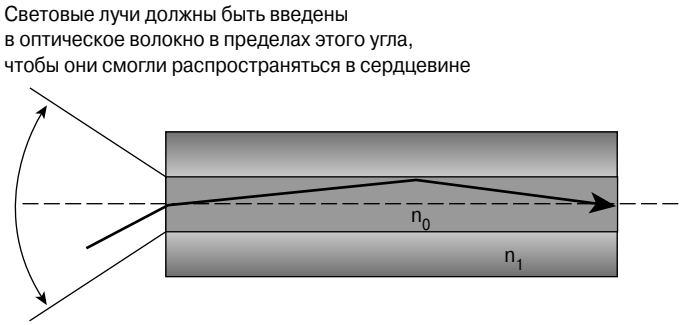


Рис. 3.21. Распространение световых лучей

Дополнительная информация: оптоволоконные кабели

Оптоволоконные кабели — это сетевая среда передачи, в которой используются световые импульсы для передачи данных. Сигналы, которые представляют собой биты данных, преобразовываются в световые импульсы. Специалисту важно понимать, что электричество все же необходимо для создания и интерпретации световых сигналов на конечных устройствах, но в самом оптоволоконном кабеле нет электрических сигналов, в отличие от медных проводников. Следует также отметить, что все компоненты, из которых состоит оптоволоконный кабель, являются хорошими изоляторами, и многие характеристики оптоволоконных кабелей превосходят соответствующие характеристики медных проводников.

Любой оптоволоконный кабель, использующийся для сетевых соединений, содержит два оптических волокна, каждое из которых имеет свою оболочку. Одно волокно переносит сигнал от устройства А к устройству Б, а второе волокно — в обратном направлении, от устройства Б к устройству А. Оптоволоконный кабель для передачи данных в обоих направлениях похож на две улицы с односторонним движением, идущие параллельно навстречу друг другу. Такой механизм передачи данных позволяет создать дуплексное коммуникационное соединение. Аналогично витой паре, которая использует разные пары проводников для передачи данных (Tx — передача) и для приема (Rx — прием), в оптоволоконном кабеле одно волокно используется для передачи, а второе — для приема данных, как показано на рис. 3.22. Обычно такие два волокна находятся в единой внешней оболочке, кроме тех точек, где к ним крепятся соединительные разъемы.

Рис. 3.22. Дуплексное оптическое волокно

В рассматриваемом кабеле два оптических волокна полностью разделены, и нет необходимости экранировать либо переплетать оптические волокна, поскольку вся световая энергия распространяется в сердцевине оптического волокна, а проблема наводок не существует в оптических линиях передачи данных. Наиболее распространенные оптоволоконные кабели состоят из нескольких пар волокон. Такое строение кабеля позволяет соединять одним кабелем телекоммуникационные узлы, этажи либо здания. Один кабель может состоять из 2-х, 4-х, 8-ми, 12-ти, 24-х, 48-ми или более отдельных волокон. При использовании медной среды передачи данных для создания каждого сетевого соединения необходимо проложить отдельный кабель неэкранированной витой пары. Оптические волокна могут работать на более высокой пропускной способности и позволяют передавать данные на большие расстояния, чем медные проводники.

Как показано на рис. 3.23 и 3.24, существуют пять типичных компонентов, из которых состоит оптоволоконный кабель:

- сердцевина;
- оболочка;
- буферный материал;
- армирующий материал;
- внешняя оболочка.

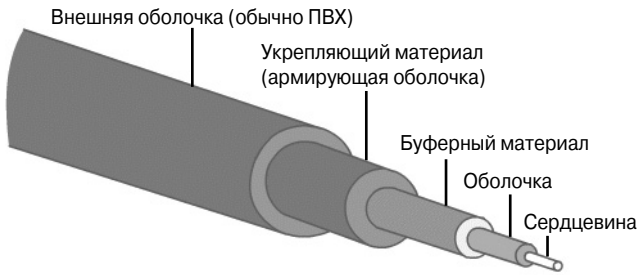


Рис. 3.23. Пять типичных компонентов оптоволоконного кабеля

Средой передачи сигналов в оптическом волокне служит сердцевина, которая расположена в центре волокна и переносит все световые импульсы. Сердцевину обычно изготавливают из кварца (диоксида кремния) или других подобных по характеристикам материалов. Сердцевина покрыта оболочкой, которая также состоит из кварца, но имеет меньшее значение коэффициента

преломления, чем сердцевина. Лучи света, распространяющиеся в сердцевине волокна, отражаются от границы сердцевина-оболочка обратно в сердцевину и продолжают свой путь внутри нее.

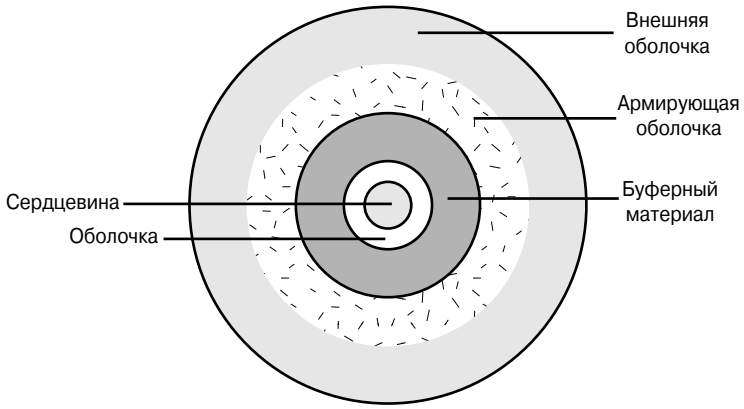


Рис. 3.24. Пять компонентов оптоволоконного кабеля в поперечном разрезе

Оболочку окружает буферный материал, который предохраняет сердцевину и оболочку от физических повреждений.

Армирующий материал, окружающий буфер, предохраняет кабель от растяжений и разломов во время его прокладки. Материал, из которого изготавливают этот слой, называется кевларом (Kevlar). Из кевлара делают пуленепробиваемые жилеты и другие защитные приспособления. Последний элемент — внешняя оболочка — защищает оптическое волокно от стирания, растворения и загрязнения. Состав вещества, из которого изготовлена внешняя оболочка, может изменяться в зависимости от предназначения оптоволоконного кабеля.

Часть оптического волокна, по которой распространяются световые лучи, называют *сердцевиной* оптического волокна. Световые лучи не могут входить в сердцевину под любыми углами, а только под углами, которые лежат в пределах числовой апертуры оптического волокна. Более того, для входящего светового луча в оптическом волокне существует ограниченное количество путей распространения. Такие оптические пути называются модами. Если диаметр сердцевины достаточно большой, в нем может существовать большое количество путей для распространения световых лучей; такое оптическое волокно называют *многомодовым*. В *одномодовом* оптическом волокне диаметр сердцевины настолько мал, что позволяет использовать только один путь (одну моду) для распространения светового луча. Различия между одномодовым и многомодовым оптическими волокнами проиллюстрированы на рис. 3.25.

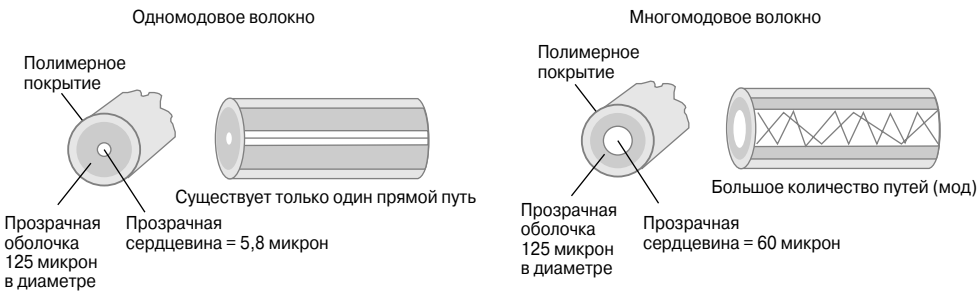


Рис. 3.25. Различия между одномодовым и многомодовым оптическими волокнами

В табл. 3.3 сравниваются характеристики одномодового и многомодового оптических волокон.

Таблица 3.3. Характеристики одномодового и многомодового оптических волокон

	Одномодовое волокно	Многомодовое волокно
Сердцевина	Тонкая сердцевина (10 микрон или менее)	Более толстая сердцевина, чем в одномодовом волокне (50 либо 62,5 микрона или более)
Дисперсия	Малая дисперсия	Большая дисперсия и, как следствие, потери сигнала
Расстояние	Пригодно для соединений на большие расстояния (до 3 км (9842 футов))	Пригодно для соединений на большие расстояния, но меньшие, чем одномодовое волокно (до 2 км (6560 футов))
Источник света	Используются лазеры как источники света на расстояниях в несколько сотен метров	Используются светодиоды (LED) как источники света в пределах локальных сетей или на расстояниях в пару сотен метров

Следующие два раздела посвящены двум простым типам оптического волокна: одномодовому и многомодовому.

Многомодовое оптоволокно

Многомодовое оптическое волокно — это волокно, в котором распространяется большое количества мод света (возможно, множество путей прохождения световых лучей) через его сердцевину, в отличие от одномодового, в котором может распространяться только одна мода. Различные моды могут проходить различные расстояния, которые зависят от угла вхождения луча в сердцевину оптического волокна. Разные углы приводят к тому, что время прохождения светом оптического пути будет различно и разные моды на другом конце волокна будут зарегистрированы с небольшим сдвигом по времени. Такое явление было названо *модовой дисперсей*. Для производства многомодового оптического волокна используется материал, который называется стеклом с градиентным коэффициентом преломления; в нем коэффициент преломления уменьшается от центра сердцевины к ее краям. Такое распределение коэффициента преломления влечет за собой уменьшение скорости распространения света в центре и увеличение скорости лучей, проходящих по краям сердцевины, и, следовательно, приводит к тому, что все моды достигают конца оптического волокна практически одновременно (это и есть дисперсия мод). Такое строение оптического волокна используется по той причине, что лучи, распространяющиеся ближе к центру сердцевины, проходят меньшее расстояние, чем лучи, которые постоянно отражаются от ее границ. Все лучи должны достичь второго конца волокна одновременно, поскольку в таком случае приемник на другом конце волокна получит четкую световую вспышку вместо длинного слабого импульса.

Стандартный многомодовый оптоволоконный кабель (широко используемый оптический кабель для локальных сетей) производится с оптическими волокнами с диаметром сердцевины, равным 62,5 либо 50 микрон, и диаметром оболочки

125 микрон. Эти кабели обычно обозначаются как 62,5/125 либо 50/125, в зависимости от диаметра сердцевины (один микрон равен одной миллионной метра). Поскольку диаметр сердцевины намного больше длинны световых волн, которые используются для передачи информации, то к такому кабелю применима лучевая модель распространения света, а световые лучи отражаются от границ сердцевины и продолжают распространяться в ней.

Инфракрасные светодиоды (Light-Emitting Diode — LED) и лазеры являются основными источниками света для многомодового оптического волокна. Светодиоды намного дешевле и менее требовательны к чистоте производства, чем лазеры, но в то же время они не могут быть использованы для передачи сигнала на такие большие расстояния, как лазеры. Многомодовое волокно (62,5/125) может быть использовано для передачи данных на расстояния, не превышающие 2000 метров[3]. Этот тип волокна используется в основном в локальных сетях и для построения опорных сетей.

Одномодовое оптоволокно

ВНИМАНИЕ!

Необходимо помнить, что лазер, использующийся с одномодовым оптическим волокном, генерирует световую волну, которая невидима для человеческого глаза. Сигнал таких лазеров обычно имеет большую мощность и поэтому может нанести вред вашим глазам. Никогда не смотрите в один из концов оптического волокна, если к другому его концу подсоединен передатчик. Никогда не смотрите в передающий порт на сетевой плате, коммутаторе или маршрутизаторе. Запомните, что необходимо сохранять все защитные насадки, которые вы сняли при установке концов оптического волокна в порты коммутаторов и маршрутизаторов.

Одномодовое оптическое волокно позволяет использовать только одну моду, распространяющуюся по сердцевине. Диаметр сердцевины одномодового оптоволокна намного меньше, чем у многомодового, обычно он лежит в пределах от 8 до 10 микрон. Наиболее распространенным является кабель с диаметром волокна 9 микрон. Маркировка 9/125 на внешней оболочке оптического кабеля говорит о том, что диаметр сердцевины равен 9 микронам, а оболочки — 125 микронам.

Малые размеры сердцевины оптического волокна рассматриваемого типа оставляют очень небольшое пространство для распространения световых лучей. В одномодовом волокне в качестве источника света используется хорошо сфокусированный инфракрасный лазер; лучи света, которые генерируются лазером, вводятся в оптическое волокно под углом в 90 градусов к поверхности. В результате световые импульсы, переносящие данные, распространяются в одномодовом оптическом волокне в основном по прямой линии, расположенной в центре сердцевины, как показано на рис. 3.26. Этот эффект значительно увеличивает скорость передачи и максимальное расстояние, на которое могут быть переданы данные.

[3] *6560 футов. — Прим. ред.*

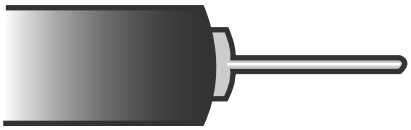


Рис. 3.26. Одномодовое оптическое волокно

Итак, одномодовое волокно позволяет передавать данные на более высоких скоростях (пропускных способностях) и на бо́льшие расстояния, чем многомодовое волокно. Такое волокно используется для передачи данных на расстояния 3000 м и более, в то время как многомодовое ограничено расстоянием всего 2000 м. Лазеры и одномодовое волокно стоят дороже, чем светодиоды и многомодовое оптическое волокно. Исходя из двух указанных особенностей, одномодовое оптическое волокно рекомендуется использовать для соединения зданий либо построения распределенных сетей (Wide-Area Network — WAN) передачи данных (например, соединения центральных офисов телефонной компании).

На рис. 3.27 проиллюстрированы относительные размеры сердцевины и оболочки всех рассмотренных выше разновидностей оптического волокна в разрезе. Самая малая и тонкая сердцевина устанавливается в одномодовом оптическом волокне, что приводит к высокой стоимости его изготовления, но это оправдывается высокой пропускной способностью и бо́льшим максимальным расстоянием, на которое можно передавать данные, чем у многомодового волокна.

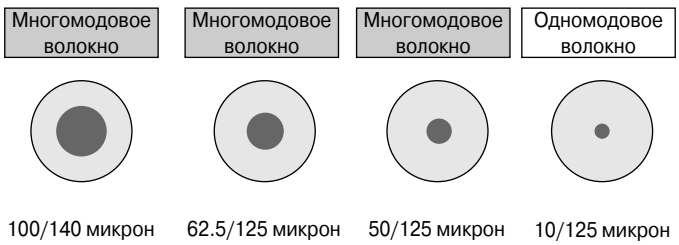


Рис. 3.27. Одномодовое и многомодовое оптические волокна

Основные характеристики оптических кабелей:

- **пропускная способность** составляет более 1 Гбит/с;
- **средняя стоимость узла** высока;
- **размеры кабеля и разъема для соединения** малы;
- **максимальная длина кабеля** — более 10 км для одномодового, до 2-х км — для многомодового.

Дополнительная информация: строение кабелей

Существуют два основных варианта строения кабелей (рис. 3.28):

- оболочка-трубка с нежестко закрепленной сердцевиной;
- оболочка с плотной набивкой.

Рис. 3.28. Различные конструкции кабеля

В кабеле с плотной набивкой буферный материал окружает оболочку оптических волокон и находится в непосредственном с ней контакте. Основное различие между указанными выше двумя типами кабеля состоит в их предназначении. Кабели с нежестко закрепленной сердцевиной используются в основном для прокладки коммуникаций между зданиями и снаружи их, в то время как кабели с плотной набивкой буферным материалом предназначены для использования внутри здания. Наиболее широко используется многомодовый оптический кабель с плотной набивкой буферным материалом внутри.

Другие оптические сетевые компоненты

Большинство данных, передаваемых по локальным сетям, представляет собой электрические сигналы. Оптические же соединения используют световые импульсы для передачи данных, поэтому необходимы устройства, которые будут преобразовывать электрические сигналы в световые на одном конце кабеля и световые в электрические — на другом его конце. В такой схеме как минимум должны присутствовать два устройства: передатчик и приемник.

Кроме передающих и приемных устройств, в этом разделе описаны и проиллюстрированы разные типы оптических соединителей, а также некоторые устройства, используемые в оптических сетях.

Передатчики

Передатчики получают данные, которые необходимо передать далее, от маршрутизаторов и коммутаторов в виде электрических сигналов. Передатчик преобразовывает электрические сигналы в эквивалентные им импульсы света. Существуют два типа источников света, которые преобразовывают и передают данные по оптическим кабелям:

- **светодиоды (Light-Emitting Diode — LED)** способны создавать инфракрасное излучение с длиной волны 850 либо 1310 нм. Излучение на таких длинах волн используется для передачи данных по многомодовым оптическим волокнам в локальных сетях. Для фокусировки и передачи светового потока в сердцевину используются линзы;
- **лазеры (Laser — Light Amplification by Stimulated Emission of Radiation)** способны создавать тонкий интенсивный луч инфракрасного излучения с длиной волны 1310 либо 1550 нм. Лазеры используются совместно с одномодовым оптическим волокном для создания соединений на больших расстояниях, обычно встречающихся в распределенных сетях (WAN), либо для построения опорной территориальной сети. С лазерами необходимо обращаться осторожно, чтобы не повредить глаза.

Каждый из источников света может очень быстро включаться и выключаться и обеспечивает формирование единиц и нулей с высокой частотой.

Приемники

На противоположном от передатчика конце оптического волокна должен находиться приемник. Его функция очень похожа на ту, которую выполняют фотоэлементы в калькуляторе с солнечными батареями. Когда свет попадает на его поверхность, он должен вырабатывать электрический ток. Первоочередная функция приемника заключается в регистрации импульсов света, которые приходят по оптическому волокну. Приемник преобразовывает световые импульсы обратно в электрический сигнал, который был получен передатчиком на другом конце волокна для передачи. Теперь сигнал снова присутствует в форме электрических импульсов и готов к передаче через медные проводники к любым электронным устройствам приема, таким, как компьютер, коммутатор и маршрутизатор. Полупроводниковые устройства, которые обычно используются в приемниках с оптоволоконными каналами, называются p-i-n диодами (PIN-фотодиодами).

PIN-фотодиоды чувствительны к определенной длине световой волны (850, 1310 либо 1550 нм), которую передатчик генерирует на другом конце кабеля[4]. Если на такой светодиод попадает световой луч с соответствующей длиной волны, он начинает вырабатывать электрический ток для сети. Электрический ток исчезает сразу же после того, как пропадает световой луч, падающий на полупроводниковый фотодиод.

[4] *Обычно полупроводниковые фотодиоды чувствительны к достаточно широкому диапазону излучения и энергетический барьер могут преодолеть как электроны, получившие энергию от фотона с определенной частотой, так и от фотона с большей частотой. — Прим. ред.*

Такой процесс вызывает появление электрического тока в цепи, которое представляет собой единицы и нули данных в медных проводниках.

Разъемы

Для подсоединения оптоволоконных кабелей к передатчикам и приемникам используются специальные разъемы, которые закрепляются на концах оптических волокон. Наиболее распространенным разъемом для многомодового оптического волокна является пользовательский разъем (Subscriber Connector — SC); его внешний вид показан на рис. 3.29. Для одномодовых оптоволоконных линий чаще используется разъем с прямым наконечником (Straight Tip — ST), который показан на рис. 3.30. По одному SC- или ST-разъему нужно устанавливать на каждое волокно. Самые новые модификации разъемов совмещают в себе передающее и принимающее оптические волокна для экономии места и по своей величине сравнимы с разъемом RJ-45.

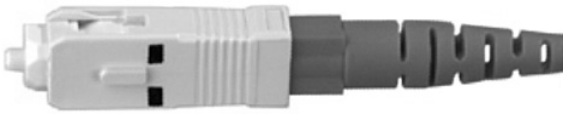


Рис. 3.29. Разъем SC

Рис. 3.30. Разъем ST

Оптические усилители и коммутационные панели

В дополнение к передатчикам, приемникам, разъемам и оптическому волокну существуют другие необходимые для построения оптической сети компоненты, такие, как усилители световых сигналов и коммутационные панели. Такие компоненты также довольно часто встречаются в оптоволоконных сетях.

Повторители выступают в роли усилителей световых сигналов; они принимают ослабленные сигналы, которые прошли большие расстояния, и восстанавливают полученные световые импульсы до их оригинальной формы, восстанавливают амплитуду и временные параметры. Восстановленные сигналы передаются далее по оптоволоконным линиям, пока не достигнут приемника на другом конце волокна.

Коммутационная панель для оптического волокна приведена на рис. 3.31. Она очень похожа на коммутационные панели, которые используются совместно с кабелями на основе медных проводников. Такие панели увеличивают возможности оптоволоконных сетей и предоставляют дополнительную гибкость разработчику сети за счет возможности быстрой перекоммутации соединений между сетевыми

устройствами, такими, как маршрутизаторы и коммутаторы, уже существующих оптических каналов (кабельных соединений).

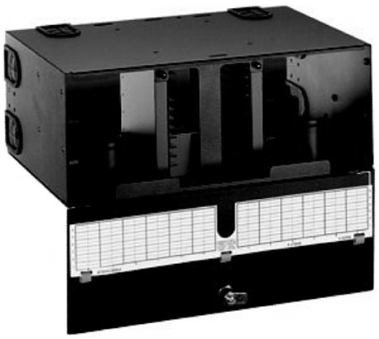


Рис. 3.31. Коммутационная панель для оптического волокна

Практическое задание 3.2.8. Выбор и приобретение оптического волокна
При выполнении этого практического задания вы ознакомитесь с разнообразными разновидностями оптического волокна и сопутствующих ему компонентов, а также их ценами на рынке.

Сигналы и помехи в оптическом волокне

В отличие от кабелей на основе медных проводников, оптические кабели не чувствительны к внешним *помехам*. Почему? Потому что свет не может попасть в сердцевину оптического волокна, за исключением единственной точки — конца кабеля, на котором находится передатчик. Волокно покрыто буферным материалом и внешней пластиковой оболочкой, которые не дают свету проникать во внутрь либо выходить за пределы оптического кабеля.

Импульсы света, которые передаются по одному из волокон, не оказывают воздействия на сигналы, передающиеся по любому из соседних волокон, поэтому для оптических волокон не существует проблем с наводками, в отличие от кабелей на основе медных проводников. Кроме того, качество оптоволоконных соединений достаточно высоко и соответствует новейшим стандартам Gigabit- и 10-Gigabit-Ethernet, в которых указано, что максимальная длина оптоволоконных каналов может быть больше 2 км. (Подробнее технология Ethernet описана в главе 7, “Технологии Ethernet”.) Структуры, которые реализованы на оптических средах, позволяют использовать технологию Ethernet в региональных и распределенных сетях.

Для передачи больших объемов данных на большие расстояния наилучшим типом соединений являются оптические. Однако они все же имеют свои ограничения при передаче данных. Когда световая энергия проходит через оптическое волокно, некоторая ее часть теряется. Такое *затухание* сигнала может быть вызвано несколькими факторами, связанными со строением оптического волокна. Один из наиболее важных факторов — *рассеивание*. Рассеивание происходит на микроскопических

неоднородностях (дефектах) в оптическом волокне, которые вызывают отражение и рассеивание некоторой части световой энергии, как показано на рис. 3.32.

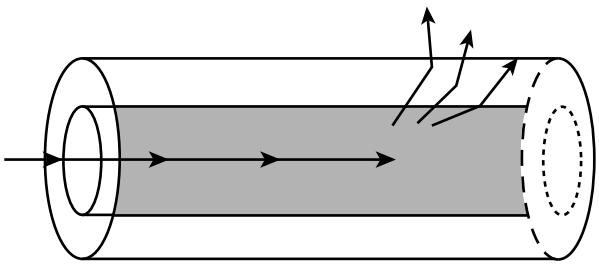


Рис. 3.32. Рассеивание

Поглощение — еще один фактор, вызывающий ослабление сигнала. Когда световые лучи встречают на своем пути в волокне некоторые химические примеси, эти примеси могут поглотить часть энергии луча. Эта часть световой энергии переходит в тепловую. Поглощение делает световой сигнал менее ярким.

К факторам, которые вызывают затухание сигнала, относятся также неточности в изготовлении волокна и шероховатость границы сердцевина-оболочка. Потери энергии происходят из-за несоответствия среды условию полного внутреннего отражения на таких неровных поверхностях и неоднородностях. Если в оптическом волокне встречаются микроскопические различия в диаметре сердцевины либо ее симметрии, это также приводит к несоблюдению правила полного внутреннего отражения, и тогда часть световой энергии проходит в оболочку и поглощается в ней.

Дисперсия светового импульса ограничивает максимальное расстояние, на которое может быть использован оптический кабель. Дисперсия — технический термин, который описывает "расползание" светового импульса и искажение его фронтов при его прохождении через оптическое волокно (рис. 3.33).

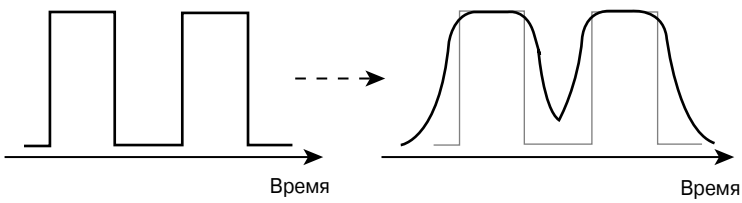


Рис. 3.33. Дисперсия

Многомодовое оптическое волокно с градиентным коэффициентом преломления было разработано для компенсации различных расстояний, которые проходят разные моды в сердцевине кабеля с большими размерами. В одномодовом оптическом волокне не возникает проблем со множеством световых путей. Но в то же время хроматическая дисперсия является общей проблемой обоих типов оптического волокна. Световые волны с определенной длиной волны распространяются в прозрачных

средах с меньшими скоростями, чем остальные. Такое различие скорости и вызывает хроматическую дисперсию. Призма способна разделить различные длины волн именно благодаря данному эффекту. В идеале светодиод или лазер должны воспроизводить всего лишь одну длину волны, и проблема хроматической дисперсии не должна существовать.

К сожалению, лазеры и особенно светодиоды излучают целый набор световых волн разной длины, и поэтому хроматическая дисперсия в оптоволокне существует и ограничивает максимальное расстояние передачи по оптическому волокну. Если попробовать передать сигнал на бо́льшее расстояние, то до приемника на втором конце волокна дойдут "размазанные" и ослабленные импульсы света, и приемник не сможет различить единицы и нули в сигнале.

Установка, обслуживание и тестирование оптического волокна

Чаще всего затухание сигнала возникает в оптических линиях из-за неправильной их установки. Если оптоволоконный кабель сильно растянут или изогнут, это может вызвать небольшие трещины в сердцевине оптических волокон, что приведет к высокому коэффициенту рассеивания световой энергии на таких дефектах. Сильные изгибы кабеля также приводят к изменению углов, под которыми световые лучи падают на границу сердцевина-оболочка. В таком случае световые лучи будут падать на границу раздела двух сред под углом, меньше критического, и вместо полного внутреннего отражения часть световых лучей будет проникать в оболочку, рассеиваться и поглощаться.

Существуют два типа дефектов-искривлений волокна:

- **макроскопические изгибы**. Их достаточно легко увидеть. Если изогнуть оптическое волокно, то часть световых лучей будет падать на границу сердцевины под углом, меньше критического, что позволит лучам проникать в оболочку. Лучи, попавшие в оболочку, не могут быть отражены обратно. Скорее всего, они будут поглощены буферным материалом, как показано на рис. 3.34;
- **микроскопические изгибы** приводят к тому же эффекту, что и макроскопические: лучи света падают на границу сердцевины под углом, меньше критического, и попадают в оболочку, как показано на рис. 3.34. Такие искривления возникают в микроскопических масштабах и невидимы для человеческого глаза.

Микроскопические искривления могут также быть вызваны высокими температурами в уже установленном оптическом волокне из-за разных температурных коэффициентов расширения и сжатия различных материалов, из которых изготовлено оптическое волокно. Такое расширение и сжатие приводит к возникновению механических напряжений внутри материалов и может вызвать искривление поверхностей, а также привести к образованию микротрещин.

Для предотвращения сильных изгибов оптического волокна его укладывают в специальные коробы. Коробы жестче, чем оптическое волокно, и поэтому прокладка оптического волокна по таким коробам исключает возможность сильных изгибов.

Коробы защищают оптическое волокно от механических повреждений, сильных изгибов и переломов, упрощают процесс укладки дополнительных коммуникаций.

После установки оптического волокна его края должны быть сколоты и отполированы, чтобы устранить шероховатости. Проблемы, связанные с неправильной обработкой концов оптического волокна, проиллюстрированы на рис. 3.35. На рис. 3.36 показана правильная техника обработки концов оптического волокна.

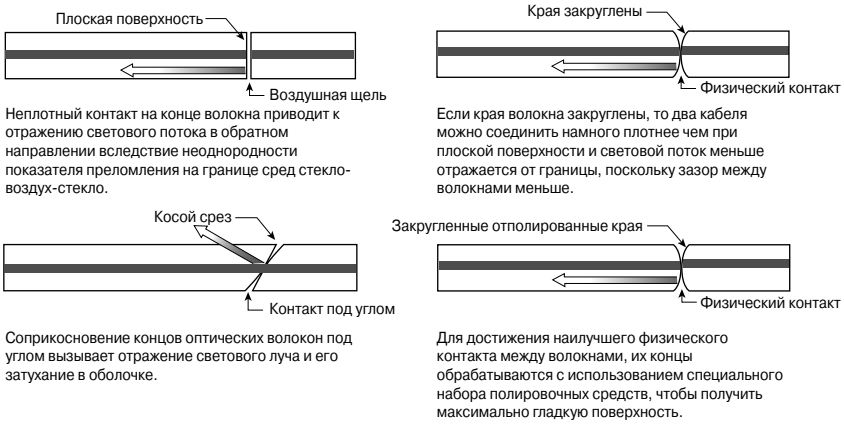


Рис. 3.35. Неправильно обработанные края оптического волокна

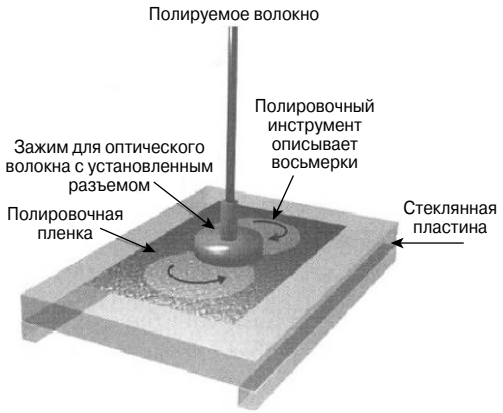


Рис. 3.36. Техника обработки краев оптического волокна

Для проверки качества обработки и полученной формы концов оптического волокна используется микроскоп либо прибор со встроенной линзой. До начала процесса полировки конца оптического волокна на него должен быть осторожно установлен разъем. Неправильно установленные разъемы, неправильные соединения либо соединение двух оптических волокон с различными диаметрами сердцевины

сильно уменьшают мощность светового сигнала. На рис. 3.37 показано соединение оптических волокон с различными диаметрами сердцевины.

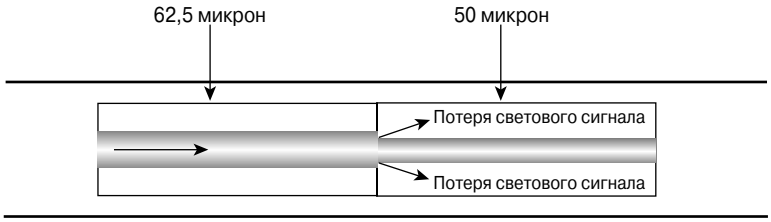


Рис. 3.37. Соединение различных типов оптического волокна

После установки оптоволоконного кабеля и разъемов для его подключения концы оптического волокна должны быть тщательно очищены. Затем их закрывают защитным колпачком во избежание повреждений при эксплуатации. Когда такое защитное покрытие снимается перед непосредственным подключением оптического волокна к порту коммутатора либо маршрутизатора, концы оптического волокна должны быть очищены снова. Концы оптических волокон очищаются гладкой тканью, увлажненной чистым беспримесным изопропиловым спиртом. Оптические порты коммутатора либо маршрутизатора также должны оставаться под защитным колпачком, если они не используются; перед использованием их нужно очистить точно так же, как и концы оптического волокна. Грязь на концах оптического волокна вызывает большие потери мощности светового потока.

Все перечисленные выше факторы — рассеивание, поглощение, дисперсия, неправильная установка и грязные концы оптического волокна — ослабляют сигнал и вызывают помехи в оптическом волокне. Перед началом использования установленных оптоволоконных линий они должны быть протестированы, чтобы убедиться, что необходимое количество световой энергии сможет достичь приемника, и последний сможет различить уровни единиц и нулей в сигнале.

При планировании и прокладке новых оптических каналов необходимо рассчитать допустимые потери сигнала. Такой допуск называют *бюджетом потери сигнала в оптическом канале (optical link loss budget)*. Это понятие похоже на ежемесячный финансовый бюджет предприятия. После того как все финансовые издержки (затухание сигнала) были вычтены из первоначального дохода, необходимое количество денег должно оставаться на счету в течение месяца, иначе предприятие станет банкротом.

Для количественного измерения потерь энергии используется единица, называемая децибелом (*decibel — dB, дБ*). Эта величина описывает процент мощности сигнала, покинувшего передатчик, который достиг приемника.

Очень важно периодически производить тестирование оптоволоконных каналов связи и регистрировать полученные результаты. Для тестирования используются несколько типов оптоволоконных тестеров. Наиболее нужные из них: измеритель коэффициента оптических потерь (Optical Loss Meter) в оптическом волокне и оптический динамический рефлектометр (Optical Time-Domain Reflectometer — OTDR).

Оба измерительных прибора тестируют оптический кабель на соответствие стандартам TIA для оптического волокна. С помощью обоих приборов также можно измерить, не выходят ли потери сигнала в оптическом волокне за допустимые пределы. Кроме того, приборы типа OTDR предоставляют информацию относительно детальной проверки оптического волокна и могут быть использованы при поиске неисправностей в линии и при возникновении некоторых проблем с передачей данных.

Дополнительная информация: беспроводная передача данных

Беспроводные системы используют электромагнитные волны, которые могут распространяться в космическом вакууме или через некоторые среды передачи данных, такие, как воздух. Для беспроводных систем не нужна физическая медная либо оптическая среда передачи данных, вследствие чего беспроводное взаимодействие является универсальным методом построения сетей. Беспроводная передача может быть осуществлена на большие расстояния при использовании высоких несущих частот. Для различных сигналов используются различные частоты, которые измеряются в герцах (Гц); разные частоты позволяют отличать один сигнал от остальных.

Беспроводные технологии окружают нас на протяжении многих лет. Спутниковое телевидение, радио, мобильные телефоны, устройства дистанционного управления, радары, системы сигнализации, беспроводные телефоны и сканеры штрихкодов присутствуют в нашей повседневной жизни. На сегодняшний день беспроводные технологии представляют собой одну из основных составных частей бизнеса и личной жизни.

Беспроводный процесс передачи данных

Радиочастотный спектр представляет собой часть электромагнитного спектра и служит для передачи голоса, видео и данных. Для него используются частоты в диапазоне от 3 кГц до 300 ГГц. В текущем разделе рассматривается небольшая область радиоспектра, в котором может происходить беспроводная передача данных.

Существует большое число разновидностей беспроводной передачи данных, как показано на рис. 3.38.

Каждая из технологий беспроводной передачи информации имеет свои преимущества и недостатки.

- **Инфракрасному (Infrared — ИК)** методу передачи данных присуща очень большая пропускная способность и низкая стоимость, но очень маленькие расстояния, на которые можно передавать данные.
- **Узкополосным (Narrowband)** технологиям присуща небольшая пропускная способность и средняя стоимость. Они требуют лицензирования и работают на небольших расстояниях.
- **Технологии с расширением спектра (Spread spectrum)** имеют среднюю стоимость и большую пропускную способность. Они используются для взаимодействия в пределах территориальной сети. Данный тип связи используется в оборудовании Cisco Aironet.
- Для **широкополосных средств персональной связи (Broadband personal communications service — PCS)** характерна низкая пропускная способность, средняя стоимость; они обеспечивают взаимодействие устройств в пределах города.
- **Технология с коммутацией каналов и пакетов данных (сотовая система передачи данных и сотовая система передачи пакетов цифровых данных — Cellular Data and Cellular Digital Packet Data, CDPD)** характеризуется низкой пропускной способностью, высокой стоимостью передачи данных и обеспечивает покрытие в пределах государства.
- **Спутниковая связь (Satellite)** имеет низкую пропускную способность, высокую стоимость и обеспечивает покрытие в пределах государства либо всего земного шара.

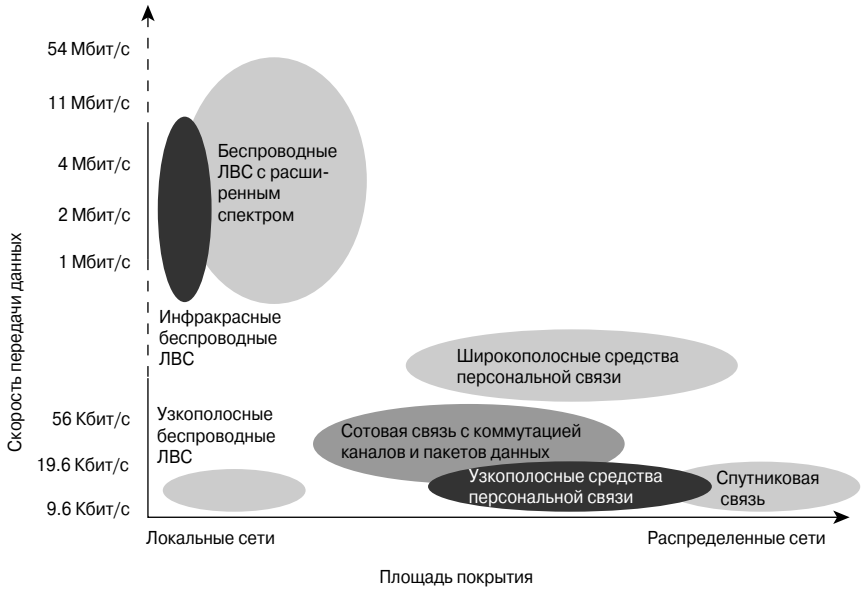


Рис. 3.38. Беспроводные сети передачи данных

Беспроводные сигналы

При рассмотрении сигнала, который используется для передачи информации в формате данных, необходимо иметь представление о следующих вещах:

- **как быстро передается ифнормация,** т.е. какой скорости передачи данных можно достичь?
- **как далеко могут быть переданы данные,** т.е. насколько устройства беспроводной ЛВС (WLAN) могут быть удалены друг от друга при сохранении максимальной скорости передачи данных?
- **как много данных может быть передано,** т.е. как много пользователей может существовать в такой сети без замедления скорости передачи данных?

Все вышеуказанные параметры определяют возможность принять хороший сигнал на максимально возможном расстоянии. Для увеличения объема передаваемых данных за единицу времени необходимо использовать более широкую полосу спектра либо дифференциальные методы передачи данных с помощью радиочастотных сигналов.

Как показано на рис 3.39, на эффективность передачи данных при использовании радиочастот влияют следующие факторы:

- **тип используемой модуляции сигнала.** Сложные методы модуляции позволяют достичь большей пропускной способности;
- **расстояние.** Чем больше расстояние между передатчиком и приемником, тем слабее сигнал будет получен на приемнике;
- **уровень шумов.** Электронные помехи и физические барьеры негативно влияют на качество радиочастотного сигнала.

В следующих разделах указанные три фактора рассматриваются подробнее.

Модуляция

Процесс модуляции заключается в изменении амплитуды, частоты либо фазы радиочастотного или светового сигнала, в зависимости от передаваемых данных. Характеристики несущей волны

практически мгновенно изменяются в зависимости от формы модулирующего сигнала. С помощью модуляции в несущую частоту вносится информация о сигнале данных (текст, голос и т.д.) для дальнейшей передачи по беспроводной сети.

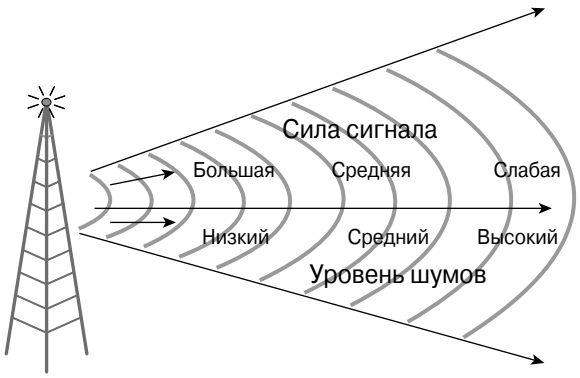


Рис. 3.39. Факторы, влияющие на эффективность радиочастотного сигнала

Ниже приведены наиболее распространенные методы модуляции (рис. 3.40).

- *Амплитудная модуляция (АМ)* предполагает модулирование амплитуды (высоты сигнала) несущей волны в зависимости от сигнала данных.
- *Частотная модуляция (ЧМ)* использует модулирование частоты несущей волны.
- *Фазовая модуляция (ФМ)* обеспечивает модулирование полярности (фазы) несущей волны.

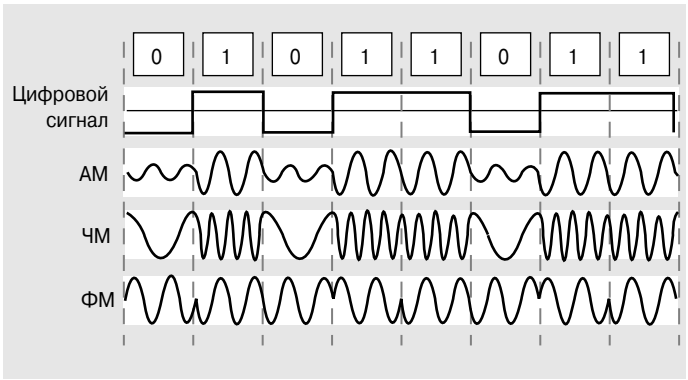


Рис. 3.40. Модуляция сигнала

Влияние расстояния на качество сигнала

Чем больше расстояние между приемником и передатчиком, тем более слабым становится несущий сигнал и тем меньше различие между полезным сигналом и шумом. В конечном итоге сигнал будет невозможно выделить на фоне шума. На таком предельном расстоянии происходит потеря связи между устройствами. Отношение сигнал/шум, необходимое для восстановления сигнала, определяется типом используемой модуляции. При увеличении пропускной способности беспроводных сетей используются более сложные схемы модуляции сигнала, при этом

уменьшается устойчивость сигнала к помехам и поэтому уменьшается максимальное расстояние, на которое можно предавать данные.

Влияние помех на качество сигнала

Электронные помехи и физические преграды негативно отражаются на качестве радиочастотного сигнала. Невозможно гарантировать нормальную работу устройств для беспроводных сетей без проведения измерений на месте параметров принимаемого сигнала. Например, стены со встроенными металлическими конструкциями заметно ограничивают максимальное расстояние для передачи данных.

Чтобы получить в приемнике достаточно чистый полезный сигнал, несущий сигнал должен иметь высокий коэффициент сигнал/шум (высокий уровень сигнала и низкий уровень шумов). Если в канале передачи данных присутствуют шумы либо помехи, то скорость взаимодействия будет уменьшаться. Помехи, скорость взаимодействия и максимальное расстояние взаимосвязаны.

Радиочастотный диапазон

Большинство радиочастот лицензировано государственными органами, такими, как Федеральная комиссия связи (Federal Communication Commission — FCC) в США. Для того что бы вещать на таких частотах, организации или предприятию необходимо получить и оплачивать лицензию.

Более просты в использовании и более дешевыми являются нелицензируемые частотные диапазоны, поскольку они не требуют приобретения права на использование. В США существуют три нелицензируемых диапазона, как показано на рис. 3.41.

- **Диапазон 900 Мегагерц (МГц).** В этом диапазоне работают беспроводные и мобильные телефоны.
- **Диапазон 2,4 Гигагерца (ГГц).** Беспроводные сети, соответствующие стандарту 802.11b, работают в частотном диапазоне 2,4 ГГц. Максимальная скорость передачи таких сетей составляет 11 Мбит/с.
- **Диапазон 5 ГГц.** Недавно Федеральная комиссия связи США открыла для нелицензируемого использования частотный диапазон 5 ГГц. Компания Cisco широко использует технологию беспроводной связи в диапазоне 5 ГГц в своих новых разработках, таких, как Cisco Aironet серии 1200. Эта серия устройств поддерживает оба диапазона (стандарты 802.11b и 802.11a). Скорость передачи данных согласно стандарту 802.11a может достигать 54 Мбит/с.

Существует зависимость между несущей частотой радиосигнала и количеством данных, которые возможно передать в таком сигнале. Чем больше пропускная способность, тем большее количество частот необходимо для передачи такого сигнала. Иными словами, чем шире частотный спектр несущей, тем большее количество данных может быть передано за единицу времени. Ширина радиочастотного спектра определяет пропускную способность как беспроводного канала передачи данных, так и многих других.

Из-за того, что в частотном диапазоне 900 МГц работают мобильные телефоны и многие другие потребительские устройства, этот диапазон часто бывает перегруженным. Поэтому пользователи вышеперечисленных устройств часто ощущают наложение сигналов либо попросту не могут подсоединиться к сети. Одним из преимуществ технологий, которые работают на рассматриваемой частоте, является то, что в диапазоне 900 МГц можно осуществлять передачу данных на большие расстояния (при тех же параметрах антенны), чем в диапазоне 2,4 ГГц. Недостатком диапазона 900 МГц является его наибольшая достоверная пропускная способность 1 Мбит/с, что является следствием ограниченного диапазона частот.

Ширина диапазона разрешенных частот для несущей 2,4 ГГц намного шире, чем в диапазоне 900 МГц, поэтому он позволяет использовать более высокие скорости передачи данных на максимальные расстояния до 25 миль. Устройства серии Cisco Aironet 340 позволяют получить максимальную пропускную способность 11 Мбит/с при использовании частоты 2,4 ГГц.

Корпорация Cisco разработала технологии передачи данных на частоте 5 ГГц по причине более широкого спектра частот и, соответственно, возможности получить более высокие скорости передачи данных. Адаптер пользователя беспроводной сети Cisco Aironet, работающий на частоте 5 ГГц, позволяет получить максимальную скорость передачи данных 54 Мбит/с;

совместим со стандартом 802.11a и функционирует в частотных диапазонах UNII-1 и UNII-2. Пользовательский адаптер совместно с точкой доступа серии Cisco Aironet 1200 представляют собой готовое решение, в котором сочетаются производительность и мобильность с безопасностью и легкостью в управлении, необходимые любой организации. В этом случае можно достичь пропускной способности более 20 Мбит/с в рассматриваемом частотном диапазоне. Недостатком технологии передачи данных на частоте 5 ГГц является ограничение по расстоянию, на которое могут быть переданы данные. Обычно максимальное расстояние для связи с использованием частоты 5 ГГц составляет 15,29 метров[5] внутри здания и 764,5 метров[6] вне каких-либо строений.

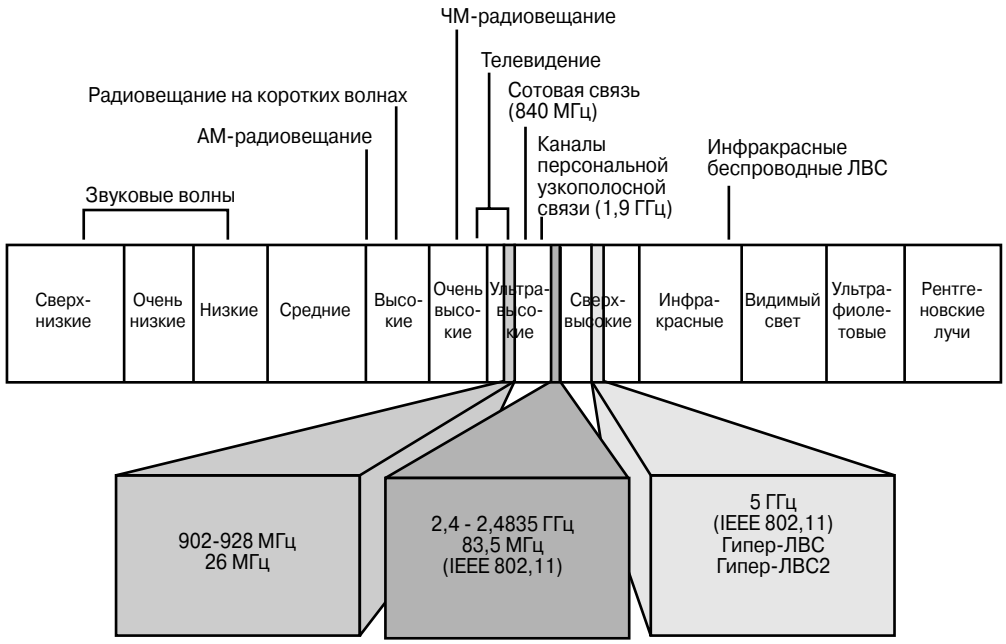


Рис. 3.41. Нетребующие лицензирования в США радиочастотные диапазоны

Технология расширения спектра

АМ и ЧМ являются наиболее распространенными радиодиапазонами, которые можно увидеть на любом бытовом радиоприемнике. Точно так же другие радиоустройства используют свои собственные частотные диапазоны и типы модуляции и полосы. Технология *расширения частотного спектра (Spread Spectrum — SS)* была разработана в 1940 году. Ее идея состоит в том, что сигнал передается посредством широкой полосы частот. Термин *расширение спектра* описывает процедуру модуляции, в которой за счет уменьшения пропускной способности достигается высокая стойкость сигнала к воздействию шумов (всегда приходится чем-то жертвовать для достижения цели). Такой тип модуляции является идеальным для передачи данных, т.к. мало подвержен радиопомехам и малой интерференции сигналов от различных источников.

Узкополосная интерференция возникает в том случае, если одновременно два устройства вещают на одной частоте в одной географически ограниченной области. Термин *полоса* (band)

[5] *50 футов. — Прим. ред.*

[6] *2500 футов. — Прим. ред.*

относится к группированию частот. Узкополосный сигнал относится к довольно узкому диапазону частот. Узкополосные шумы разрушают определенные каналы передачи данных либо компоненты расширенного спектра.

Расширение спектра, как показано на рис. 3.42, — система модуляции, в которой передаваемый сигнал распыляется по частотному диапазону, намного более широкому, чем минимальная пропускная способность, необходимая для передачи сигнала. Основы этого метода заключаются в том, что в каналах с сосредоточенными помехами используется избыточная пропускная способность, а это приводит к увеличению вероятности того, что полученная информация соответствует отправленной.

Рис. 3.42. Технология расширения спектра

Для использования диапазонов частот, не требующих получения лицензии, необходимо применять технологию расширения спектра. Существуют два способа получения расширенного спектра: *расширение спектра со скачкообразным изменением частоты* (Frequency-Hopping Spread Spectrum — FHSS) и расширение спектра прямого преобразования (Direct-Sequence Spread Spectrum — DSSS). В следующем разделе преобразования FHSS и DSSS рассмотрены подробно.

Механизмы FHSS и DSSS

Как и любой другой метод модулирования, методы FHSS и DSSS имеют свои преимущества и недостатки.

При использовании модуляции FHSS передача происходит скачками с одной частоты на другую в случайном порядке. На рис. 3.43 приведен пример использования FHSS-модуляции: несущая частота изменяется прыжками с C (2,42 ГГц) на A (2,40 ГГц), затем на D (2,43 ГГц), затем на B (2,41 ГГц) и в конце на E (2,44 ГГц). Такая техника модуляции позволяет передавать данные с резким изменением частоты вблизи сосредоточения помех, что делает сигнал более чистым, а передачу данных — более надежной. Несмотря на некоторые преимущества, технология FHSS является довольно медленной, и приемник должен иметь тот же шаблон изменения частоты, что и передатчик.

Более надежной является передача сигнала с помощью технологии DSSS. Как показано на рис. 3.44, в этой технологии каждый бит представляется некоторой последовательностью нулей и единиц, которая называется *элементарной последовательностью*. Даже если при передаче произошла потеря 40% такой последовательности, можно восстановить значение, которое было передано. Преимуществами данной технологии также являются высокая пропускная способность и возможность передачи данных на большие расстояния.

Из-за ограничения по скорости передачи данных на уровне 2 Мбит/с технологию FHSS рекомендовано использовать только для очень специфического применения, например, для некоторых типов водных судов. Для всех остальных беспроводных ЛВС рекомендуют применять технологию DSSS. Один из последних стандартов, 802.11b, позволяет получить скорость передачи данных, равную 11 Мбит/с, используя технологию DSSS. С помощью технологии FHSS невозможно получить скорости передачи данных выше 2 Мбит/с.

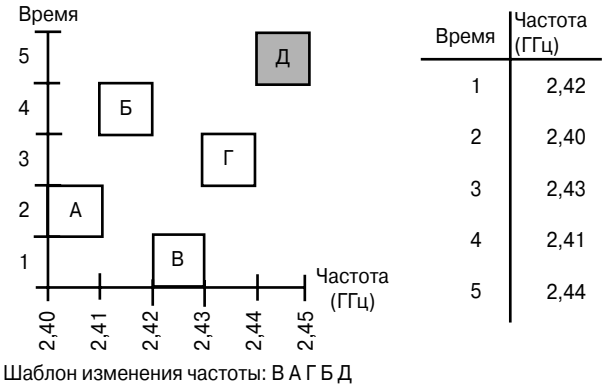


Рис. 3.43. Расширение спектра со скачкообразным изменением частоты

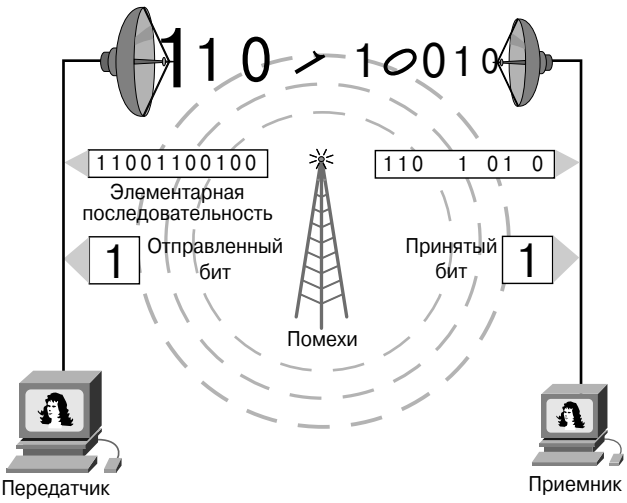


Рис. 3.44. Расширение спектра прямого преобразования (DSSS)

Беспроводные сети

Когда появились первые компьютеры, они были доступны только для больших корпораций, государственных учреждений и университетов. С того времени технологии ушли далеко вперед, и теперь производительность карманного персонального компьютера ни в чем не уступает первым компьютерам. То же можно сказать и о сетевых технологиях.

Различные типы сетей, рассмотренные ранее в текущей главе, требуют наличия физических соединений для их функционирования. Преимуществами таких сетей являются высокая скорость передачи данных, надежность и обеспечение доступа к сети в заранее заданных областях. Физическое соединение позволяет увеличить

производительность и обеспечить совместное использование принтеров, серверов и программного обеспечения. Тем не менее, такие сетевые решения требуют от сетевых устройств постоянного местоположения, передвижение устройств разрешено только в пределах установленных кабельных систем и в пределах офиса.

Появление беспроводных технологий связи позволило избежать вышеуказанных ограничений и ощутить компьютерному миру настоящую мобильность. Несмотря на то что беспроводная связь не обеспечивает высоких скоростей передачи данных, а также безопасности и постоянной доступности, ее гибкость оправдывает ее использование и обеспечивает высокие уровни продаж оборудования.

Беспроводные сети доступа очень просты в установке. Самая простая беспроводная сеть может быть настроена и запущена уже через несколько минут после включения рабочей станции. Соединение с поставщиком услуг сети Internet осуществляется посредством кабельных соединений, маршрутизатора, модема для кабельных сетей либо модема для выделенных линий, а беспроводная точка доступа выступает в роли концентратора для беспроводных устройств. В небольшом офисе концентратор и оборудование доступа могут быть совмещены в одном устройстве.

Структура и стандарты беспроводных сетей

Существуют определенные рекомендации и стандарты для беспроводных технологий. Беспроводные сети, которые разработаны и развернуты в соответствии с такими стандартами, будут совместимы друг с другом. Основным разработчиком стандартов для беспроводных технологий является Институт инженеров по электротехнике и электронике (IEEE), а его стандарты соответствуют нормам, которые установлены федеральной комиссией связи США (FCC).

В качестве основной технологии, которая описана в стандарте 802.11, выступает технология DSSS. Беспроводные устройства, работающие на скоростях от 1 до 2 Мбит/с, используют технологию DSSS, которая теоретически может обеспечить максимальную скорость передачи данных вплоть до 11 Мбит/с, но, тем не менее, обычно ее не используют для получения скоростей выше 2 Мбит/с. Следующий (т.е. более новый) стандарт 802.11b позволяет увеличить скорость передачи данных до 11 Мбит/с. Несмотря на то что теоретически технологии DSSS и FHSS могут использоваться в одной беспроводной сети, на практике возникают проблемы совместимости между устройствами различных производителей, поэтому Институт IEEE создал ряд стандартов, отвечающих запросам производителей.

Стандарт IEEE 802.11b носит название Wi-Fi (высокоскоростные беспроводные сети) и описывает взаимодействие устройств с использованием технологии DSSS на скоростях 1, 2, 5,5 и 11 Мбит/с. Все устройства, соответствующие стандарту 802.11b, совместимы с устройствами, отвечающими стандарту 802.11 и использующими систему DSSS. Такая совместимость очень важна, поскольку позволяет модернизировать беспроводную сеть без замены всех сетевых плат и точек доступа.

Устройства, соответствующие стандарту 802.11b, позволяют достигать более высоких скоростей передачи данных благодаря использованию технологии кодирования данных, которая отличается от базового стандарта 802.11, позволяя передавать

большее количество данных в том же временном интервале. Большинство устройств, соответствующих стандарту 802.11b, не достигают пропускной способности в 10 Мбит/с, реальная скорость передачи данных обычно находится в пределах 2-4 Мбит/с.

Стандарт 802.11a описывает работу устройств, использующих диапазон 5 ГГц. Поскольку в этом стандарте используются другие частоты, устройства, соответствующие стандарту 802.11a (5 ГГц), несовместимы с устройствами, соответствующими спецификации 802.11b (2.4 ГГц). Стандарт 802.11a предусматривает передачу данных на скорости 54 Мбит/с, и при помощи запатентованной технологии, именуемой *методом удвоения скорости,* можно достичь скорости передачи данных 108 Мбит/с. В большинстве работающих сетей, которые построены на основе этого стандарта, скорость передачи данных лежит в пределах от 20 до 26 Мбит/с.

Стандарт 802.11g описывает взаимодействие с той же пропускной способностью, что и стандарт 802.11a, но в него входит поддержка обратной совместимости с предыдущими беспроводными стандартами. Устройства, соответствующие этому стандарту, используют модуляцию по методу ортогонального мультиплексирования деления частоты (Orthogonal Frequency Division Multiplexing — OFDM). Корпорация Cisco Systems разработала устройство, которое позволяет взаимодействовать устройствам, соответствующим стандартам 802.11a и 802.11b, в одной беспроводной сети. Такое устройство выступает в роли шлюза и позволяет взаимодействовать несовместимому оборудованию между собой.

Устройства и структуры беспроводных сетей

Наименьшее количество устройств, из которых может состоять беспроводная сеть, — это два устройства с беспроводными сетевыми адаптерами. На рис. 3.45 показан внутренний беспроводный сетевой адаптер, а на рис. 3.46 — внешний беспроводный сетевой адаптер с USB-интерфейсом. Беспроводные устройства могут быть установлены как в настольные, так и в портативные или карманные компьютеры. Оборудованные адаптерами беспроводной связи, они создают *сеть сопряженных устройств*, которая очень схожа с одноранговой кабельной сетью. Оба устройства в такой среде работают и как сервер, и как клиент. Несомненно, такая конфигурация позволяет объединить несколько устройств и установить между ними связь, но обеспечивает низкий уровень безопасности, как, впрочем, и малую пропускную способность. Для беспроводных соединений существует проблема совместимости устройств; если приходится использовать сетевые адаптеры различных производителей, то в большинстве случаев они не могут работать друг с другом.

Наиболее часто для доступа отдельных устройств к беспроводной сети в сеть помещают точку доступа (Access Point —AP), которая выступает в роли концентратора для беспроводных устройств. Внешний вид точки доступа показан на рис. 3.47. Точка доступа подключена к кабельной сети и предоставляет беспроводным устройствам доступ к остальной сети, обеспечивает подключение к сети Internet. Точка доступа комплектуется антенной, которая предоставляет возможность доступа беспроводным устройствам к сети в некой области (называемой областью покрытия); такая область называется *ячейкой.*

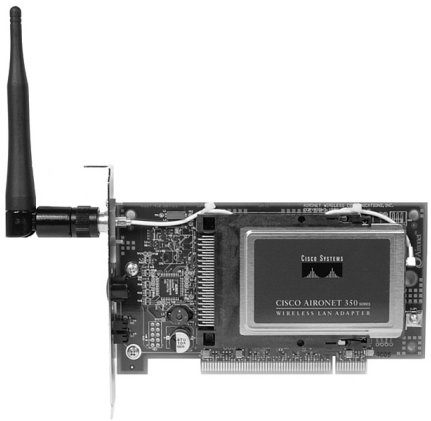


Рис. 3.45. Внутренний беспроводный сетевой адаптер

Рис. 3.46. Внешний беспроводный сетевой адаптер с US- интерфейсом

Рис. 3.47. Точка беспроводного доступа

В зависимости от типа помещения, в котором установлена точка доступа, размеры одной ячейки могут колебаться от нескольких десятков метров до десятков километров. В большинстве случаев размер ячейки составляет от 90 до 150 метров. Для создания беспроводной сети в более широких пределах необходимо установить несколько точек доступа с перекрывающимися ячейками, а также разрешить *роуминг*[7] *(roaming)* между ячейками, как показано на рис. 3.48. Роуминг в беспроводных сетях очень схож с роумингом, который предоставляют телефонные компании. Перекрытие отдельных ячеек очень важно, т.к. позволяет беспроводному устройству свободно перемещаться без потери соединения в пределах беспроводной локальной компьютерной сети. Рекомендуемый процент перекрытия ячеек должен составлять около 20-30. Такое перекрытие позволяет осуществлять процедуру роуминга, позволяя при этом устройству отсоединяться от одной точки доступа и соединяться со второй без потери соединения с беспроводной сетью.

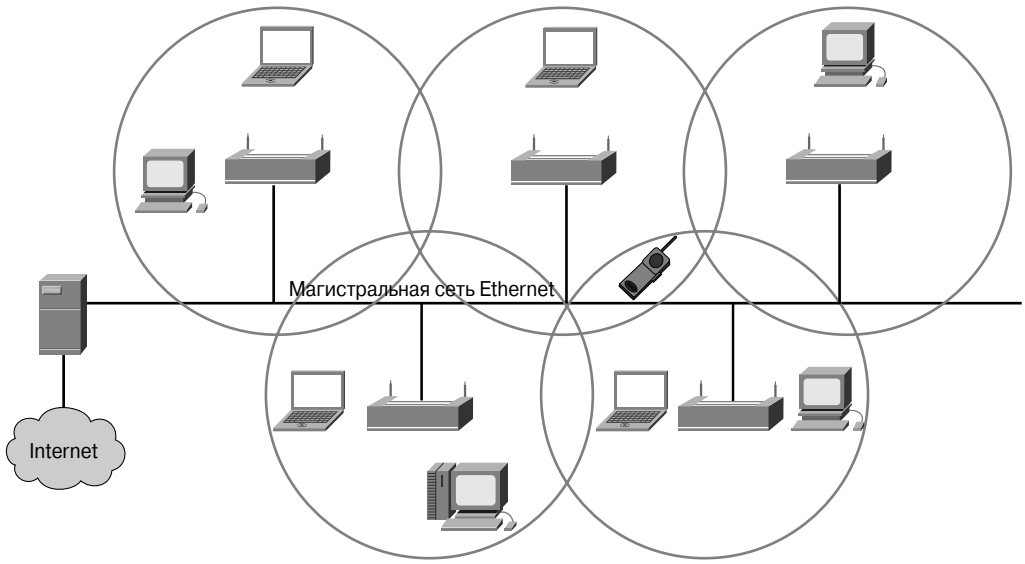


Рис. 3.48. Роуминг

Если устройство-клиент было включено в пределах беспроводной локальной сети, оно прослушивает эфир для нахождения совместимых устройств, с которыми можно было бы соединиться. Такой процесс называют *сканированием*. Процесс сканирования может быть как пассивным, так и активным.

В активном режиме сканирования устройство посылает зондирующие запросы, с помощью которых пытается найти совместимое устройство и использовать его для подключения к сети. В зондирующем запросе содержится идентификационный номер набора служб (Service Set Identifier — SSID) для той сети, к которой

[7] *Автоматическое переключение между сетями. — Прим. ред.*

хочет подключиться устройство. Если была найдена точка доступа с нужным идентификационным номером, она отвечает устройству зондирующим ответом и, соответственно, выполняет этапы аутентификации и подключения устройства к сети.

Устройства, которые находятся в пассивном режиме сканирования, прослушивают эфир и принимают сигнальные фреймы. Источником таких фреймов являются точки доступа и беспроводные станции. Когда устройство получает сигнальный фрейм с необходимым ему идентификатором SSID, оно пытается подсоединиться к беспроводной сети. Процесс пассивного сканирования является непрерывным, устройство может соединяться или разъединяться с точками доступа, в зависимости от изменения уровня их сигналов.

Взаимодействие в беспроводной сети

После установления соединения устройства с беспроводной сетью дальнейшее взаимодействие осуществляется посредством фреймов, которые идентичны фреймам сетей стандарта 802.2. Беспроводные локальные сети не используют фреймы стандарта 802.3, поэтому термин *беспроводная сеть Ethernet* не совсем корректен. В беспроводных локальных сетях существуют три типа фреймов: контрольные, управляющие и фреймы данных. Ниже приведен список фреймов, относящихся к каждому из указанных типов.

- Управляющие фреймы:
  - фрейм запроса на соединение;
  - фрейм-ответ на запрос об установлении соединения;
  - фрейм зондирующего запроса;
  - фрейм зондирующего ответа;
  - сигнальный фрейм;
  - фрейм аутентификации.
- Контрольные фреймы:
  - готовность к передаче (Request To Send — RTS);
  - готовность к приему (Clear To Send — CTS);
  - подтверждение (Acknowledgement).
- Фреймы данных.

Только фреймы данных схожи с фреймами стандарта 802.3. Размер поля данных спецификации 802.3 ограничен 1500 байтами, поэтому общий размер фрейма не может превышать 1518 байтов. В то же время размеры фрейма в беспроводных сетях могут достигать 2346 байтов, но обычно модули передачи данных беспроводных локальных сетей не превышают 1518 байтов по той причине, что точки доступа соединяются с проводной сетью стандарта Ethernet.

Исходя из того, что связь на основе радиоволн осуществляется с использованием общей среды передачи данных, в беспроводных локальных сетях могут возникать

коллизии, так же, как и в кабельной сети с общим доступом к среде передачи данных. Из-за такой ситуации в беспроводных сетях используется множественный доступ с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance — CSMA/CA). Этот тип доступа к среде передачи данных немного похож на множественный доступ с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access with Collision Detection — CSMA/CD), который используется в технологии Ethernet. Технология CSMA/CD подробно рассмотрена в главе 6, " Основы технологии Ethernet ".

Если одно из устройств передает фрейм, принимающее устройство должно отправить в ответ позитивное подтверждение (acknowledgment — ACK), поэтому эффективная скорость передачи данных в такой сети падает до 50% от номинальной. Непроизводительные затраты в сумме с затратами на реализацию протокола предотвращения коллизий уменьшают актуальную скорость передачи данных до 5,0-5,5 Мбит/с для беспроводных сетей, соответствующих стандарту 802.11b, с номинальной пропускной способностью 11 МБит/с.

Качество беспроводных сетей данных также зависит от силы сигнала и понижения качества сигнала вследствие его передачи на большие расстояния или из-за наличия помех. Как только сигнал становится слабым либо зашумленным, активируется алгоритм адаптивного выбора скорости передачи данных (Adaptive Rate Selection — ARS), и скорость передачи данных начинает уменьшаться с 11 МБит/с до 5,5 МБит/с, с 5,5 МБит/с до 2 МБит/с, либо с 2 МБит/с до 1 МБит/с, как показано на рис. 3.49.

Аутентификация и подключение

Аутентификация в беспроводных локальных сетях осуществляется на втором уровне модели OSI, и этот процесс является процессом аутентификации устройства, а не пользователя. Данный момент — принципиальный вопрос безопасности в беспроводных сетях, необходим для поиска неисправностей и общего обслуживания беспроводных сетей.

Процесс аутентификации беспроводного устройства состоит из обмена фреймами аутентификации между сетевым адаптером и точкой доступа. Клиент посылает точке доступа фрейм запроса на аутентификацию. Точка доступа принимает такой фрейм, обрабатывает его и выносит решение об аутентификации клиента. Сетевой адаптер будет извещен о вынесенном решении посредством фрейма-ответа. Точка доступа может также быть настроена на выполнение процедуры аутентификации клиентов посредством сервера аутентификации, который может провести расширенную проверку параметров и прав клиентского устройства.

Процесс подключения беспроводного устройства к точке доступа выполняется после прохождения аутентификации. После подключения клиентские устройства могут использовать услуги точки доступа для передачи данных.

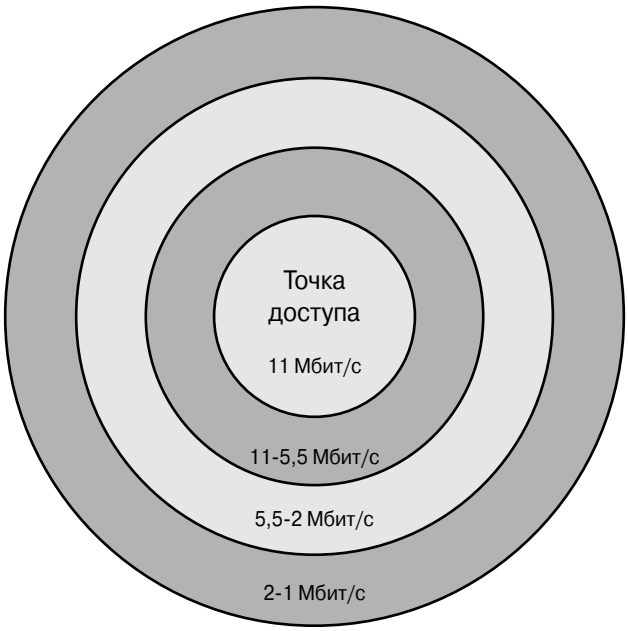


Рис. 3.49. Адаптивный механизм выбора скорости передачи данных

Возможные состояния беспроводного устройства

Беспроводное устройство может находиться в одном из трех состояний:

- **не аутентифицировано и не подключено.** Устройство отключено от сети и не подключено ни к одной точке доступа;
- **аутентифицировано, но не подключено.** Устройство аутентифицировано для доступа к сети, но не подключено ни к одной из точек доступа;
- **аутентифицировано и подключено.** Устройство подключено к сети и может выполнять прием/передачу данных с использованием услуг точки доступа.

Методы аутентификации

В стандарте IEEE 802.11 предусмотрено использование двух методов аутентификации:

- **аутентификация по методу открытой системы (Open system).** В таком процессе аутентификации проверяется только значение SSID. Этот метод может быть использован в средах с безопасным и небезопасным окружением, но несмотря на это, программы захвата и анализа трафика нижних уровней могут получить значение SSID для конкретной беспроводной локальной сети;
- **аутентификация по методу общего ключа (Shared key).** Этот процесс аутентификации требует использования алгоритма криптования WEP (Wired Equivalent Privacy — протокол обеспечения безопасности для беспроводных сетей).

Механизм WEP является довольно простым алгоритмом, в котором используются 64- или 128-битовые ключи. Точка доступа настраивается с использованием зашифрованного ключа; любому устройству для подключения к соответствующей беспроводной локальной сети через такую точку доступа необходимо иметь совпадающий ключ. Статически установленные ключи WEP обеспечивают намного более высокий уровень безопасности, чем метод открытой системы, но не могут обеспечить полной защиты от взлома.

Возможность неавторизованного вторжения в беспроводные локальные сети привела к разработке большого количества систем для обеспечения безопасности в таких сетях.

Радиочастотный и микроволновой спектр

Компьютеры передают данные в виде электрических сигналов. Радиопередатчики преобразовывают электрические сигналы в радиоволны, радиоволны создаются за счет изменений электрического тока в антенне передатчика. Радиоволны распространяются в пространстве по прямым линиям от антенны, однако они ослабевают (затухают) по мере удаления от передающей антенны. В беспроводных локальных сетях уровень сигнала на расстоянии 10 метров[8] от передающей антенны составляет всего 1/1000 от оригинального. Точно так же, как и видимый свет, радиоволны могут быть поглощены некоторыми материалами и отражены другими, кроме того, при пересечении границы раздела двух материалов радиоволны изменяют направление своего движения (преломляются или изгибаются). Радиоволны поглощаются и рассеиваются каплями воды в воздухе.

Все перечисленные выше особенности радиоволн должны быть учтены в начале планирования беспроводной территориальной, локальной сети или сети здания. Процесс определения возможного месторасположения точек доступа беспроводной локальной сети называется процессом исследования пространства.

Из-за ослабления радиосигнала по мере удаления от передатчика приемник также должен быть укомплектован антенной. Когда радиосигнал попадает на антенну приемника, в ней возникают слабые электрические токи. Такие токи являются следствием распространения радиосигнала и соответствуют токам, протекавшим в антенне передатчика при излучении радиоволн. Приемник усиливает слабый принятый сигнал.

В передатчике электрический сигнал, полученный от компьютера либо сетевой платы, не пересылается напрямую в антенну передатчика. Получаемые сигналы данных используются для изменения параметров другого, более сильного сигнала, который называется *несущим*.

Приемник демодулирует несущий сигнал, полученный из своей антенны, фиксирует изменения параметров полученного сигнала и восстанавливает из них оригинальный электрический сигнал данных.

[8] *30 футов. — Прим. ред.*

Сигналы и помехи в беспроводных локальных сетях

В проводной технологии Ethernet довольно просто определить причину возникновения помех: обычно они являются следствием интерференции сигналов от различных проводников или излучающих устройств. При рассмотрении технологии радиосвязи приходится учитывать другие разновидности помех.

- **Узкополосные помехи.** Как следует из названия, узкополосные помехи не влияют на весь спектр беспроводного сигнала. Одним из решений проблемы узкополосных помех является смена рабочего частотного канала точки доступа. В действительности диагностика причины возникновения узкополосных помех может быть очень дорогим и трудоемким занятием. Для нахождения источника помех необходимо использовать анализаторы спектра, даже самые дешевые модели которых стоят от 3000 до 4000 долларов в Соединенных Штатах Америки. Источниками узкополосных помех могут быть персональные приборы радиосвязи и любительские радиостанции.
- **Широкополосные помехи.** Широкополосные помехи оказывают влияние на весь спектр сигнала. В технологии Bluetooth[9] несущая частота изменяется несколько раз в секунду в пределах диапазона 2,4 ГГц и может вызвать серьезные помехи в сети, соответствующей стандарту 802.11b. Рекомендуется выключать все приборы Bluetooth перед подключением к беспроводной сети. В условиях домашней либо офисной сети серьезные помехи могут вызывать обычные микроволновые печи. Излучение от микроволновой печи энергии порядка 1 Вт в радиочастотный спектр могут вызвать серьезные нарушения в работе беспроводной сети. На качество работы сети негативно влияют также беспроводные телефоны, работающие в диапазоне 2,4 ГГц.
- **Погодные помехи.** В большинстве своем радиосигналы не подвержены влиянию крайних проявлений погодных условий, но несмотря на такой факт, туман либо очень высокая влажность воздуха могут вызвать серьезные помехи. Такие помехи могут быть также вызваны разрядами молнии, которые заряжают атмосферу и искажают радиоволны.

Первым и наиболее очевидным фактором, влияющим на область распространения сигнала, является аппаратура передающей станции и тип используемой антенны. Более мощная станция передает сигнал на большие расстояния, а использование параболической направленной антенны дает возможность концентрировать излучаемую энергию в одном направлении, тем самым увеличивая возможное расстояния взаимодействия.

В условиях небольших офисов (Small Office/Home Office — SOHO) большинство точек доступа используют ненаправленные антенны, которые передают сигнал во всех направлениях, но при этом уменьшается расстояние взаимодействия (рис. 3.50).

---

[9] *Технология Bluetooth (Голубой Зуб) — новая универсальная технология беспроводной связи разнотипных микропроцессорных устройств локальной сети в диапазоне 2,4 ГГц, названная так в честь датского короля X века Гарольда II по прозвищу "Голубой Зуб", всемирно прославившегося собирательством датских земель. — Прим. ред.*

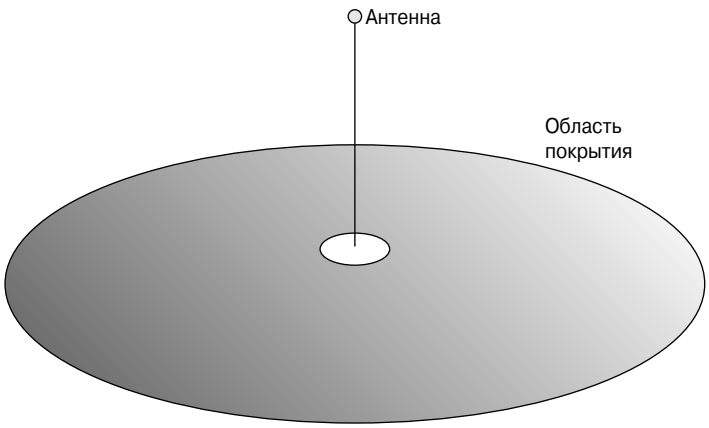


Рис. 3.50. Ненаправленная антенна

Безопасность в беспроводных сетях

В связи с бурным развитием сетей, в том числе и беспроводных, значительно возросли требования к безопасности. Увеличение безопасности приводит к увеличению времени обслуживания системы в целом.

Беспроводные точки доступа излучают радиоволны на большие площади, которые не ограничиваются физическими строениями, что делает радиосигналы доступными для подслушивания. Это приводит к повышенной уязвимости беспроводных сетей. Радиоволны от беспроводных мостов сконцентрированы в одном луче. Взломщик должен находиться на пути следования луча, чтобы перехватить информацию в процессе передачи данных. Исходя из этого, беспроводные точки доступа требуют большей безопасности, чем мосты.

Протокол WEP

Протокол обеспечения безопасности для беспроводных сетей (WEP — Wired Equivalent Privacy) описан в стандарте 802.11. Разработан для защиты процесса передачи данных по беспроводным сетям между сетевыми адаптерами и точками доступа. В стандарте 802.11q предусмотрено использование 40-битового ключа для шифрования. Но, несмотря на такое требование, большинство производителей, таких, как корпорация Cisco, поддерживают необязательный стандарт для ключа длиной 128 битов.

Основные задачи протокола WEP включают в себя:

- запрет доступа к беспроводной сети неавторизированных пользователей, которые не обладают соответствующим ключом WEP;
- предотвращение дешифрации перехваченных данных беспроводных сетей без соответствующего ключа WEP.

В протоколе WEP используется метод кодирования потока RC4, разработанный Роном Райвестом (Ron Rivest), сотрудником компании RSA Data Security Inc.

(RSADSI). Алгоритм RC4 является симметричным алгоритмом шифрования потоков данных и поддерживает ключи переменной длинны. Симметричные алгоритмы шифрования используют один и тот же ключ для процесса шифрования и декодирования данных, поэтому ключ должен быть общим у всех конечных точек, осуществляющих процедуры шифрования и дешифрования.

Совсем недавно аналитики по шифрованию обнаружили брешь в аутентификации и схеме шифрования протокола WEP, который описан в стандарте 802.11 для беспроводных сетей, поэтому были разработаны расширения протокола WEP. Несмотря на существенные улучшения, все же не рекомендуется использовать данный протокол в качестве единственного механизма обеспечения безопасности в беспроводных сетях. Кроме протокола WEP, необходимо использование механизмов безопасности более высокого уровня, таких, как средства сетей VPN либо брандмауэры.

Решения на основе технологий VPN, EAP и LEAP

Чтобы избежать многих ограничений беспроводных сетей, было разработано большое количество решений и протоколов для обеспечения безопасности в беспроводных сетях, таких, как виртуальные частные сети (Virtual Private Network — VPN) и расширяемый протокол аутентификации (Extensible Authentication Protocol — EAP). Точка доступа, использующая протокол EAP, не выполняет аутентификации пользователей; для этой цели служит выделенный сервер, способный провести более тщательную проверку параметров клиента. При использовании интегрированного сервера VPN данная технология создает туннель, применяя существующий протокол, например, IP. Такой туннель представляет собой соединение на третьем уровне эталонной модели, в отличие от соединения второго уровня между сетевой платой и точкой доступа.

Ниже приведено краткое описание протоколов EAP и LEAP.

- **EAP-MD5 Challenge (Запрос MD5-хэша протокола EAP).** Механизм EAP является одним из первых методов аутентификации и во многом похож на протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP), который используется в проводных сетях для защиты паролей. Протокол EAP позволяет клиентским сетевым адаптерам, поддерживающим различные типы аутентификации, выполнять процедуру аутентификации с различными конечными серверами, такими, как RADIUS.
- **Упрощенный расширяемый протокол аутентификации (Lightweight Extensible Authentication Protocol — LEAP).** Корпорация Cisco разработала разновидность протокола EAP, который базируется на обоюдной аутентификации, названной LEAP. При обоюдной аутентификации должны быть аутентифицированы как сетевой адаптер клиента, так и точка доступа, через которую клиент пытается подключиться к корпоративной сети. При использовании такого типа аутентификации корпоративная сеть будет защищена от использования неавторизированных точек доступа для подключения к сети. Аутентификация

LEAP стандартно используется на всех беспроводных точках доступа корпорации Cisco. Технология LEAP предоставляет безопасность в процессе обмена данными, шифрование данных с использованием динамических ключей WEP и поддерживает обоюдную аутентификацию.

Механизмы безопасности технологии VPN включают несколько методов:

- **аутентификация пользователя** позволяет только авторизованным пользователям подключаться, передавать и принимать данные, используя беспроводную сеть;
- **шифрование** предоставляет средства обеспечения конфиденциальности данных и дополнительную защиту данных от злоумышленников;
- **аутентификация данных** проверяет целостность данных, позволяет аутентифицировать устройство-отправитель и получателя данных.

Технология VPN эффективно увеличивает уровень безопасности в беспроводных сетях по той причине, что свободные беспроводные локальные сети автоматически пересылают данные между клиентами, которые находятся в пределах одной беспроводной сети. Зона покрытия беспроводных сетей не ограничена стенами здания, и без использования дополнительных технологий увеличения уровня безопасности неавторизованные пользователи могут проникать в сеть без особых проблем. Поэтому необходимо устанавливать минимальную низкоуровневую безопасность в беспроводной локальной сети.

Резюме

В этой главе были изложены следующие ключевые темы, касающиеся сетевых технологий:

- материя состоит из атомов. Атом состоит из протонов, нейтронов и электронов. Протоны и нейтроны сосредоточены в центральной части атома — ядре;
- электричество основано на возможности электронов некоторых типов атомов отделяться от орбит своих атомов и передвигаться в определенном направлении под действием внешних сил. Заряды противоположных знаков притягиваются, а одного знака — отталкиваются. Электрический ток протекает в направлении от негативного полюса к позитивному по электрической цепи;
- все материалы могут быть разделены на несколько групп — изоляторы, полупроводники и проводники, в зависимости от того, насколько легко создается в них электрический ток;
- затухание связано с сопротивлением среды потоку электронов и приводит к ослаблению сигнала. Ток может течь только в замкнутых цепях, которые состоят из проводников, источника тока и нагрузки;
- основные электротехнические величины, такие, как напряжение, электрический ток, сопротивление и импеданс, используются для описания параметров

электрических цепей; их необходимо понимать, чтобы проектировать и изготавливать электрические приборы. Перечисленные характеристики могут быть измерены с помощью мультиметра;

- существует переменный и постоянный электрический ток. Переменный ток используется для подачи электричества в жилые дома, школы и офисы. Постоянный ток используется в электрических приборах, работающих от батареек либо аккумуляторов;
- коаксиальный кабель состоит из четырех основных частей: центрального медного проводника, изоляции из пластика, плетенного медного экрана и внешней оболочки;
- кабель UTP состоит из четырех витых пар и используется во множестве различных сетей;
- в кабеле STP комбинируется экранирование, компенсирование сигналов и переплетение пар. В кабеле ScTP витые пары защищены общим экраном;
- в сетях передачи данных используются три кабеля, которые производятся на основе витой пары: прямой, перекрещенный и консольный;
- оптическое волокно является хорошей средой передачи данных при условии его правильной установки, тестирования и обслуживания;
- световая энергия, один из типов электромагнитных волн, используется для безопасной передачи информации на относительно большие расстояния;
- световой сигнал, который передается по оптическому стекловолокну, вырабатывается передатчиком, преобразующим электричество в свет. Приемник на другом конце оптического волокна преобразовывает световой сигнал обратно в электрический;
- оптоволокно используется попарно для дуплексной передачи данных;
- световые лучи подчиняются законам отражения и преломления при прохождении через оптические волокна, что позволяет изготавливать соответствующие волокна с эффектом полного внутреннего отражения;
- полное внутреннее отражение позволяет световому сигналу оставаться внутри сердцевины оптического волокна даже в том случае, если волокно изогнуто в разумных пределах;
- наибольшей проблемой является затухание светового сигнала в очень длинном кабеле, особенно в том месте, где кабель соединяется с соединительными панелями либо спаян. Исходя из этого, концы кабеля и соединители должны быть правильно установлены и протестированы высококачественными оптическими тестерами перед их использованием;
- оптические кабельные соединения необходимо периодически проверять, чтобы быть уверенным в том, что их передаточные характеристики не ухудшились;

- если в телекоммуникационном оборудовании используются мощные источники света, например, лазеры, следует с особой осторожностью обращаться с таким оборудованием, чтобы не повредить глаза и не ухудшить зрение;
- спецификации, или стандарты, представляют собой набор правил или процедур, которые широко используются в качестве универсальных методов решения технических задач;
- в беспроводном взаимодействии как часть электромагнитного спектра используется радиочастотный спектр для передачи данных, голоса и видео;
- в беспроводных коммуникациях используются три типа фреймов: контрольные, управляющие и фреймы данных;
- процесс модуляции заключается в изменении амплитуды, частоты и фазы несущего сигнала, в зависимости от сигнала данных для его передачи;
- для использования преимуществ, не требующих лицензирования радиочастотных диапазонов, необходимо использовать технологии расширения спектра. Существуют две важные техники модуляции: FHSS и DSSS. Используя технологию DSSS, можно достичь более высокой надежности передачи данных и более высокой пропускной способности;
- беспроводные сигналы ухудшаются при отдалении их от источника. Беспроводные устройства, подключенные за пределами границы оптимального расстояния, работают на меньшей пропускной способности;
- помехи могут быть вызваны различными структурами (железобетонные стены) либо электрическими приборами. Оба фактора влияют на максимальный радиус беспроводного взаимодействия;
- в беспроводных сетях используется множественный доступ с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance — CSMA/CA);
- в беспроводных сетях происходит аутентификация устройства, а не пользователя;
- к беспроводным стандартам относятся: IEEE 802.11, IEEE 802.11a, IEEE 802.11b и IEEE 802.11g;
- технология WEP описана в стандарте IEEE 802.11 и обеспечивает безопасное взаимодействие между сетевым адаптером клиента и точкой доступа;
- существует большое количество решений и протоколов для обеспечения безопасности беспроводных локальных сетей: VPN, EAP, LEAP и др.;
- к беспроводным устройствам относятся сетевые карты, сетевые карты PCMCIA для портативных компьютеров, внешние USB-устройства, точки беспроводного доступа и беспроводные мосты.

Ключевые термины

AM (амплитудная модуляция) — процесс изменения высоты (амплитуды) несущей волны.

Ассоциация промышленности средств связи (Telecommunications Industry Association — TIA) — организация, которая разрабатывает стандарты для телекоммуникационной промышленности.

Ассоциация электронной промышленности (Electronics Industries Association — EIA) — это группа разработчиков стандартов для электрических систем передачи сигналов. Ассоциации EIA и TIA разработали большое количество известных стандартов для передачи информации.

Дисперсия мод — при распространении по оптическому волокну нескольких мод, в зависимости от угла попадания лучей в оптическое волокно, эти лучи проходят различные расстояния, достигая точки назначения (принимающий конец оптического волокна) с небольшой разницей во времени.

Дисперсия — это расширение (“расплывание”) светового импульса при прохождении по оптическому волокну.

Длина волны — расстояние от одной точки одной волны до соответствующей точки следующей (соседней) волны. Длина волны света обычно измеряется в нанометрах (нм).

Затухание — уменьшение энергии сигнала при его прохождении через среду передачи данных.

Защищенная витая пара (Shielded Twisted Pair — STP) — тип кабеля витой пары, в которой каждая пара имеет свой экран, а весь кабель защищен общим экраном.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers — IEEE) — профессиональная организация, одним из направлений работы которой является разработка стандартов для передачи данных и сетей. Доминирующими стандартами для построения локальных сетей являются стандарты организации IEEE.

Коаксиальный кабель состоит из внешнего цилиндрического проводника, который окружает центральный проводник.

Коммутационная панель — объединение определенного количества разъемов и портов, которое можно установить в монтажную стойку либо настенный шкаф в кабельном узле. Коммутационные панели выступают в роли пассивного коммутационного оборудования и используются для быстрого изменения топологии подключения устройств.

Многомодовое оптическое волокно — волокно, в котором существует более одного пути для прохождения световых лучей.

Наводки — это воздействие электромагнитных волн, излучаемых одним проводником, на другой близлежащий проводник.

Неэкранированная витая пара (Unshielded Twisted Pair — UTP) — среда передачи данных, представляющая собой четыре пары свитых медных проводников в пластиковой оболочке без металлизированного экрана. Широко используется в различных сетях.

Одномодовое оптическое волокно — такое волокно, в котором существует только один путь для распространения светового луча; по своей сути противоположно многомодовому оптическому волокну.

Опорная сеть, или магистраль (backbone) — часть сети, по которой проходит весь трафик, предназначенный для различных участков сети.

Оптоволоконный кабель — среда передачи данных для модулированного светового луча. По сравнению с другими средами передачи данных, он является более дорогим, но нечувствительным к электромагнитной интерференции кабелем. Иногда его называют просто оптическим волокном.

Отражение лучей света, падающих на границу раздела двух физических сред, происходит под тем же углом (углом падения), но в обратном направлении.

Полное сопротивление (импеданс) — сопротивление движению электронов в цепи с переменным током (включает в себя активное и реактивное сопротивление).

Преломление — эффект изменения направления распространения светового луча при переходе через границу раздела двух физических сред.

Протокол обеспечения безопасности для беспроводных сетей (Wired Equivalent Privacy — WEP) — механизм обеспечения безопасности, описанный в стандарте 802.11, предназначен для защиты процесса взаимодействия сетевой платы и точки доступа от несанкционированного прослушивания.

Радиочастотная интерференция — шумы, возникающие в проводниках из-за воздействия на них радиочастотных сигналов.

Расширение спектра сигнала прямой последовательности (Direct-Sequence Spread Spectrum — DSSS) — технология, в которой передача данных является более надежной, поскольку каждый бит (0 или 1) представляется некой последовательностью нулей и единиц, которая называется элементарной последовательностью.

Расширение спектра со скачкообразным изменением частоты (Frequency-Hopping Spread Spectrum — FHSS) — процесс расширения спектра и передачи данных методом скачкообразного изменения несущей частоты по случайному закону. Такой тип передачи данных позволяет избежать влияния узкополосных шумов, в результате чего сигнал будет более чистым и увеличится надежность передачи данных.

Расширение спектра — особая техника модуляции сигнала, разработанная в 1940-х годах, позволяющая расширить передаваемый сигнал на широкий диапазон радиочастот. Этот термин описывает модуляцию, которая пренебрегает пропускной способностью, для того чтобы получить более высокое соотношение сигнал/шум.

Сеть с использованием толстого коаксиального кабеля (thicknet) — это один из самых старых типов локальных сетей, реализованных на базе стандарта 10BASE5. Единственным преимуществом таких сетей является возможность передачи данных на расстояния до 500 м без использования усилителей.

Сеть с использованием тонкого коаксиального кабеля (thinnet) — это сеть с использованием простого тонкого коаксиального кабеля, базирующаяся на стандарте 10BASE2. В таких сетях возможна передача данных на расстояния до 185 м, но довольно сильно упрощается работа с кабельным хозяйством.

Сопротивление — свойство материалов препятствовать прохождению через них электрического тока.

Среда передачи данных относится к многочисленным типам физического окружения, через которое происходит передача сигнала. Наиболее распространенные среды передачи данных включают в себя витую пару, коаксиальный кабель, оптическое волокно и атмосферу (через которую происходит передача данных с помощью микроволн, лазеров и инфракрасных сигналов).

Стандарт — набор широко используемых либо официально рекомендованных правил и процедур.

Угол отражения — угол между отраженным лучом и нормалью к поверхности.

Угол падения — угол между падающим лучом и нормалью к поверхности.

ФМ (фазовая модуляция) — изменение фазы несущего сигнала.

ЧМ (частотная модуляция) — изменение частоты несущей волны.

Шум — нежелательный электрический сигнал в проводе, который накладывается на сигнал данных, изменяя при этом его форму.

Электромагнитная интерференция (ElectroMagnetic Interference — EMI) — это взаимодействие электрического поля с электронными компонентами, устройствами и системами, негативно влияющее на их работу.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Выберите правильную пару из двух колонок.

1) Нейтрон.	а) Частица, имеющая негативный заряд.
2) Протон.	б) Частица, не имеющая заряда (нейтральная).
3) Электрон.	в) Частица, имеющая позитивный заряд.

а) 1-а, 2-б, 3-а.

б) 1-а, 2-в, 3-б.

в) 1-б, 2-в, 3-а.

г) 1-б, 2-а, 3-в.

2. Какое утверждение неверно по отношению к электричеству?

а) Заряды различных знаков притягиваются.

б) Заряды одного знака отталкиваются.

в) Как для зарядов различного знака, так и для одинаковых сила взаимодействия увеличивается при приближении зарядов друг к другу.

г) Ни один из указанных выше вариантов.

3. Сопоставьте приведенные ниже характеристики и величины их измерения.

1) Напряжение.	а) Ом.
2) Электрический ток.	б) Ампер.
3) Сопротивление.	в) Вольт.

а) 1-в, 2-б, 3-а.

б) 1-б, 2-в, 3-а.

в) 1-а, 2-в, 3-б.

г) 1-в, 2-б, 3-а.

4. Движение электронов в _____ цепи называется _____.

а) Разомкнутой; напряжением.

б) Замкнутой; напряжением.

в) Разомкнутой; электрическим током.

г) Замкнутой; электрическим током.

5. Какова может быть максимальная длина кабеля STP?

а) 100 футов.

б) 150 футов.

в) 100 метров.

г) 1000 метров.

6. Сколько пар проводов содержится в кабеле UTP?

а) 2.

б) 4.

в) 6.

г) 8.

7. Какой разъем используется для кабеля UTP?

а) STP.

б) BNC.

в) RJ-45.

г) RJ-69.

8. Какое преимущество присуще коаксиальному кабелю по сравнению с кабелями STP и UTP?

а) Используя коаксиальный кабель, можно получить скорость передачи данных от 10 Мбит/с до 100 Мбит/с.

б) Этот тип кабеля дешев.

в) Он может быть использован для передачи данных на большие расстояния без использования усилителей.

г) Ничего из вышеперечисленного.

9. Что дает свивание пар в кабеле витой пары?

а) Делает кабель более тонким.

б) Удешевляет кабель.

в) Уменьшает проблемы, связанные с помехами.

г) Позволяет уместить шесть пар в объеме четырех.

10. Зачем нужны стандарты EIA/TIA?

а) Они описывают жесткую структуру реализации эталонной модели OSI.

б) Они описывают правила для производителей, при соблюдении которых достигается совместимость оборудования.

в) Они описывают минимальные требования к среде передачи данных для неоднородных сетей, в которых используется оборудование разных производителей.

г) Ни один из указанных выше вариантов.

11. _____ оптическое волокно передает несколько световых потоков, полученных от светодиода.

а) Многомодовое.

б) Многоканальное.

в) Многофазное.

г) Ни одно из указанных выше.

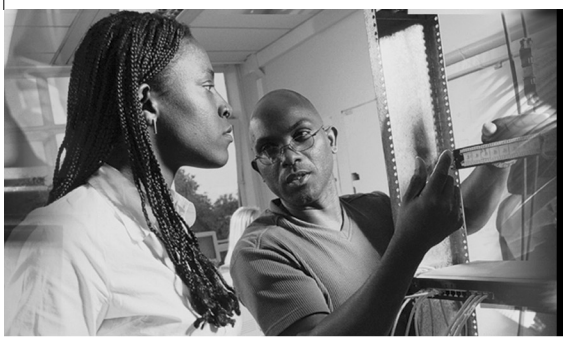
12. В чем состоит основное преимущество оптического волокна?

а) Дешевизна.

б) Легкость установки.

в) Оно является индустриальным стандартом и присутствует на любом складе электронных компонентов.

г) Оно позволяет строить сети с бо́льшей пропускной способностью, чем коаксиальный кабель и витая пара.



ГЛАВА 4

Тестирование кабелей

В этой главе...

- показаны различия между синусоидальными и прямоугольными сигналами;
- рассматриваются изменения сигналов с частотой и со временем;
- описаны две разновидности медного кабеля;
- рассказывается, как волоконно-оптический кабель переносит сигналы;
- дано описание процесса затухания;
- рассмотрены источники шума в медной среде передачи;
- рассмотрены экспоненты и логарифмы;
- определены десять основных параметров, которые используются при тестировании кабелей согласно стандартам TIA/EIA;
- дано понятие децибела;
- описана развертка сигнала по времени и частоте;
- рассмотрены единицы измерения аналоговой и цифровой полосы пропускания;
- описаны временные параметры сигналов;
- указаны методы проверки оптического волокна;
- описан стандарт кабеля категории 6.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

волна, с. 231,
частота, с. 231,
амплитуда, с. 231,
герц, с. 231,
импульс, с. 231,
синусоидальные волны, с. 231,
логарифм, с. 234,
децибел, с. 234,
осциллограф, с. 236,
спектральный анализатор, с. 236,
узкополосная интерференция, с. 238,
полоса пропускания, с. 239,
затухание, с. 243,
импеданс, с. 244,
перекрестные наводки, с. 245,
внешние перекрестные наводки, с. 245,
NEXT, с. 245,
FEXT, с. 245,
PSNEXT, с. 246,
TIA/EIA-568-B, с. 248,

шум, с. 237,
тепловой шум, с. 238,
интерференция радиосигналов, с. 238,
электромагнитная интерференция, с. 238,
белый шум, с. 238,
входные потери, с. 248,
ELFEXT, с. 248,
PSELFEXT, с. 248,
Задержка распространения сигнала, с. 251,
смещение задержки, с. 251.

В этой главе рассматриваются вопросы, связанные с тестированием передающей среды, используемой для физических соединений в локальных сетях (Local-Area Network — LAN). Для того чтобы LAN- и WAN-сети эффективно функционировали, необходимо, чтобы среда сети Ethernet на физическом уровне удовлетворяла промышленным стандартам для скоростей 10, 100, 1000 и 10 000 Мбит/с. Используемый в тексте главы термин *сигнал* относится к сигналам, содержащим данные, которые передаются от передатчика приемнику. При прохождении по физической передающей среде сигнал ослабляется, однако приемник должен быть способен правильно и однозначно определять состояние каждого бита данных (единица или нуль). В противном случае уровень ошибок окажется слишком высоким, и сеть LAN или WAN станет неработоспособной.

Передающая среда физически и в буквальном смысле слова является магистралью сети. Низкое качество кабелей приводит к сбоям и ненадежной работе сети. Все три типа передающей среды (медный, оптоволоконный кабели и атмосфера (беспроводная связь)) требуют тестирования и замеров качества; это тестирование и является основным предметом рассмотрения в настоящей главе.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в настоящей главе.

Частотное тестирование кабеля

При описании тестирования передающей среды на основе медного провода, оптоволоконных кабелей и беспроводной среды, при оценке их качества и измерении характеристик используются особые электрические и математические концепции и термины, такие, как сигнал, волна, частота и шум. Понимание их необходимо при изучении работы сетей, анализе кабельной схемы и ее тестировании.

Волны

Под термином *волна (wave)* понимается перемещение энергии в пространстве из одного места в другое. Существует много различных типов волн, однако все они могут быть описаны в рамках этого определения.

Для понимания сущности этого понятия целесообразно рассматривать волну как возмущение в некоторой среде. Например, в неподвижном ведре с водой возмущения отсутствуют, поэтому волн там нет. И наоборот, в океане всегда имеются волны, вызываемые ветром, приливами и отливами.

Океанские волны можно описать их высотой и амплитудой, которая может быть измерена в метрах. Другой характеристикой волны является частота, с которой они ударяются о берег. Эта характеристика может быть представлена двумя способами: задана временны*м* промежутком между последовательными волнами или описана частотой колебаний. Период волны представляет собой время между двумя последовательными волнами. Для волновых или колебательных процессов *частота (frequency)* определяется тем, сколько раз в секунду волны достигают берега.

Под термином *амплитуда (amplitude)* для электрического сигнала подразумевается аналог высоты океанской волны, однако измеряется он не в метрах, а в вольтах. Если сигнал регулярно повторяется, то под периодом сигнала понимается время одного его цикла, измеряемое в секундах, так же как период океанской волны определяется временем между двумя последовательными волнами. Частота электрического сигнала определяется количеством полных циклов (или волн) в секунду и измеряется в *герцах* (*hertz*).

Если возмущение вызывается намеренно и имеет постоянную, предсказуемую длительность, оно называется *импульсом (pulse)*. Импульсы являются важным типом электрического сигнала, поскольку они задают значения передаваемых данных. На рис. 4.1 проиллюстрированы понятия амплитуды и частоты. Специалистов по сетям интересуют следующие особые типы волн:

- электрические волны (изменение напряжения) в медном проводе;
- световые волны в оптоволоконном кабеле;
- используемые в беспроводной среде переменные электрические и магнитные поля, называемые электромагнитными волнами.

Синусоидальные волны и прямоугольные импульсы

Синусоиды, или *синусоидальные волны* (*sine waves*), представляют собой графическое изображение математических функций, как показано на рис. 4.2.

Синусоидальные волны обладают следующими характеристиками:

- имеют периодический характер (это означает, что они имеют фиксированную форму и регулярно повторяются);
- они непрерывно изменяют свою амплитуду (т.е. любые две смежные точки на графике имеют различные значения).

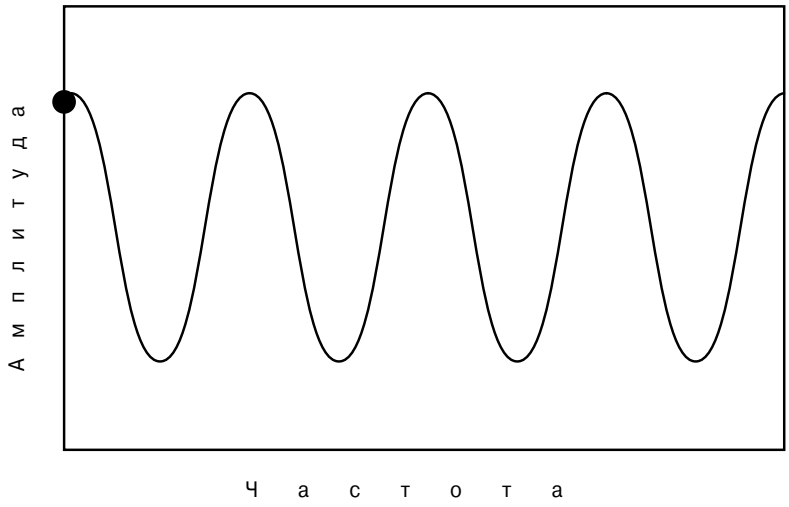


Рис. 4.1. Амплитуда и частота

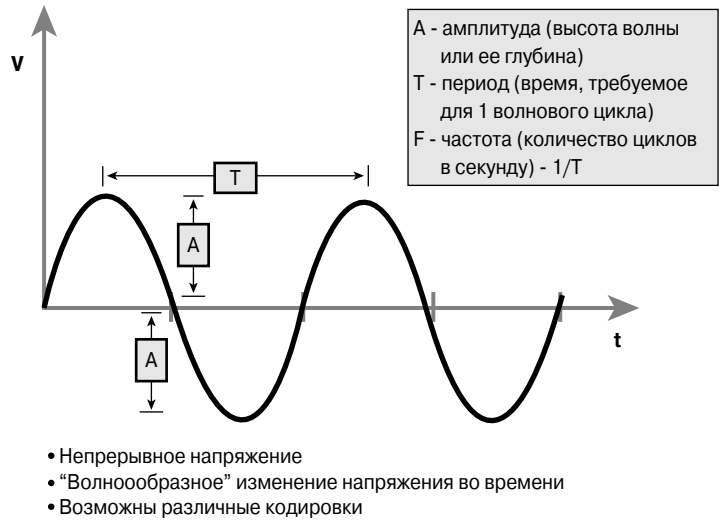


Рис. 4.2. Аналоговые сигналы

Синусоидальные волны являются графическим представлением многих регулярно происходящих природных явлений, таких, как изменение расстояния от Земли до Солнца, расстояние до земли при поездке на "чертовом колесе" (Ferris wheel) или время суток, когда восходит солнце. Поскольку амплитуда синусоидальной волны изменяется непрерывным образом, эту величину можно рассматривать как аналог природного явления; такие волны еще называют аналоговыми.

Меандры, *или прямоугольные волны*, обычно называемые *прямоугольными импульсами*, как и синусоидальные волны, имеют периодический характер. Однако амплитуда таких импульсов не всегда является непрерывной функцией времени. В течение некоторого промежутка времени ее значение остается постоянным, затем резко изменяется, снова остается постоянным и вновь скачком возвращается к первоначальному значению, как показано на рис. 4.3. Прямоугольные импульсы отображают цифровые сигналы или импульсные величины. У них, как и у всяких волн, есть амплитуда, период и частота.

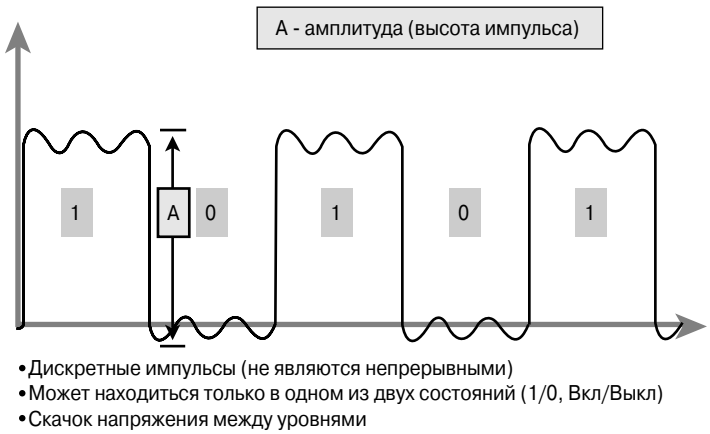


Рис. 4.3. Цифровые сигналы

Возведение в степень и логарифмы

Как уже говорилось в главе 1, “Введение в компьютерные сети”, в сетевой сфере широко используются три системы счисления:

- двоичная (или бинарная, с основанием 2);
- десятичная (с основанием 10);
- шестнадцатеричная (с основанием 16).

Отметим, что основанием системы счисления называется количество различных возможных символов в позиции числа. Например, бинарные (двоичные) числа могут иметь в одной позиции только две различных цифры (0 и 1), десятичные — 10 различных цифр (от 0 до 9), а шестнадцатеричные — 16 цифр (цифры 0 до 9 и буквы от A до F).

Отметим также, что число, равное 10×10, может быть записано как 10^2 (10 в квадрате, или 10, возведенное во вторую степень, или 10, умноженное на себя). Аналогичным образом число 10×10×10 может быть записано как 10^3 (10 в кубе, или 10, возведенное в третью степень, или 10, дважды умноженное на само себя).

При записи числа в таком виде говорят, что 10 является основанием, а 2 или 3 — показателем степени. Приводимый ниже пример иллюстрирует эти рассуждения.

$y = 10^x$	$y = 10^x$
x: 2	x: 3
y: 100	y: 1000

Основание системы счисления также влияет на значение каждой цифры. Наименьшая значащая цифра числа дает *базовое значение (base)*, т.е. основание, возведенное в нулевую степень, или число единицу. Следующая цифра дает величину, равную основанию, возведенному в первую степень ($base^1$).

Это значение равно двум для двоичных чисел, 10 — для десятичных и 16 — для шестнадцатеричных.

Числа, записанные в виде основания, возведенного в некоторую степень, используются для того, чтобы представить большие числа в более простом виде. Запись одного миллиарда в виде 10^9 выглядит значительно проще, чем в виде 1 000 000 000, и при такой записи значительно меньше вероятность ошибиться. При тестировании кабелей приходится иметь дело с очень большими числами, поэтому предпочтительнее их записывать в виде основания со степенью.

Один из методов работы с очень малыми и очень большими числами в сетевых технологиях заключается в их преобразовании согласно некоторому правилу или математической функции. Такая функция называется *логарифмом*. Обычно логарифмы связаны с базовыми значениями, т.е. с их основой, и носят соответствующее название. Так, например, десятичный логарифм обозначается как log.

Чтобы рассчитать десятичный логарифм числа, можно воспользоваться калькулятором. Тем не менее, во многих случаях значение можно вычислить очень быстро вручную, например, $\log (10^9)$ будет равен 10, $\log (10^{-3})$ равен -3. Логарифм может быть рассчитан для любого положительного числа даже в том случае, если оно не кратно 10, но не может быть получен для отрицательного числа. Подробное изучение логарифмов выходит за рамки этой книги. Следует помнить, что логарифмирование используется для расчета децибелов, которые являются мерой изменения сигналов в медных, оптических и беспроводных средах передачи данных.

Децибелы

Важным способом описания сетевых сигналов является использование единицы измерения, называемой *децибелом* (*decibel — dB, дБ)*. Эта единица измерения тесно связана с понятиями возведения в степень и логарифма, описанными в предыдущих разделах. Величина, представляющая количество децибелов, вычисляется по приведенным ниже формулам.

$$dB = 10 \times \log_{10} (P_{final}/P_{ref})$$

или

$$dB = 20 \times \log_{10} (V_{final}/V_{reference})$$

Обычно параметры световых волн в оптоволоконном кабеле или радиоволн в атмосфере измеряются в физических единицах энергии (ваттах), а параметры электромагнитных волн в медных кабелях — в единицах напряжения (вольтах).

В указанных выше формулах имеет место следующее:

- децибелы (dB) характеризуют увеличение или уменьшение энергии волны. При ослаблении сигнала по мере прохождения по среде количество децибелов отрицательно, а при усилении сигнала — положительно;
- величина $\log_{10}$ указывает, что величина в скобках преобразована с использованием логарифмирования по основанию 10;
- P_{final} — энергия сигнала, выраженная в ваттах;
- P_{ref} — первоначальная энергия сигнала, выраженная в ваттах;
- V_{final} — напряжение сигнала, выраженное в вольтах;
- V_{ref} — первоначальное напряжение, выраженное в вольтах.

Приведенный ниже пример иллюстрирует вычисление значений в децибелах.

$$P_{final} = P_{ref} \times 10^{(dB/10)},$$
$$dB = 20,$$
$$P_{ref} = 2 \text{ кВт},$$
$$P_{final} = 200 \text{ кВт}.$$

При подстановке в эту формулу значений параметров dB и P_{ref} конечное значение энергии изменяется. Эти вычисления могут быть использованы для того, чтобы узнать, какую часть своей первоначальной энергии сохранил сигнал после прохождения большого расстояния через различные материалы или через различные модули электронных систем, таких, как радиоустройства.

Рассмотрим еще несколько важных для понимания описанных выше величин примеров.

- Если значение P_{final} равно одному микроватту (мкВт, 10^{-6} Вт), а значение P_{ref} равно одному милливатту (мВт, 10^{-3} Вт), то чему равно затухание или усиление сигнала? Будет полученная величина положительной или отрицательной? Чему соответствует полученное значение: усилению или ослаблению сигнала?
- Предположим, ослабление сигнала в оптоволоконном канале равно -84 дБ, и начальная мощность лазерного источника (P_{final}) равна одному милливатту (мВт, 10^{-3} Вт). Сигнал какой мощности будет присутствовать на входе приемного устройства?
- Предположим, на выходе кабеля присутствует напряжение, которое равно двум микровольтам (мкВ, 2×10^{-6} В); изначально источник вырабатывает напряжение 1 Вольт. Чему будет равен коэффициент затухания или усиления сигнала? Будет полученная величина положительной или отрицательной? Чему соответствует полученное значение: усилению или ослаблению сигнала?

Ответы на эти вопросы читателю предлагается дать самостоятельно.

Изменение амплитуды сигнала в зависимости от времени и частоты

Одним из наиболее важных фактов нашего "информационного века" является то, что данные, представляющие символы, слова, изображения, видеофильмы и музыку, могут быть представлены в электронном виде, т.е. в форме изменений электрического напряжения в проводах или электронных устройствах. Данные, представляемые изменениями напряжения, могут быть преобразованы в световые волны или радиоволны и вновь в изменения напряжения. Рассмотрим пример работы аналогового телефона. Звуковые волны голоса абонента попадают на микрофон телефонного аппарата. Микрофон преобразует изменения энергии звука в изменения электрического напряжения, которые представляют голос.

Если эти изменения представить в виде графической зависимости от времени, то получится график, показывающий голосовые данные. *Осциллограф (oscilloscope*) представляет собой важное измерительное электронное устройство, используемое для наглядного отображения электрических сигналов, таких, как синусоидальные изменения напряжения и электрические импульсы. Ось X экрана отображает время, а ось Y — изменения напряжения или тока. Как правило, для измеряемых величин в устройстве имеются два входа, сигналы которых отображаются на оси Y, поэтому одновременно можно наблюдать два меняющихся сигнала.

Анализ сигнала с помощью осциллографа называется временны*м* анализом (time-domain analysis), поскольку ось X, или область определения математической функции сигнала, отображает время. Для изучения сигналов в инженерной практике также используется анализ зависимости амплитуды сигнала от частоты. При частотном анализе ось X представляет частоту сигнала. Графическое отображение спектрального анализа создается электронным устройством, которое называется *спектральным анализатором (spectrum analyzer*), и для построения спектра сигнала использует преобразование Фурье. На рис. 4.4 показаны несколько сигналов в том виде, как они отображаются на экране осциллографа и как их показывает спектральный анализатор.

При передаче электромагнитных сигналов используются различные частоты, для того чтобы сигналы не накладывались друг на друга. Например, радиосигналы с частотной модуляцией (Frequency Modulation — FM) используют частоты, отличные от тех, которые применяются для телевидения или спутникового вещания. При настройке на радиостанцию слушатель изменяет частоту, которую принимает радиоприемник.

Аналоговые и цифровые сигналы

Чтобы представить себе, насколько сложны сигналы, которые используются для передачи данных в компьютерных сетях и в тестировании структурированных кабельных систем, необходимо знать, как именно изменяются аналоговые сигналы и их частотные характеристики с течением времени. Прежде всего следует представить себе синусоидальную электрическую волну определенной частоты, которая после преобразования в звуковую может восприниматься человеческим ухом.

После преобразования такой волны с помощью динамика в звук человек услышит звук определенной высоты (тон). Каким образом такой звук определенной высоты будет изображен на экране анализатора спектра?

Теперь представим себе комбинацию из нескольких синусоидальных волн. Результирующая волна будет иметь намного более сложную форму, чем простая синусоидальная волна. Человеческое ухо будет воспринимать несколько звуков различный высоты. Как анализатор спектра изобразит такую ситуацию? В спектре комбинированной сложной волны будут присутствовать несколько полос, каждая из которых будет отображать соответствующую частоту каждого тона. И, наконец, представим себе, как выглядит очень сложный сигнал, например, голос или сигнал музыкального инструмента. Как для такого сигнала будет выглядеть график анализатора спектра? Если в сигнале присутствует множество тонов, то спектр сигнала будет непрерывным.

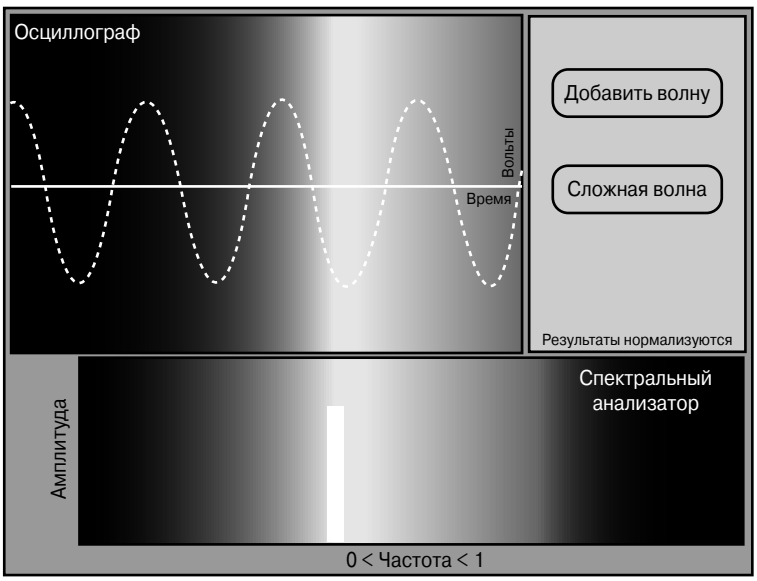


Рис. 4.4. Фурье-спектр сигнала

Изменение амплитуды шума в зависимости от времени и частоты

Важным понятием, широко применяемым в коммуникационных системах, включая локальные сети (LAN), является *шум (noise)* (рис. 4.5). Аналогично тому, как под обычным шумом понимаются нежелательные звуки, в сфере коммуникаций под шумом понимаются нежелательные сигналы. Шум может вызываться природными причинами или технологическими источниками и в коммуникационных системах добавляется к полезному сигналу. Во всех коммуникационных системах присутствуют

шумы. Хотя шум не может быть полностью уничтожен, его влияние можно минимизировать, если известны его источники. Источниками шумов являются:

- соседние кабели, по которым передаются сигналы, переносящие данные;
- *тепловой шум*, который является следствием тепловых колебаний электронов и узлов в кристаллической решетке проводника;
- *интерференция (наложение) радиосигналов (Radio Frequency Interference — RFI)*, представляющая собой шум от других сигналов, передаваемых поблизости;
- *электромагнитная интерференция (Electromagnetic Interference — EMI)*, представляющая собой шум от расположенных поблизости источников электромагнитного излучения, таких, как моторы и источники света;
- шум от лазеров, которые являются передатчиками или приемниками оптического сигнала.

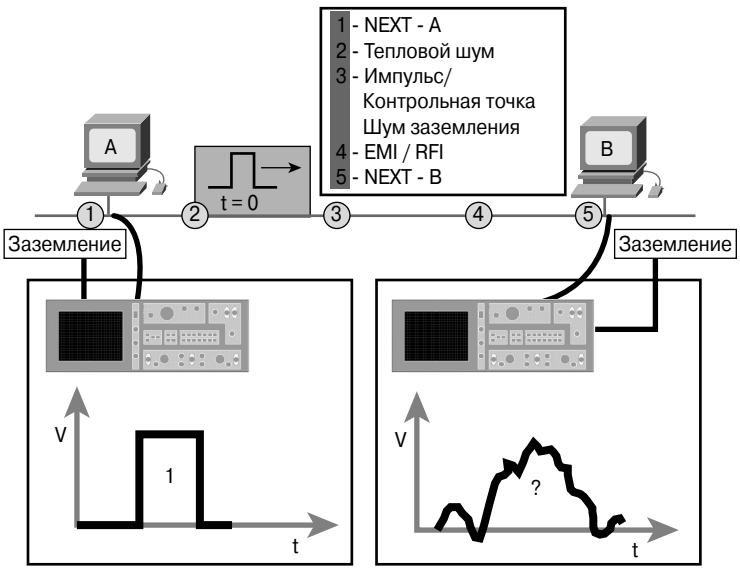


Рис. 4.5. Распознавание и определение шума

Шум, который затрагивает в равной степени все частоты передачи сигнала, называется *белым (white noise)*. Влияние шумов, которые затрагивают лишь узкую полосу частот, называется узкополосной интерференцией (*narrowband interference*). При детектировании сигнала в радиоприемнике белый шум представляет собой интерференцию со всеми радиочастотами, в то время как узкополосная интерференция затрагивает лишь близкие к основной несущей частоты. В локальных сетях (LAN) белый шум влияет на все передаваемые данные, в то время как узкополосная интерференция искажает лишь сигналы определенных частот. Однако если полоса частот, затрагиваемая узкополосной интерференцией, включает в себя все частоты сигналов, используемые в LAN-сети, то работа всей сети нарушается.

Полоса пропускания

В коммуникационных системах исключительно важным понятием является полоса пропускания. При изучении локальных сетей LAN важны два типа полосы пропускания: аналоговая и цифровая.

Под *аналоговой полосой пропускания (analog bandwidth*) понимается диапазон частот аналоговой электронной системы. Аналоговая полоса пропускания может быть использована для описания диапазона частот, на которых происходит передача сигнала радиостанцией или электронным усилителем. В качестве единицы измерения аналоговой полосы пропускания используется частота, т.е. количество циклов в секунду, измеряемая в герцах (Гц). Примерами значений аналоговой полосы пропускания могут служить 3 кГц в телефонной сети, 20 кГц — для звуковых сигналов, 5 кГц — для автомобильных радиостанций и 200 кГц — для радиостанций в диапазоне FM.

Значение *цифровой полосы пропускания (digital bandwidth*) показывает, какой объем информации может быть передан из одного места в другое за определенный период времени. Базовой единицей измерения цифровой полосы пропускания является количество битов в секунду. Однако, поскольку в LAN-сетях типичными являются скорости в несколько миллионов битов в секунду, их часто выражают в килобитах в секунду (Кбит/с) и в мегабитах в секунду (Мбит/с), как показано в табл. 4.1. Ширина полосы пропускания ограничивается свойствами физической среды, используемой технологией и физическими законами.

Таблица 4.1. Единицы измерения цифровой полосы пропускания

Единицы измерения цифровой полосы пропускания	Аббревиатура	Эквивалент в битах в секунду
Битов в секунду	бит/с	1 бит/с = базовая единица измерения полосы пропускания
Килобитов в секунду	Кбит/с	1 Кбит/с = 1000 бит/с = 10^3 бит/с
Мегабитов в секунду	Мбит/с	1 Мбит/с = 1000 000 бит/с = 10^6 бит/с
Гигабитов в секунду	Гбит/с	1 Гбит/с = 1 000 000 000 бит/с = 10^9 бит/с

При тестировании кабеля аналоговая полоса пропускания используется для определения цифровой полосы пропускания медного кабеля. Частоты аналогового сигнала передаются с одного конца кабеля и принимаются на другом конце. После этого два сигнала сравниваются, и это позволяет определить степень затухания сигнала в кабеле. В целом передающая среда, которая имеет более широкую аналоговую полосу пропускания и которой присущ небольшой уровень ослабления, будет также обеспечивать и более высокую цифровую полосу пропускания.

Сигналы и шум в сетевой среде

Под шумами понимаются любые возмущения в физической передающей среде, которые затрудняют для получателя распознавание сигналов полезных данных. Медные кабели подвержены влиянию многих источников шума, однако в оптоволоконных кабелях, применяемых в качестве передающей среды, количество возможных источников шума значительно меньше. Некоторый уровень шумов в передающей среде неизбежен, однако приемлемый уровень шумов должен быть, насколько возможно, уменьшен. Подобно тому, как при разговоре двух собеседников высокий уровень внешнего шума делает их слова трудными для понимания, сигналы данных могут подавляться слишком высоким уровнем шумов, и в этом случае получатель сигнала может их не распознать.

Критически важным фактором уменьшения шума является техника установки кабеля и правильно выполненное подключение разъемов на обоих концах кабеля. При соблюдении стандартов сигналы данных ослабляются в меньшей степени, и уровень шума не превышает максимально допустимых значений.

После установки кабеля должно быть выполнено его тестирование и проверено его соответствие стандартам спецификаций TIA/EIA-568-B ассоциации индустрии телекоммуникаций/ассоциации электронной индустрии (Telecommunications Industry Association/Electronics Industries Association). Проблемы должны быть выявлены и устранены до установки сетевого аппаратного обеспечения. Нужно также периодически проверять соответствие установленного кабеля спецификациям. Кабели и разъемы со временем подвергаются старению и износу, поэтому для надежной работы сети необходимо периодически выявлять и устранять потенциальные проблемы. При тестировании кабелей и устранении их неисправностей необходимо использовать специальные тестеры качества кабелей.

Передача сигналов по медному проводу и по оптоволоконному кабелю

В медном кабеле сигналы данных представляются изменениями напряжения, которые описывают нули и единицы цифрового сигнала. В передатчике и приемнике измерения уровня напряжения осуществляются относительно нулевого уровня, который определяется заземлением. Такой нулевой уровень сигнала является точкой отсчета напряжений. Для того чтобы она была точной, передающее и принимающее устройства должны быть надежно заземлены. Для эффективной работы LAN-сети принимающее устройство должно быть способно четко различать нули и единицы, передаваемые как уровни напряжения. Телекоммуникационные сигналы передаются с помощью малых напряжений, не превосходящих 5 Вольт. Несмотря на то что современные технологии Ethernet поддерживают скорости передачи в несколько миллиардов битов в секунду, каждый бит должен четко распознаваться, даже если его длительность крайне мала. Для улучшения распознавания данных не могут быть использованы ни усиление сигнала в приемнике, ни увеличение его длительности. Поэтому следует добиваться того, чтобы максимально сохранить первоначальную

мощность сигнала при его прохождении по кабелю и через сетевые разъемы. Учитывая возможность появления в ближайшем будущем еще более высокоскоростных протоколов Ethernet, при установке новых кабельных систем следует использовать наилучшие на данный момент типы кабелей: неэкранированный кабель витой пары (Unshielded Twisted-Pair — UTP) 5-й категории (Category 5 — CAT 5) или более качественный кабель, качественные разъемы и соединительные устройства, такие, как монтажные блоки (punch-down block) и коммутационные панели.

Существуют два типа медного кабеля: экранированный и неэкранированный. У экранированных кабелей имеется защитная оболочка, которая защищает передаваемые сигналы данных от источников помех (также называемых наводками). Некоторые типы экранов защищают сигнал от внешних источников шума, другие защищают одну пару проводов в кабеле от шумов, порождаемых электрическими сигналами других пар проводов того же кабеля.

Коаксиальный кабель является одной из разновидностей экранированного кабеля (рис. 4.6). Он состоит из прочного медного проводника, окруженного изолирующим материалом, а затем плетеным проводящим экраном. В локальных сетях плетеный экран электрически заземляется для защиты внутреннего проводника от внешних электрических шумов. Этот экран также помогает предотвратить потерю мощности сигнала за счет того, что электромагнитное поле сигнала заключено в самом кабеле; это делает коаксиальный кабель менее "шумящим", чем кабель на основе витой пары, однако вместе с тем увеличивает его стоимость. Необходимость заземления экрана и большие размеры такого кабеля усложняют его установку по сравнению с другими типами медных кабелей.

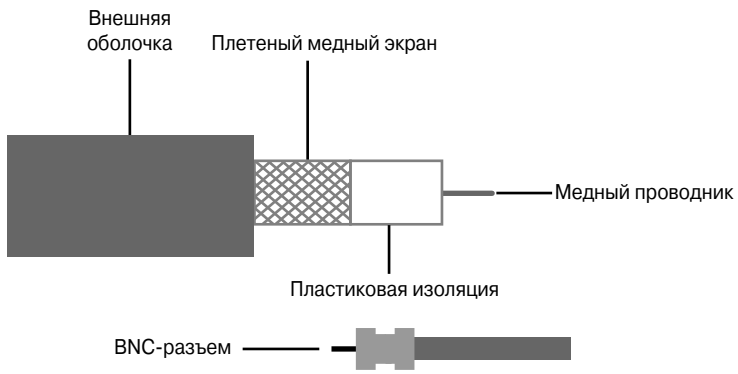


Рис. 4.6. Коаксиальный кабель

Кроме коаксиального кабеля, широко используются два типа кабелей на основе витой пары:

- экранированная витая пара (Shielded Twisted-Pair — STP) (рис. 4.7);
- неэкранированная витая пара (Unshielded Twisted-Pair — UTP) (рис. 4.8).

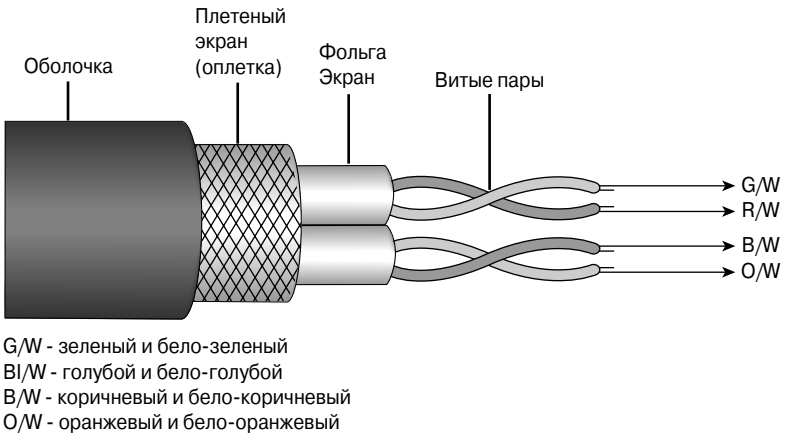


Рис. 4.7. Экранированный кабель на основе витой пары

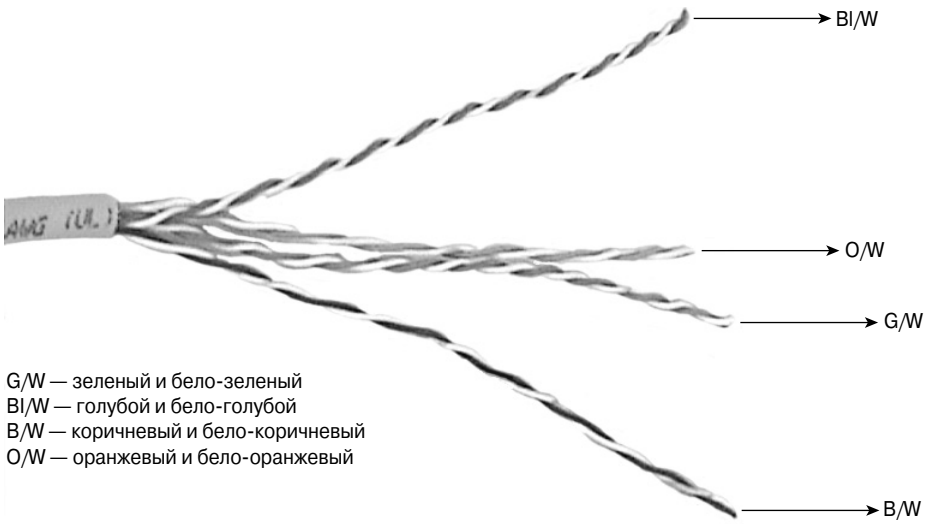


Рис. 4.8. Неэкранированный кабель на основе витой пары

Кабель STP, который также называют экранированной витой парой (Screened Twisted-Pair — ScTP) или фольгированной витой парой (Foil Twisted Pair — FTP), имеет внешний проводящий экран, который электрически заземлен для защиты передаваемого сигнала от внешних электрических воздействий. В кабеле STP также используются внутренние экраны из фольги для защиты каждой пары проводов от шума, создаваемого другими парами. Кабель STP имеет бо́льшую стоимость, его более трудно устанавливать, поэтому он используется реже, чем неэкранированная витая пара UTP. У кабеля UTP отсутствует экран, и он является наиболее “шумящим”

из всех медных кабелей, однако используется чаще других по причине его невысокой стоимости и легкости установки.

В оптоволоконном кабеле, показанном на рис. 4.9 и 4.10, передача данных осуществляется в виде световых импульсов различной интенсивности, которые отображают двоичные нули и единицы. При передаче светового сигнала его интенсивность, в отличие от электрического сигнала, практически не уменьшается. На оптические сигналы не оказывают воздействия электрические шумы, а сам оптоволоконный кабель не требует заземления. По этой причине оптоволоконный кабель часто используется для соединений между зданиями и этажами отдельного здания. По мере того как стоимость оптоволоконных кабелей снижается, а требования к скорости передачи возрастают, их использование расширяется и, возможно, в будущем они станут чаще всего используемой средой передачи для локальных сетей LAN.

Рис. 4.9. Разъем оптоволоконного кабеля

Рис. 4.10. Оптоволоконный кабель

Затухание сигналов и входные потери при прохождении сигнала по медному проводу

Под *затуханием (attenuation*) сигнала понимается уменьшение его амплитуды по мере перемещения по каналу, как показано на рис. 4.11. Степень затухания увеличивается при увеличении длины канала и возрастании частоты сигнала. По этой причине затухание сигнала в кабеле измеряется специальным кабельным тестером с использованием самых высоких частот, которые им поддерживаются.

Затухание выражается в децибелах (dB) с отрицательным знаком (поскольку величина убывает). Меньшим значениям в децибелах соответствуют более качественные каналы (с меньшим ослаблением сигнала). Затухание сигнала вызывается несколькими факторами:

- сопротивление медного кабеля вызывает превращение части электрической энергии сигнала в тепловую ;
- потеря энергии сигнала также вызывается его выходом за изолирующую оболочку кабеля и импедансом (сопротивлением переменному току) в случае дефектных разъемов.

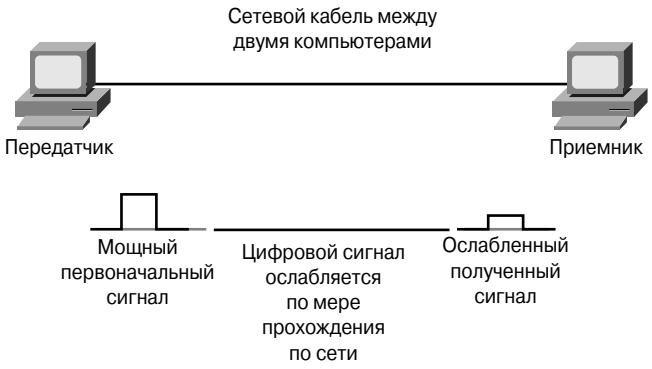


Рис. 4.11. Затухание сигнала

Под *импедансом (impedance)* понимается сопротивление кабеля переменному току (Alternating Current — AC), измеряемое в омах. Нормальным (характерным) значением импеданса кабеля категории 5 (CAT 5) является значение 100 Ом. Если разъем кабеля CAT 5 установлен ненадежно, то значение его импеданса может быть иным. Такое различие значений импеданса называется *разрывом импеданса (impedance discontinuity)*, или *несоответствием импеданса (impedance mismatch)*.

Разрывы импеданса ослабляют сигнал, поскольку при этом часть энергии передаваемого сигнала вместо движения к получателю, как эхо, отражается в направлении передающего устройства. Этот эффект усиливается, если таких разрывов несколько, поскольку в таком случае часть энергии сигнала отражается в направлении передающего устройства, а при возвращении сигнала к первому разрыву часть его вновь отражается в первоначальном направлении, в результате чего происходит многократное эхо. Эхо-сигналы поступают к получателю с разными интервалами и тем самым затрудняют точное распознавание полезных данных. Этот эффект называется дребезжанием (jitter[1]) и приводит к ошибкам в получаемых данных.

Комбинация эффектов затухания сигнала и разрывов импеданса в коммуникационном канале называется *входными потерями (insertion loss)*. Для эффективного и надежного функционирования сети желательно добиться одинакового значения импеданса во всех кабелях и разъемах, с тем, чтобы во всей системе не было его разрывов.

Источники шумов в медном проводе

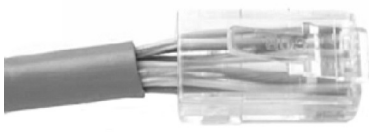
Шум представляет собой электрическую энергию в передающем кабеле, которая затрудняет получателю распознавание данных, получаемых от передатчика. Сертификация медных кабелей TIA/EIA-568-B требует, чтобы кабель прошел тестирование для ряда различных типов шумов. Кабель UTP не имеет защитного экрана от внешних источников шума, таких, как электродвигатели, флуоресцирующие источники света и источники шумов внутри кабеля.

[1] *Этот термин часто используют также для обозначения флуктуации фазы сигнала, что приводит к путанице. — Прим. ред.*

Под *перекрестными наводками (crosstalk)* понимается передача сигналов от одной пары другим смежным парам того же кабеля. При изменении напряжения в какой-либо из пар кабеля возникает электромагнитное поле. Эта энергия излучается передающей парой как радиосигнал от передатчика. Смежные пары проводов при этом действуют как антенны, генерируя более слабый, но аналогичный сигнал, воздействующий на другие пары. Перекрестные наводки могут вызвать интерференцию (наложение) данных, передаваемых по смежным проводам; перекрестные наводки могут также вызываться другим, отдельно расположенным поблизости кабелем. Перекрестные наводки, которые вызываются сигналами от другого кабеля, называются *внешними перекрестными наводками (alien crosstalk)*. Отрицательное воздействие внешних перекрестных наводок возрастает с увеличением частоты передаваемого сигнала.

При тестировании кабеля величина внешних перекрестных наводок измеряется путем подачи на одну проводную пару тестового сигнала и последующего замера амплитуды нежелательных перекрестных наводок в других парах этого же кабеля. При более высоких скоростях передачи величина перекрестных наводок увеличивается и оказывает бо́льшее неблагоприятное воздействие на передаваемые полезные сигналы.

Нежелательные перекрестные наводки возникают также в том случае, когда скрученные провода расплетаются и, таким образом, становятся подверженными наводкам от другой пары проводов, как показано на рис. 4.12. Поэтому для уменьшения перекрестных наводок необходимо обеспечить соответствующее скручивание проводных пар. Чем выше категория кабеля UTP, тем больший уровень скручивания требуется для того, чтобы минимизировать перекрестные наводки даже при высоких скоростях передачи. Для надежной работы локальной сети LAN необходимо свести уровень расплетения проводных пар к минимуму. Об этом особенно важно помнить при запрессовке разъемов на концах кабеля UTP.



Некачественно подсоединенный разъем. Провода расплетены на слишком большой участке

Качественно подсоединенный разъем. Провода расплетены лишь настолько, сколько потребовалось для его подсоединения

Рис. 4.12. Разъем, подверженный перекрестным наводкам

Существуют три типа перекрестных наводок:

- перекрестные наводки на ближнем[2] конце кабеля (Near-end crosstalk — NEXT);
- перекрестные наводки на дальнем конце кабеля (Far-end crosstalk — FEXT);

[2] *Ближний конец кабеля зачастую называют* передающим, *а дальний* — принимающим. — *Прим. ред.*

- суммарная мощность перекрестных наводок на ближнем конце кабеля (power sum near-end crosstalk — PSNEXT).

Перекрестные наводки на ближнем конце кабеля (Near-end crosstalk (NEXT), показанные на рис. 4.13, вычисляются как отношение амплитуды напряжения тестового сигнала к уровню сигнала перекрестных наводок, измеряемому на том же конце провода, на котором подается тестовый сигнал. Это отношение выражается в децибелах (dB) и имеет отрицательный знак.

Малые отрицательные значения свидетельствуют о бо́льшем уровне шумов, а бо́льшие по абсолютной величине — о меньшем, подобно тому, как малые отрицательные температуры свидетельствуют о большем количестве тепла, чем при больших отрицательных температурах. По традиции, кабельные тестеры не указывают знак "минус" при индикации отрицательных значений коэффициента NEXT. Показание тестера 30 dB (в действительности -30) при измерении параметра NEXT указывает на меньший уровень NEXT-шумов и более высокое качество кабеля, чем показание NEXT, равное 10 dB (в действительности -10).

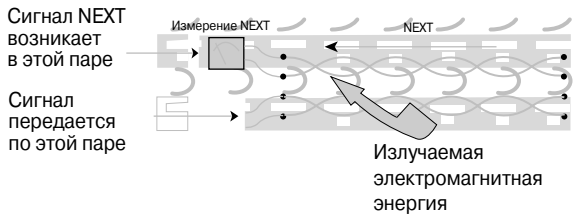


Рис. 4.13. Перекрестные наводки на ближнем конце кабеля

Параметр NEXT должен быть измерен между всеми возможными сочетаниями двух пар UTP-канала и с обоих его концов. Для сокращения времени тестирования некоторые инструменты для кабельного тестирования позволяют пользователю измерять величину NEXT с бо́льшим шагом по частоте, чем указанный в стандарте TIA/EIA. Однако полученные таким образом измерения могут не соответствовать спецификации TIA/EIA-568-B и при этом могут быть не замечены дефекты кабеля. Для надежной оценки эффективности работы канала параметр NEXT должен быть измерен с обоих концов кабеля высококачественным тестирующим устройством. Такое тестирование также является обязательным для полного соответствия высокоскоростным кабельным спецификациям.

Вследствие ослабления сигнала перекрестные наводки на большом расстоянии от передатчика, называемые перекрестными наводками на дальнем конце *(far-end crosstalk — FEXT*), создают меньшие искажения, чем перекрестные наводки на ближнем конце (NEXT), как показано на рис. 4.14. Шум, возникающий из-за наводок FEXT, также возвращается к источнику сигнала, однако его уровень при возвращении уменьшается. Таким образом, наводки FEXT создают меньше проблем, чем наводки NEXT.

Суммарная мощность перекрестных наводок на ближнем конце (Power sum near-end crosstalk — PSNEXT), показанная на рис. 4.15, отражает кумулятивный эффект перекрестных наводок NEXT от всех проводных пар кабеля. В кабеле с четырьмя парами проводов параметр PSNEXT вычисляется на основе результатов трех тестовых измерений параметра NEXT между данной парой и тремя остальными. При одновременной передаче сигналов от нескольких источников суммарный эффект от перекрестных наводок может весьма неблагоприятно повлиять на сигнал. Согласно спецификации TIA/EIA-568-B, тест PSNEXT является обязательным.

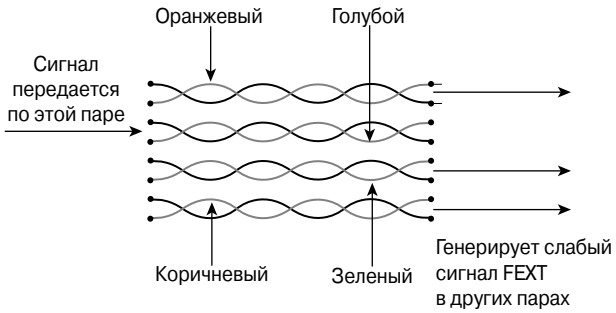


Рис. 4.14. Перекрестные наводки на дальнем конце кабеля

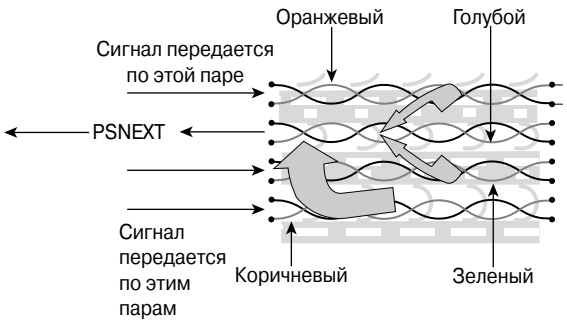


Рис. 4.15. Суммарная мощность перекрестных наводок на ближнем конце (PSNEXT)

Некоторые Ethernet-стандарты, такие, например, как 10BASE-T или 100BASE-TX, допускают получение данных только от одной пары в каждом из двух возможных направлений. Однако для новейших технологий, таких, как 1000BASE-T, в которых возможно получение данных одновременно по нескольким парам в одном и том же направлении, измерение суммарной мощности перекрестных наводок имеет большую важность и является обязательным.

Стандарты тестирования кабелей

Стандарт *TIA/EIA-568-B* определяет десять тестов, которые должен пройти медный кабель для того, чтобы он мог быть использован в современных высокоскоростных LAN-сетях Ethernet. Все кабельные каналы должны быть протестированы на максимальных для данного типа кабеля скоростях. Первичными параметрами тестирования, которые должны быть проверены для того, чтобы кабельный канал удовлетворял стандартам TIA/EIA-568-B, являются следующие:

- соответствие карты распайки проводов и контактов разъемов (Wire map);
- входные потери (Insertion loss);
- перекрестные наводки на ближнем конце (Near-end crosstalk — NEXT);
- суммарная мощность перекрестных наводок на ближнем конце (Power sum near-end crosstalk — PSNEXT);
- перекрестные наводки равного уровня на дальнем конце (Equal-level far-end crosstalk — ELFEXT);
- суммарная мощность перекрестных наводок равного уровня на дальнем конце (Power sum equal-level far-end crosstalk — PSELFEXT);
- возвратные потери;
- задержка распространения;
- фактическая длина кабеля;
- смещение задержки (Delay Skew).

Стандарт Ethernet определяет, что каждый из контактов разъема RJ-45 имеет свое назначение, как показано на рис. 4.16. Карта сетевого интерфейса (Network Interface Card — NIC) передает сигналы по контактам 1 и 2, а получает сигналы на контактах 3 и 6. Провода кабеля UTP должны быть соединены с соответствующими контактами на каждом конце кабеля. Проверка соответствия проводов и контактов разъемов обеспечивает отсутствие в кабеле незамкнутых цепей или цепей короткого замыкания.

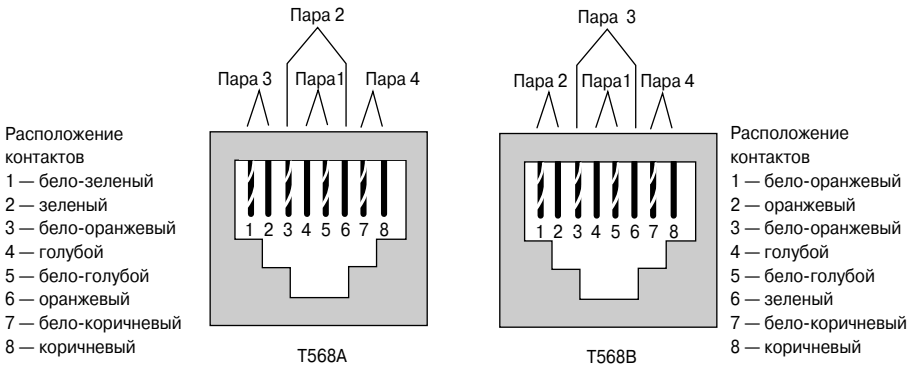


Рис. 4.16. Стандарты Ethernet для разъемов RJ-45

Незамкнутая цепь образуется в том случае, когда провод ненадежно подсоединен к контакту разъема. Короткое замыкание возникает, когда два провода оказываются непосредственно соединены друг с другом.

При проверке соответствия также проверяется, что все восемь проводов на обоих концах кабеля подсоединены к требуемым контактам. Тест подсоединения проводов может обнаруживать несколько различных типов дефектов в проводах. Дефект инвертированной (реверсированной) пары (reversed-pair fault) возникает в том случае, когда проводная пара правильно подсоединена к штекеру на одном конце кабеля, но подсоединена в обратном порядке на другом конце. Как показано на рис. 4.17, если на одном конце кабеля бело-оранжевый провод (провод с белой полосой, или полосатый) подсоединен к контакту 1, а оранжевый — к контакту 2, а на другом, наоборот, оранжевый с полосой подсоединен к контакту 2, а просто оранжевый к контакту 1, то у кабеля появляется дефект инвертированной пары.

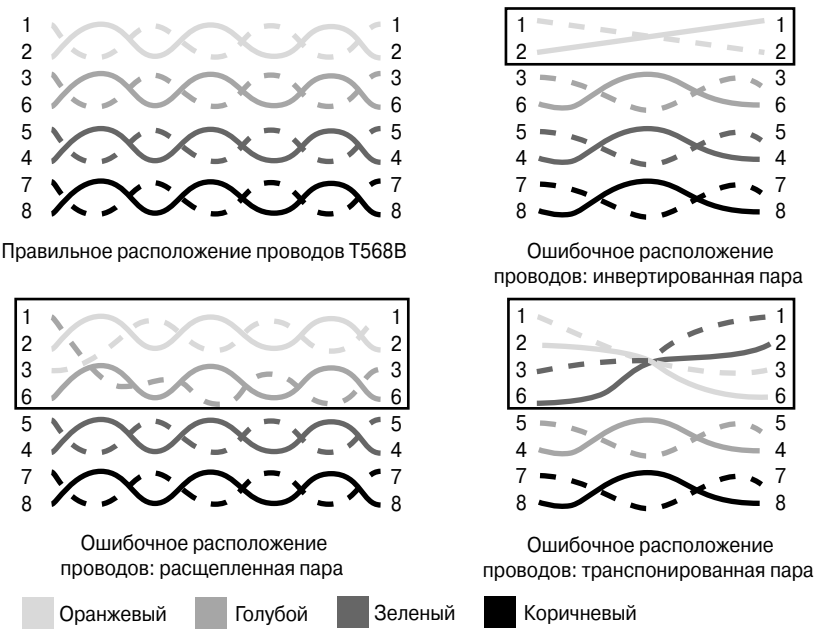


Рис. 4.17. Дефекты кабеля, обнаруживаемые при проверке правильности подключения проводов кабеля к контактам разъема

Дефект кабеля, называемый разделением, или расщеплением пары (split-pair wiring fault), возникает в том случае, когда на обоих концах кабеля два провода от разных пар подсоединены к неправильным контактам. Читателю предлагается самостоятельно найти ошибку в подсоединении проводов к контактам на рис. 4.17. При разделении пары возникают две принимающие или передающие пары, каждая с двумя проводами, которые не скручены друг с другом.

Дефект перестановки пар (transposed-pair wiring fault) возникает в том случае, когда на обоих концах кабеля оба провода пары подсоединены к совершенно разным контактам. Этот случай отличается от описанной выше инвертированной пары, где на обоих концах использованы одни и те же контакты. Транспонированная пара также возникает в том случае, когда два различных цветовых кода на монтажных блоках (punch-down block) (представляющих T568A и T568B) используются в разных местах на одном и том же канале.

Другие параметры тестирования

Сочетание эффектов ослабления сигнала и разрывов импеданса в коммуникационном канале называется *входными потерями (insertion loss)*. Потери при вводе сигнала в кабель измеряются в децибелах и возрастают при увеличении частоты и скорости передачи. Для того чтобы кабель мог быть использован в качестве канала связи в локальной сети, стандарт TIA/EIA-568-B требует, чтобы кабель и его разъемы прошли тест на входные потери.

Перекрестные наводки измеряются в четырех отдельных тестах:

- тесте наводок на ближнем конце NEXT;
- тесте ELFEXT;
- тесте PSELFEXT;
- тесте возвратных потерь (return loss).

Кабельный тестер измеряет параметр NEXT путем подачи тестового сигнала на одну кабельную пару и измерения амплитуды перекрестных наводок в остальных кабельных парах. Значение параметра NEXT, выраженное в децибелах, вычисляется как отношение амплитуд тестового сигнала и наводок, измеряемых на одном и том же конце кабеля. Следует помнить о том, что величина в децибелах, отображаемая тестером, является отрицательной и, соответственно, чем больше эта абсолютная величина, тем ниже уровень потерь NEXT в данной проводной паре.

При тестировании *перекрестных наводок равного уровня на дальнем конце (Equal-level far-end crosstalk — ELFEXT*) измеряется параметр FEXT. Коэффициент ELFEXT в децибелах (dB) определяется как отношение измеренного значения FEXT и входных потерь проводной пары, сигнал которой искажается при FEXT-тестировании. Получаемое при тестировании значение ELFEXT особенно важно в Ethernet-сетях, использующих технологию 1000BASE-T.

Параметр *суммарной мощности перекрестных наводок равного уровня на дальнем конце (power sum equal-level far-end crosstalk — PSELFEXT*) отражает общий эффект наводок ELFEXT от всех проводных пар.

Потери при возвращении сигнала выражают в децибелах величину отраженных сигналов, вызванных разрывами импеданса во всех соединительных точках канала. Необходимо отметить, что главным фактором потерь при возвращении является не ослабление сигнала, а то, что эхо-сигналы, вызванные отражением от точек разрыва импеданса, попадают к получателю с различными интервалами и вызывают дребезжание сигнала.

Временны*е* параметры кабеля или канала

Измерение величины *задержки распространения сигнала (propagation delay*) представляет собой простой метод определения времени, которое требуется сигналу для прохождения по всему тестируемому кабелю. Задержка распространения сигнала в проводе зависит от его длины, степени скручивания и электрических свойств. Она измеряется в сотых долях наносекунды (одна наносекунда (нс) равна одной миллиардной доле секунды, т.е. 0,000000001 с). Для различных категорий кабеля UTP стандарт TIA/EIA-568-B устанавливает различные предельные значения задержки распространения. Измерение задержки распространения является основой для измерения длины кабеля. Стандарт TIA/EIA-568-B-1 определяет, что физическая длина кабеля вычисляется с использованием проводной пары с минимальной электрической задержкой. Тестеры измеряют длину кабеля на основе рефлектометрического теста (Time Domain Reflectometry — TDR), а не по длине оболочки кабеля. Это связано с тем, что провод внутри кабеля перекручен, и в действительности сигнал проходит большее расстояние, чем физическая длина кабеля. При измерении TDR кабельный тестер посылает импульсные сигналы по проводной паре и измеряет время, необходимое для того, чтобы этот импульс вернулся обратно по той же проводной паре.

Тест TDR используется не только для определения длины кабеля, но и для определения расстояния до дефектного участка кабеля, такого, как короткое замыкание или разомкнутая цепь. Если при прохождении по каналу импульс встречается с дефектом, таким, как разрыв цепи, короткое замыкание или ненадежное соединение, то весь импульс или его часть отражаются и вновь поступают на тестер, что позволяет приблизительно определить расстояние до дефектного участка. Такое вычисление может оказаться полезным при нахождении на всей длине кабеля точки ненадежного соединения, например, настенную розетку.

Задержки распространения в различных проводных парах одного и того же кабеля могут несколько различаться в зависимости от степени скручивания и электрических свойств каждой проводной пары. Такое различие значений задержки называется *смещением, или искажением задержки (delay skew*). Оно является критически важным параметром для высокоскоростных сетей, таких, как сети Ethernet 1000BASE-T, в которых данные передаются одновременно по нескольким проводным парам. Если смещение задержки оказывается слишком большим, то биты от различных проводных пар поступают получателю в разные моменты времени, и данные не могут быть правильно собраны в нужном порядке. Даже если в кабельном канале в настоящее время не предполагается передачи данных такого типа, тестирование смещения задержки позволяет удостовериться, что для этого канала возможна модернизация до более высоких скоростей передачи.

Все кабельные каналы локальной сети LAN должны пройти тесты, описанные выше, как этого требует стандарт TIA/EIA-568-B, для того чтобы была уверенность в том, что они будут надежно функционировать и на более высоких скоростях и частотах. Рекомендуется выполнять тестирование кабелей при их прокладке и регулярно впоследствии, для того чтобы убеждаться, что кабель по-прежнему удовлетворяет промышленным стандартам. Чтобы тесты давали правильные и точные результаты,

при тестировании кабелей следует использовать высококачественные приборы. Необходимо аккуратно документировать полученные результаты тестов.

Тестирование оптоволоконных кабелей

Оптоволоконный канал состоит из двух отдельных стеклянных волокон, которые функционируют как отдельные независимые маршруты передачи данных. Одно стекловолокно передает данные в одном направлении, а другое — в обратном. Каждое стекловолокно окружено оболочкой, которая не пропускает свет, поэтому в оптоволоконных кабелях не возникает проблемы перекрестных наводок. Оболочка, внешняя электромагнитная интерференция (EMI) и шумы также не влияют на прохождение сигнала по такому кабелю. Ослабление сигнала имеет место, но оно значительно слабее, чем у медных проводов. Однако в оптоволоконных каналах существует явление, аналогичное разрывам импеданса в каналах на основе кабеля UTP. Когда световой пучок встречается с оптическим разрывом, часть светового сигнала отражается в обратном направлении и лишь часть первоначального светового сигнала продолжает двигаться по каналу в направлении получателя. Это приводит к тому, что к получателю поступает только часть световой энергии, а это затрудняет распознавание сигнала. Так же, как и в кабеле UTP, ненадежные соединения являются главной причиной отражения света и потери мощности сигнала при его прохождении по оптоволоконному кабелю.

Поскольку шумы в оптоволоконных каналах не являются проблемой, основной проблемой при их использовании является обеспечение достаточной мощности сигнала, поступающего к получателю. Если к получателю поступает значительно ослабленный сигнал, то происходят ошибки передачи данных. Тестирование оптоволоконного кабеля в первую очередь включает в себя подачу светового потока в кабель и измерение мощности светового сигнала, который поступает к получателю.

В оптоволоконных каналах требования, касающиеся допустимого ослабления мощности сигнала, которое не нарушает требований получателя, должны быть вычислены. Результат такого вычисления называется бюджетом потерь оптического канала. Прибор, используемый для тестирования оптоволоконного кабеля, проверяет, не превышен ли в канале бюджет потерь. Если кабель не проходит тест, этот прибор указывает, на каком расстоянии от конца кабеля находится оптический разрыв. Обычно проблемы вызываются одним или несколькими ненадежными разъемами. Тестирующий прибор указывает место ненадежных соединений, которые должны быть заменены. После устранения неисправности кабель необходимо протестировать снова.

Новый кабельный стандарт

20 июня 2002 года было опубликовано дополнение к стандарту TIA-568 для кабеля 6-й категории. Официальное название этого стандарта: ANSI/TIA/EIA-568-B.2-1. Новый стандарт определяет первоначальный набор из десяти тестов для кабелей Ethernet-сетей и проходные баллы для каждого из этих тестов. Кабели, сертифицируемые как кабели 6-й категории, должны пройти все десять тестов.

Хотя тесты 6-ой категории (CAT 6) по существу не отличаются от стандартов CAT 5, однако кабели 6-й категории должны пройти эти тесты с более высокими оценками. Кабель CAT 6 должен быть способен передавать сигналы с частотами до 250 МГц и иметь низкие уровни перекрестных наводок и потерь при возврате. Качественный кабельный тестер, аналогичный приборам серии Fluke DSP-4000 или Fluke OMNIScanner2, может выполнить все тестовые измерения, требуемые кабельными сертификатами CAT 5, CAT 5e и CAT 6 для постоянных каналов.

Практическое задание 4.2.9a. Кабельный тестер Fluke 620: проверка соответствия распайки проводов и контактов разъемов
В этой лабораторной работе предлагается изучить распайку проводов сети LAN с помощью кабельного измерителя CableMeter Fluke 620.

Практическое задание 4.2.9b. Кабельный тестер Fluke 620: тестирование кабеля и обнаружение ошибок
В этой лабораторной работе изучается тестирование кабеля, т.е. функции Pass/Fail кабельного измерителя локальных сетей Fluke 620.

Практическое задание 4.2.9c. Кабельный тестер Fluke 620: измерение длины кабеля
В этой лабораторной работе изучается функция измерения фактической длины кабеля с помощью тестера кабельных сетей Fluke 620.

Практическое задание 4.2.9d. Fluke LinkRunner: тестирование локальной сети
В этой лабораторной работе функция LinkRunner измерителя Fluke используется для определения того, активен ли кабельный спуск; определяется его скорость, возможность дуплексного соединения и тип службы. Возможна также проверка соединений на сетевом уровне с помощью команды **`ping`**.

Практическое задание 4.2.9e. Fluke LinkRunner: тестирование кабелей и сетевого адаптера NIC
В этой лабораторной работе функция LinkRunner измерителя Fluke используется для определения длины и проверки целостности кабеля, а также определяется место, где кабель заканчивается (terminates). Возможно также тестирование функций сетевого адаптера NIC.

Резюме

В этой главе были рассмотрены перечисленные ниже основные темы и определения.

- Волны создаются возмущениями среды и представляют собой энергию, перемещающуюся из одного места в другое. Все волны имеют такие характеристики, как амплитуда, период и частота.
- Синусоидальные волны представляются периодическими непрерывными функциями. Аналоговые сигналы имеют вид синусоидальных волн.

- Импульсы (прямоугольные волны) представляют собой периодические функции, значение которых остается постоянным в течение некоторого времени, а затем резко изменяется. Импульсами представляются цифровые сигналы.
- Для больших чисел часто используется представление в виде основания со степенью. Возведение основания в определенную степень эквивалентно умножению числа на само себя соответствующее количество раз (например, $10^3 = 10 \times 10 \times 10 = 1000$).
- Логарифмы связаны с представлением числа в виде основания со степенью. Логарифм по основанию 10 числа равен показателю степени, в которую нужно возвести число 10 для того, чтобы получить данное число (например, $\log_{10} 1000 = 3$, поскольку $10^3 = 1000$).
- Децибелы описывают степень усиления или ослабления сигнала. Отрицательные значения соответствуют ослаблению, а положительные — усилению сигнала.
- Временной анализ дает на экране осциллографа графическое представление зависимости напряжения или тока от времени. Частотный анализ графически представляет изменение напряжения или мощности в зависимости от частоты с использованием спектрального анализатора. Частотный анализ представляет собой графическое отображение зависимости напряжения или мощности от частоты, получаемое с помощью спектрального анализатора.
- В сфере коммуникаций под шумом понимаются нежелательные сигналы. Шумы могут вызываться другими кабелями, радиочастотами (RFI) и электромагнитным излучением (EMI). Белый шум затрагивает все частоты, в то время как узкополосный шум воздействует только на некоторые частоты.
- Под аналоговой полосой пропускания понимается диапазон частот, связанных с определенным типом аналоговой передачи, таким, например, как телевидение или FM-радио.
- Ширина цифровой полосы пропускания характеризует объем информации, который может быть передан из одного места в другое за определенный промежуток времени. В качестве единиц измерения используются различные количества битов в секунду.
- Глубокое усвоение затронутых в настоящей главе тем важно для понимания различных концепций тестирования кабелей, рассмотренных в следующей главе.
- Физический уровень эталонной модели OSI является тем уровнем, на котором имеют место большинство проблем локальных сетей. Единственным способом предотвратить или устранить эти проблемы является использование кабельных тестеров. Знание возможных источников шума в среде LAN важно для правильной установки кабельных разъемов и отрезков кабеля.
- Медная среда передачи может быть экранированной или нет. Неэкранированный кабель больше, чем экранированный, подвержен влиянию шумов.

- Деградация сигнала может быть вызвана многими факторами: шумом, затуханием, несоответствием импеданса и перекрестными наводками. Все перечисленные факторы значительно уменьшают производительность сети.
- Стандарт TIA/EIA-568-B требует проведения для каждого медного кабеля десяти тестов, чтобы создаваемая сеть соответствовала современным требованиям к высокоскоростным локальным сетям технологии Ethernet.
- Согласно сетевым стандартам, оптическое стекловолокно также необходимо тестировать после установки.
- Кабель категории 6 отвечает более жестким частотным требованиям, чем самый распространенный сегодня кабель категории 5, и именно его рекомендуется использовать для современных сетей.

Ключевые термины

Амплитуда (amplitude) электрического сигнала представляет его высоту, однако измеряется не в метрах, а в вольтах.

Анализатор спектра (spectrum analyzer) — электронное устройство, вычерчивающее графики зависимости различных величин от частоты. В инженерной практике используется для анализа спектра (т.е. составляющих) различных сигналов.

Аналоговая полоса пропускания (analog bandwidth) — этот термин обычно применяется по отношению к диапазону частот аналоговой электронной системы. Термин может также использоваться для описания диапазона частот, передаваемых радиостанцией или электронным усилителем.

Белый шум (white noise) — это шум, в равной степени затрагивающий все частоты передачи.

Внешние наводки (alien crosstalk) — наводки, вызываемые сигналами, проходящими вне кабеля.

Волна (Wave) представляет собой перемещение энергии из одного места в другое.

Входные потери (insertion loss) представляют собой сочетание эффектов ослабления сигнала и разрывов импеданса в канале связи.

Герц (hertz) — единица измерения частоты электрического сигнала, отражающая количество полных циклов в секунду.

Децибел (decibel) — важный способ описания сетевых сигналов в единицах, отражающих уменьшение или увеличение энергии электромагнитной волны. Значение в децибелах обычно отрицательно, поскольку оно отражает потерю энергии по мере прохождения волны, однако оно может быть и положительным, отражая увеличение энергии сигнала, если он усиливается.

Задержка распространения (propagation delay) — это легко вычисляемая величина, показывающая, сколько времени требуется сигналу для прохождения тестируемого кабеля.

Затухание сигнала (attenuation) представляет собой уменьшение амплитуды сигнала по мере его прохождения по каналу.

Импеданс (impedance) — величина, характеризующая сопротивление кабеля переменному току (AC), измеряется в омах.

Импульс (pulse) характеризует значение передаваемых данных. Если возмущение вызвано целенаправленно и имеет фиксированный и предсказуемый характер, оно называется импульсом.

Интерференция в радиочастотном диапазоне (RFI — radio frequency interference) представляет собой шум от сигналов, передаваемых вблизи кабеля.

Логарифм — это число, показывающее, в какую степень надо возвести основание для получения заданного числа.

Осциллограф (Oscilloscope) — электронное устройство, используемое для наблюдения электрических сигналов, таких, как волны и импульсы напряжения.

Перекрестные наводки (crosstalk) — это передача сигнала от одной проводной пары близлежащим. Смежные проводные пары того же кабеля при этом действуют как антенны, генерируя слабый, но подобный передаваемому электрический сигнал, который может интерферировать передаваемые по этим парам собственные сигналы.

Перекрестные наводки на дальнем конце (FEXT — far-end crosstalk) представляют собой наводки, возникающие в том случае, когда сигналы одной витой пары вступают во взаимодействие с сигналами другой пары при поступлении на дальний конец кабельной системы с несколькими парами.

Перекрестные наводки равного уровня на дальнем конце (ELFEXT — equal-level far-end crosstalk) — тест, в котором замеряется значение FEXT.

Перекрестные наводки на ближнем конце (NEXT — near-end crosstalk) — величина, измеряемая как отношение амплитуд напряжений тестового сигнала и возникающих помех при измерении на одном и том же конце канала.

Прямоугольные волны (square waves) — график величины, которая не изменяется непрерывно во времени. Такие величины остаются постоянными в течение некоторого времени, затем внезапно изменяют свое значение, снова сохраняют новое значение, а затем внезапно возвращаются к первоначальному значению.

Синусоидальные волны (sine waves) — графическое изображение математических функций, описывающих многие природные явления, регулярно происходящие во времени, такие, например, как изменение расстояния от Земли до Солнца, расстояние до земли точки вращающегося "чертового колеса" или время восхода солнца.

Смещение задержки (delay skew) — величины задержки распространения в различных парах одного и того же кабеля могут несколько отличаться ввиду различного количества оборотов скручивания и различий электрических параметров пар. Под смещением задержки понимаются такие различия задержки между парами.

Стандарт TIA/EIA-568-B определяет десять тестов, которые должен пройти медный кабель для того, чтобы быть пригодным к использованию в современных высокоскоростных локальных сетях Ethernet.

Суммарная мощность помех на ближнем конце (PSNEXT — power sum near-end crosstalk) — величина, характеризующая кумулятивный эффект потерь NEXT от всех проводных пар кабеля.

Суммарная мощность помех равного уровня на дальнем конце (power sum equal-level far-end crosstalk — PSELFEXT) описывает суммарный эффект потерь ELFEXT от всех проводных пар.

Узкополосная интерференция (narrowband interference) представляет собой помехи, затрагивающие лишь узкий диапазон частот.

Флуктуации фазы (дребезжание сигнала, jitter) представляют собой малые отклонения времени получения сигнала или его фазы, которые могут привести к ошибкам в передаваемых данных или потере синхронизации. Чем длиннее кабель, тем бо́льшие отклонения могут в нем присутствовать. Отклонения также зависят от величины затухания сигнала, скорости передачи и частот. В телефонии этим термином обозначают дребезг контактов.

Цифровая полоса пропускания (digital bandwidth) описывает объем информации, который может быть передан из одного места в другое за определенное количество времени.

Частота (frequency) — промежуток времени между отдельными волнами.

Шум (noise) — в сфере коммуникации под шумом понимаются нежелательные сигналы. Шумы могут вызываться естественными или технологическими источниками и в коммуникационных системах добавляются к полезному сигналу.

Электромагнитная интерференция (EMI — electromagnetic interference) представляет собой шум от близлежащих источников, таких, как двигатели и источники света.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Какое из указанных ниже описаний относится к оптоволокну?

а) Это среда, в которой используется мощная лампа накаливания.

б) Это среда, сердцевина которой сделана из кевлара с высоким коэффициентом преломления.

в) Это среда, в которой используется эффект полного внутреннего затухания.

г) Это среда, скорость передачи информации в которой превышает скорость передачи для остальных сред.

2. Что такое затухание сигнала?

а) Уменьшение мощности сигнала.

б) Увеличение амплитуды сигнала.

в) Задержка распространения сигнала.

г) Время, которое требуется сигналу для достижения пункта назначения.

3. Что обычно является причиной перекрестных наводок?

а) Неправильная или некачественная запрессовка разъемов на концах кабеля.

б) Отсутствие общего нулевого сигнала в кабеле.

в) Помехи от переменного тока блока питания расположенного рядом монитора или жесткого диска компьютера.

г) Радиосигналы FM-станций, сигналы телевещания, помехи от остального офисного оборудования.

4. Какие из перечисленных ниже тестов являются обязательными для медного кабеля в рамках стандарта TIA/EIA-B? (Выберите все приемлемые ответы.)

а) Измерение гармоник сигнала.

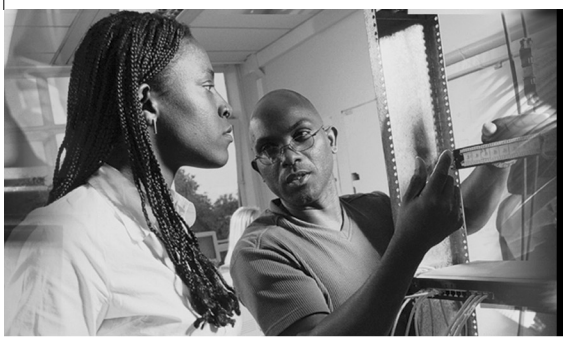
б) Проводимость материала.

в) Карта распайки разъемов.

г) Уровень поглощения сигнала.

д) Входные потери.

е) Задержка распространения сигнала.



ГЛАВА 5

Кабельные соединения сетей LAN и WAN

В этой главе...

описаны среды передачи данных, которые используются на физическом уровне современных локальных сетей, их преимущества и недостатки; рассказано, как технология Ethernet используется в территориальных сетях;

- описаны требования к разъемам для различных типов Ethernet-сред;
- рассматриваются разновидности соединений, которые используются в различных реализациях технологий физического уровня;
- рассказывается, зачем необходимы разъемы RJ-45, в каких ситуациях используется прямой кабель, а в каких — перекрещенный;
- описаны ситуации, когда и зачем нужно использовать консольный кабель;
- дано определение, что такое повторитель;
- рассказывается, что такое концентратор, и описываются их три типа;
- описаны стандартные методы использования беспроводных сетей;
- рассмотрены две наиболее распространенные технологии беспроводных сетей;
- описаны основные функции мостов;
- описаны основные функции сетевых плат;
- объясняется, почему сетевая плата компьютера считается сетевым устройством второго уровня;
- описана одноранговая сеть и рассмотрен принцип ее работы;
- описаны клиент-серверные структуры и сети;
- рассмотрены методы реализации технологий физического уровня распределенных сетей;
- описаны основные функции устройств CSU/DSU;
- рассказывается, что такое DTE и DCE-устройства;
- описан метод именования интерфейсов в маршрутизаторах;
- рассказано, как установить консольное соединение с устройствами Cisco;
- рассмотрены BRI-соединения маршрутизаторов;

- рассмотрены сходства и отличия мостов и коммутаторов;
- рассмотрены преимущества коммутаторов;
- описаны соединения технологии DSL;
- описаны кабели, которые используются для подключения к маршрутизаторам.

Ключевые определения главы

Ниже дан список основных определений главы, полные расшифровки терминов приведены в конце:

RJ-45, с. 264,
интерфейс подключаемых устройств, с. 266,
конвертер гигабитового интерфейса, с. 266,
прямой кабель, с. 269,
перекрещенный кабель, с. 269,
повторитель, с. 272,
активный концентратор, с. 274,
интеллектуальный концентратор, с. 274,
пассивный концентратор, с. 274,
одноранговая система, с. 281,
консольный кабель, с. 297.

Несмотря на то что каждая локальная сеть (LAN) в какой-то степени уникальна, многие аспекты дизайна инфраструктуры являются общими для всех сетей. Например, большинство локальных сетей соответствуют одним и тем же стандартам и содержат одинаковые компоненты. В этой главе основное внимание уделяется Ethernet-сетям и наиболее распространенным устройствам сетей LAN.

В соединениях распределенных сетей (WAN) на сегодняшний день могут быть использованы различные технологии: от коммутируемого доступа по телефонной сети до широкополосного канала. Средства распределенных сетей отличаются шириной полосы пропускания, стоимостью и тем оборудованием, которое для них требуется. В текущей главе подробно описаны несколько разновидностей соединений сетей WAN.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Прокладка кабелей в локальных сетях

Кабельная система локальной сети относится к первому уровню эталонной модели OSI. Для того чтобы правильно выбрать нужные типы кабелей для соединения между собой сетевых устройств, необходимо хорошо понимать реализацию физического уровня в локальных сетях спецификации Ethernet, которая описывает технологию LAN-сетей, определяемую на канальном уровне.

При проектировании сети важно знать области использования различных типов кабелей и правильно выбрать типы разъемов, используемых для подключения к сети Ethernet.

В этом разделе описываются реализация физического уровня LAN-сети и основные принципы реализации технологии Ethernet в территориальной локальной сети (campus LAN). В этой главе также обсуждаются различные типы разъемов, рекомендуемых для использования в сетях Ethernet, и стандарты проводов кабелей UTP.

Физический уровень локальной сети

Среда Ethernet представляет собой наиболее часто используемую технологию локальных сетей. Впервые сеть Ethernet была реализована группой, получившей название DIX (корпорации Digital, Intel и Xerox). Группой DIX была создана и реализована первая спецификация LAN-сети Ethernet, которая послужила базой появившегося в 1980 году стандарта 802.3 Института инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineer — IEEE). Позднее институт IEEE расширил группу, разрабатывавшую стандарт 802.3, до трех новых комитетов, известных как 802.3u (Fast Ethernet), 802.3z (гигабитовая технология Ethernet с использованием оптоволоконного кабеля [Gigabit Ethernet over Fiber]) и 802.3ab (гигабитовая технология Ethernet с использованием кабеля UTP [Gigabit Ethernet over UTP]).

Кабельный аспект LAN-сетей рассматривается на первом уровне эталонной модели взаимодействия открытых систем (Open System Interconnection — OSI). LAN-сети поддерживаются многими топологиями и физическими передающими средами. На рис. 4.1 показано подмножество реализаций физического уровня, которые могут быть использованы для сети Ethernet.

Для обозначения различных передающих сред используются определенные пиктограммы. Например, для последовательной линии используется символ, напоминающий удлиненную букву “z” или разряд молнии; для сети Ethernet обычно используется символ, состоящий из прямой линии и перпендикулярно отходящих от нее отрезков; символом сети Token Ring является окружность с подсоединенными к ней узлами, а для сетей FDDI — две концентрические окружности с подсоединенными к ним устройствами, как показано на рис. 5.2.

Базовой функцией передающей среды является передача информации в форме битов или байтов по локальной сети LAN. За исключением беспроводных сетей LAN (в которых в качестве среды выступает атмосфера или пространство), в остальных видах сетевых сред сетевые сигналы заключены в проводе, кабеле или оптоволоконном

кабеле. Сетевая передающая среда рассматривается как компонент первого уровня локальной сети.

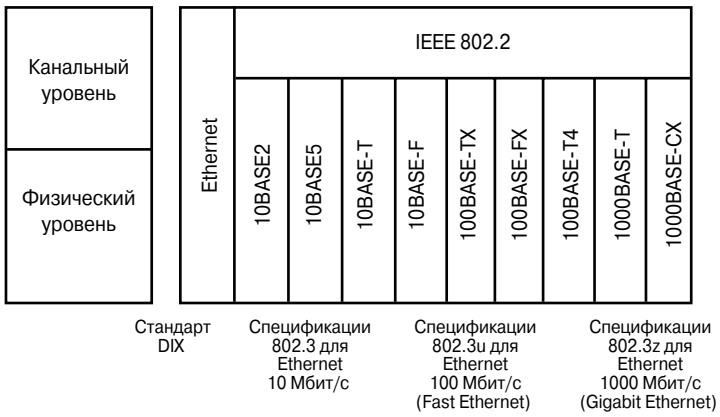


Рис. 5.1. Стандарты LAN-сетей на физическом уровне

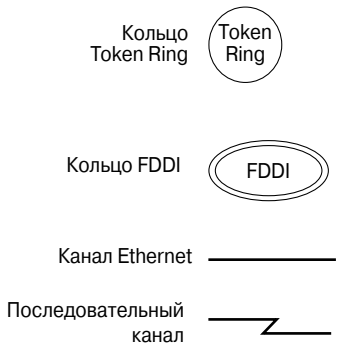


Рис. 5.2. Пиктограммы соединений физического уровня передающих сред локальных сетей

Компьютерные сети могут быть построены с использованием различных передающих сред. Каждая сетевая среда имеет свои достоинства и недостатки. Показатель, который является достоинством для одной среды (например, невысокая стоимость у кабеля CAT5), может оказаться недостатком для другой (например, для дорогостоящего оптоволоконного кабеля). Первичными параметрами при оценке преимуществ и недостатков передающих сред являются следующие:

- максимально допустимая длина кабеля;
- стоимость;
- простота установки;
- подверженность интерференции.

Передавать сетевые сигналы могут коаксиальный кабель, оптоволоконный кабель и даже вакуум. Однако основной средой, которая подробно рассматривается в этой главе, является неэкранированный кабель витой пары 5-й категории (Category 5 Unshielded Twisted-Pair cable — CAT 5 UTP).

Использование технологии Ethernet в территориальных сетях

Учитывая разнообразие скоростей технологии Ethernet, используемых в территориальных сетях, необходимо определить, требуется ли в каких-либо областях сети провести модернизацию до одной из разновидностей Fast Ethernet. При правильно подобранных аппаратном обеспечении и кабельной инфраструктуре соединения 10 Мбит/с или 100 Мбит/с могут быть реализованы в любой части сети. Как показано в табл. 5.1, Ethernet-соединения со скоростью 10 Мбит/с обычно используются на уровне конечного пользователя для подсоединения настольных рабочих станций, а более скоростные технологии применяются для соединения между собой серверов и сетевых устройств, таких, как маршрутизаторы и коммутаторы.

Таблица 5.1. Рекомендации по выбору Ethernet-соединений

	Ethernet 10BASE-T	Fast Ethernet	Gigabit Ethernet
Соединения уровня конечного пользователя (между устройством конечного пользователя и устройством рабочей группы)	Обеспечивают соединение между устройствами конечного пользователя и коммутаторами уровня пользователя	Предоставляют высокопроизводительным рабочим станциям (PC) доступ к серверам со скоростью 100 Мбит/с	На этом уровне, как правило, не используются
Уровень рабочей группы (соединение устройства рабочей группы с магистралью)	На этом уровне, как правило, не используются	Обеспечивают соединение между конечным пользователем и рабочей группой; между рабочей группой и магистралью; между блоком серверов и магистралью	Обеспечивают высокоскоростные каналы между рабочей группой и магистралью; высокоскоростные каналы к блоку серверов
Уровень магистрали	На этом уровне, как правило, не используются	Обеспечивают соединения с приложениями, которым требуется небольшая или средняя ширина полосы пропускания (low- to medium-volume)	Обеспечивают соединения между высокоскоростными магистралями и сетевыми устройствами

В современных сетях, несмотря на возможность обеспечить соединения по технологии Gigabit Ethernet от магистрали вплоть до конечного пользователя, стоимость кабелей и портов коммутаторов могут сделать такое решение практически неосуществимым. Перед принятием решения в такой ситуации необходимо правильно определить потребности сети. Например, в сети, работающей с традиционными Ethernet-скоростями, легко может возникнуть переполнение, если в ней будут работать программные продукты нового поколения: мультимедиа, графические приложения и системы управления базами данных.

В целом Ethernet-технологии могут быть использованы в территориальных LAN-сетях несколькими приведенными ниже способами.

- На уровне пользователя достаточно высокая производительность может быть получена с использованием соединений Fast Ethernet. Технологии Fast Ethernet и Gigabit Ethernet могут быть использованы для клиентов или серверов, которым требуется широкая полоса пропускания.
- Технология Fast Ethernet часто используется в качестве канала между сетевыми и устройствами уровня пользователя; при этом поддерживается агрегирование потоков данных от всех Ethernet-сегментов в канал доступа.
- Во многих сетях типа "клиент-сервер" возникают проблемы оттого, что многие клиенты пытаются получить доступ к одному и тому же серверу, создавая переполнение в точке подсоединения сервера к LAN-сети. Для того чтобы повысить производительность модели "клиент-сервер" в территориальной LAN-сети и избежать заторов на сервере, следует использовать каналы Fast Ethernet или Gigabit Ethernet для соединения между собой серверов предприятия. Технологии Fast Ethernet и Gigabit Ethernet предоставляют эффективное решение проблемы слишком медленно работающей сети.
- Каналы Fast Ethernet могут также быть использованы для обеспечения соединений между уровнем рабочих групп и магистралью. Поскольку модель территориальной сети LAN поддерживает двойные (dual) каналы между каждым маршрутизатором рабочей группы и коммутатором магистрали, становится возможным перераспределение нагрузки (load balance) для агрегированных потоков данных от коммутаторов множественного доступа к каналам.
- Технологии Fast Ethernet (и Gigabit Ethernet) могут быть использованы в соединениях между коммутаторами и магистралью. В соединениях между магистральными коммутаторами следует использовать среду с максимальной скоростью, которую может позволить себе предприятие.

Требования к среде Ethernet и разъемам

В дополнение к потребностям сети и еще до выбора конкретной реализации технологии Ethernet необходимо рассмотреть требования к среде и разъемам. Используемые для поддержки конкретной реализации сети Ethernet кабели и разъемы определяются органами стандартизации Ассоциации электронной промышленности и (новые стандарты) Ассоциации телекоммуникационной промышленности (Electronic Industries

Association/Telecommunications Industry Association — EIA/TIA). Категории кабелей для сетей Ethernet определяются стандартами EIA/TIA-568 (SP-2840) на провода для кабелей промышленных коммерческих телекоммуникаций. Ассоциации EIA/TIA определяют для кабелей UTP использование разъема *RJ-45*. Аббревиатура *RJ* означает *registered jack (зарегистрированный разъем)*, а число 45 относится к модели физического разъема, имеющего восемь проводников.

В табл. 5.2 сравниваются спецификации кабелей и разъемов для типичных реализаций Ethernet. Наиболее важным является различие сред, используемых в сетях Ethernet со скоростью передачи 10 Мбит/с, с одной стороны, и Ethernet-технологий, которые работают на скорости 100 Мбит/с и 1000 Мбит/с, с другой. В современных сетях, в которых наблюдается сочетание требований технологий с использованием скоростей 10 Мбит/с и 1000 Мбит/с, необходимо переходить на использование кабеля UTP CAT 5 для поддержки среды Fast Ethernet.

На рис.5.3 показаны различные типы соединений, используемых при реализации физического уровня.

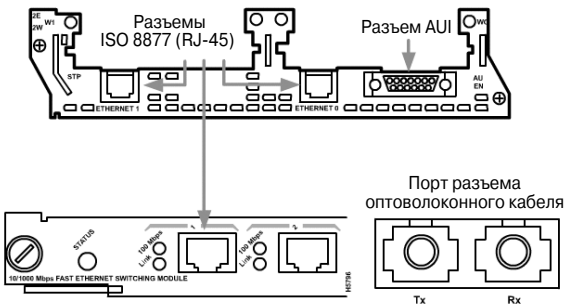


Рис. 5.3. Различные типы разъемов

Типы соединений

В этом разделе кратко описываются типы соединений, используемых при реализации физического уровня сети, и интерфейсное устройство — конвертер гигабитового интерфейса (Gigabit Interface Converter — GBIC), который используется в качестве "переходника" между системами Ethernet и оптоволоконными системами. В этом разделе рассматриваются следующие устройства:

- **RJ-45** — разъем, используемый на конце кабеля витой пары;
- **AUI** — разъем, служащий интерфейсом между сетевой картой компьютера или интерфейсом маршрутизатора, с одной стороны, и кабелем Ethernet — с другой;
- **GBIC** — конвертор, используемый в качестве интерфейса между системой Ethernet и оптоволоконной системой.

Таблица 5.2. Сравнение требований к передающей среде Ethernet

	Тип передающей среды	Максимальная длина сегмента (м, в скобках — футов)	Тип топологии	Разъем
10BASE2	Коаксиальный кабель 50 Ом (thinnet)	185 (606,94)	Шинная	British Naval Connector (BNC)
10BASE5	Коаксиальный кабель 50 Ом (thicknet)	500 (1640,4)	Шинная	Интерфейс подсоединяемого модуля (Attachment unit interface AUI)
10BASE-T	EIA/TIA CAT 3, 4, 5 UTP, две пары	100 (328)	Звездообразная	ISO 8877 (RJ-45)
100BASE-TX	EIA/TIA CAT 5 UTP, две пары	100 (328)	Звездообразная	ISO 8877 (RJ-45)
100BASE-FX	62.5/125 многомодовый оптоволоконный кабель	400 (1312,3)	Звездообразная	Сдвоенный разъем для подключения к среде: ST или SC
1000BASE-CX	STP	25 (82)	Звездообразная	ISO 8877 (RJ-45)
1000BASE-T	EIA/TIA CAT 5 UTP, четыре пары	100 (328)	Звездообразная	ISO 8877 (RJ-45)
1000BASE-SX	62.5/50 многомодовый оптоволоконный микрокабель	275 (853) для оптоволоконного кабеля 62,5 мкм; 550 (1804,5) для оптоволоконного кабеля 50 мкм	Звездообразная	SC
1000BASE-LX	62,5/50 мкм многомодовый оптоволоконный кабель; 9 мкм многомодовый оптоволоконный кабель	440 (1443,6) для оптоволоконного кабеля 62,5 мкм; 550 (1804,5) для оптоволоконного кабеля 50 мкм; от 3000 до 10000 для одномодомового оптоволоконного кабеля	Звездообразная	SC

Разъем RJ-45

Разъем RJ-45 и соответствующее гнездо используются наиболее часто. Соединения RJ-45 будут подробно обсуждаются в разделе “Кабель UTP и его установка” этой главы.

Интерфейс подключаемых устройств

В некоторых случаях тип гнезда на плате сетевой карты (NIC) не соответствует типу среды, к которой его следует подсоединить. Существует специальный *интерфейс подключаемых устройств* (Attachment Unit Interface — AUI), который позволяет решить указанную проблему. Этот физический разъем имеет 15 контактов и служит интерфейсом между адаптером сетевой карты (NIC) и кабелем Ethernet. В Ethernet-сетях стандарта 10BASE5 (thicknet) используется короткий кабель для соединения интерфейса AUI на компьютере с трансивером на главном кабеле. В Ethernet-сетях стандарта 10BASE2 (thinnet) коаксиальный кабель Ethernet подсоединяется непосредственно к адаптеру NIC в задней части компьютера.

Дополнительная информация: конвертер гигабитового интерфейса

Конвертер гигабитового интерфейса (Gigabit Interface Converter — GBIC) представляет собой заменяемое без выключения питания (hot-swappable) устройство ввода-вывода, которое подсоединяется к порту Gigabit Ethernet. Основное преимущество конвертеров GBIC состоит в том, что они взаимозаменяемы. Это их свойство предоставляет пользователям дополнительную гибкость при размещении технологии 1000BASE-X без необходимости менять физический интерфейс (или модуль) на маршрутизаторе или коммутаторе.

Оптоволоконный конвертер GBIC представляет собой трансивер, который преобразует постоянный электрический ток в оптический сигнал, оптические сигналы — в электрические токи, которые соответствуют цифровому сигналу. Типичные оптические конверторы GBIC могут работать со следующими средами:

- коротковолновыми (1000BASE-SX);
- длинноволновыми соединениями дальней связи (1000BASE-LX/LH);
- технологиями с расширенной дистанцией (1000BASE-ZX).

Обычно конвертеры GBIC используются в качестве интерфейса между Ethernet-системами и оптоволоконными системами Fiber Channel и Gigabit Ethernet. На рис. 5.4 показан конвертор GBIC, а на рис. 5.5 изображен модуль Gigabit Ethernet Cisco модели WS-X2931 без конвертера GBIC.

Рис. 5.4. Конвертер GBIC

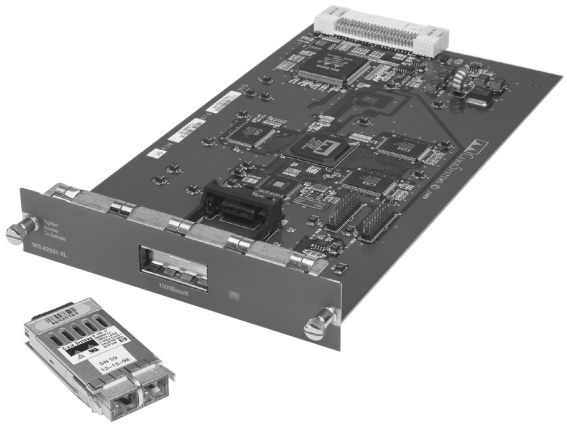


Рис. 5.5. Модуль Gigabit Ethernet Cisco WS-X2931 с извлеченным конвертером GBIC

Кабель UTP и его установка

Если посмотреть на прозрачный штекер RJ-45 на конце кабеля UTP, то можно увидеть восемь цветных проводов. Эти провода скручены в четыре пары. На четыре провода (две пары) подается положительное (или настоящее) напряжение; это сигнальные провода ("tip", от T1 до T4); остальные четыре (от R1 до R4) заземлены и передают инверсное (или фиктивное) напряжение и называются нулевым уровнем ("ring"). Термины tip и ring (контакт и заземление) появились в первые дни появления телефона. В настоящее время эти термины относятся к положительному и отрицательному контактам в проводной паре. Эти два провода в первой проводной паре кабеля или гнезда обозначаются как T1 и R1, во второй паре — как T2 и R2, и т.д.

Разъем RJ-45 запрессован на конце кабеля и является внешней частью разъема. Если посмотреть на него с лицевой части (т.е. когда зажим направлен вниз), то контакты нумеруются от 8 до 1 слева направо, как показано на рис. 5.6. Гнездо, показанное на рис. 5.7, представляет собой внутренний (female) компонент разъема и встраивается в сетевое устройство, стену, в напольную розетку или в распределительную панель. Если смотреть со стороны порта устройства, то контакты гнезда нумеруются от 1 до 8 слева направо.

Для того чтобы токи в разъеме проходили в правильном направлении, порядок проводов в штекере и гнезде должен соответствовать стандартам EIA/TIA-568-A и EIA/TIA-568-B.

Кроме правильного выбора кабеля соответствующей категории EIA/TIA для соединения устройств (что определяется стандартом распайки, используемым в разъеме), необходимо также определить, какой из приведенных ниже двух типов кабелей будет использоваться:

- *прямой кабель (straight-through)*, в котором порядок контактов остается неизменным по всей длине кабеля, и таким образом контакт 1 остается одним и тем же на обоих концах кабеля;

- *перекрещенный кабель (crossover*), в котором контакты в каждой паре на конце кабеля инвертируются (меняются местами) для передачи и приема сигналов в требуемом порядке.

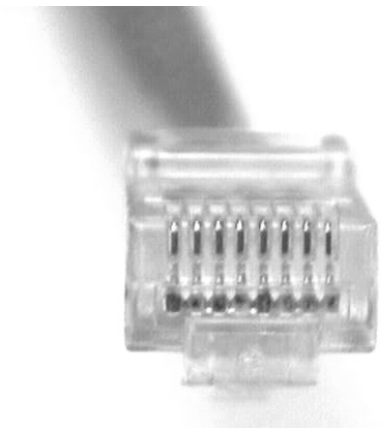


Рис. 5.6. Расположение контактов в разъеме RJ-45

Рис. 5.7. Гнездо RJ-45 и порядок проводов в нем

Если расположить рядом два конца кабеля с разъемами RJ-45, то в каждом из них видны цветные провода (или контакты). Если порядок цветных проводов на каждом конце один и тот же, то такой кабель называется прямым (straight-through). На рис. 5.8 показано, что порядок проводов обоих разъемов одинаков.

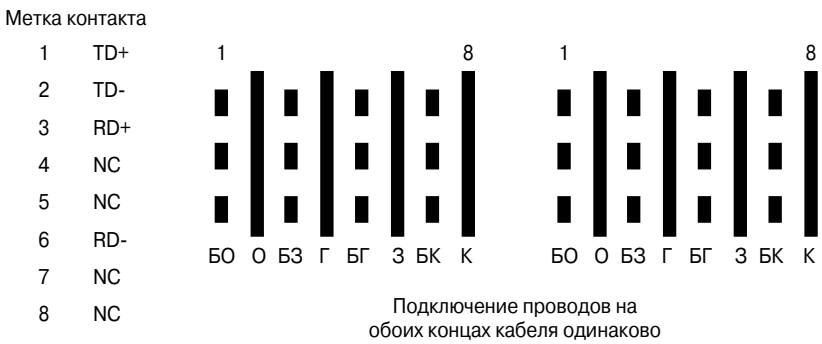


Рис. 5.8. Прямой кабель UTP

Согласно спецификации Ethernet, в кабеле UTP категории 5 для передачи сигналов (TD) и приема (RD) используются только провода 1, 2, 3 и 6. Остальные четыре провода не используются. Как показано на рис. 5.8, в прямом кабеле RJ-45 контакты 1, 2, 3 и 6 на одном конце соединения соединены с контактами 1, 2, 3 и 6 на другом конце. Однако в технологии Gigabit Ethernet используются все восемь проводов.

Прямой кабель может быть использован для соединения между собой таких устройств, как PC или маршрутизаторы, с другими устройствами, такими, как концентраторы или коммутаторы. Как показано на рис. 5.9, прямой кабель может использоваться только в том случае, когда лишь один конец кабеля подсоединен к порту устройства, обозначенному символом *x*[1].

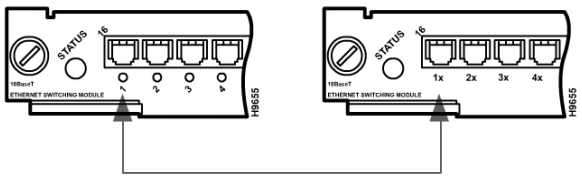
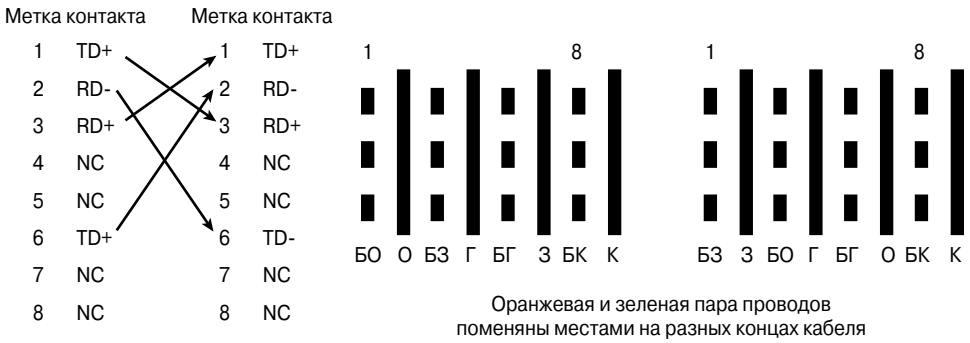


Рис. 5.9. Соединение устройств с помощью прямого кабеля

При использовании перекрещенного кабеля по разъемам RJ-45 на двух концах кабеля можно обнаружить, что некоторые контакты одного конца кабеля на другом конце кабеля подсоединены к иным контактам. В частности, для сетей Ethernet контакт 1 на одном конце кабеля RJ-45 на другом конце подсоединен к контакту 3, а контакт 2 — к контакту 6, как показано на рис. 5.10.



БО — бело-оранжевый
О — оранжевый
БЗ — бело-зеленый
Г — голубой
БГ — бело-голубой
З — зеленый
БК — бело-коричневый
К — коричневый

Рис. 5.10. Перекрещенный кабель UTP

[1] *Символом* x *обычно обозначают разъем с перекрестной распайкой, например, магистральный разъем концентратора, им же помечают и соответствующий тип кабеля — перекрестный. — Прим. ред.*

Перекрещенный кабель может быть использован для соединения между собой “одинаковых” устройств, например, коммутатора с другим коммутатором или коммутатора с концентратором. На рис. 5.11 показано, что инвертированный кабель используется в тех случаях, когда на портах обоих устройств, соединенных таким кабелем, присутствует символ *x* или на обоих такой символ отсутствует.

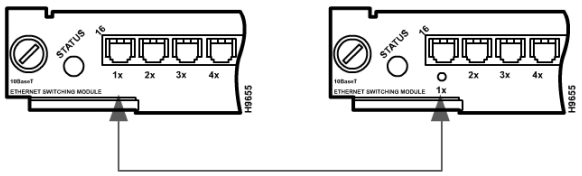


Рис. 5.11. Соединение устройств инвертированным кабелем

Ниже приводятся рекомендации по выбору типа кабеля для соединения между собой сетевых устройств.

Прямой кабель следует использовать для соединения:

- коммутаторов с маршрутизаторами;
- коммутаторов с ПК или серверами;
- концентраторов с ПК или серверами.

Инвертированный кабель следует использовать для соединения:

- коммутаторов с коммутаторами;
- коммутаторов с концентраторами;
- концентраторов с концентраторами;
- маршрутизаторов с маршрутизаторами;
- ПК с ПК;
- маршрутизаторов с ПК.

Презентация: прямой кабель
В этой презентации показан прямой кабель.

Презентация: перекрещенный кабель
В этой презентации показан перекрещенный кабель.

Практическое задание. Запрессовка разъема RJ-45
В этой лабораторной работе рассмотрен процесс правильной запрессовки разъема RJ-45 и описана процедура установки разъема в настенную розетку.

Повторители

Сети LAN объединяют между собой много устройств различных типов. Они называются аппаратными компонентами локальных сетей. В последующих разделах обсуждаются некоторые типовые компоненты аппаратного обеспечения, используемые в среде LAN. Устройства сетей LAN могут включать в себя повторители, концентраторы, мосты, а также коммутаторы и маршрутизаторы, которые преобладают в современных локальных сетях.

Как упоминалось выше, существует множество различных передающих сред, каждая из которых имеет свои достоинства и недостатки. Одним из недостатков кабеля категории 5 UTP является ограничение на длину кабеля. Максимальная длина кабеля UTP для одного участка сети составляет 100 м (примерно 333 фута). Если требуется большее расстояние, то нужно использовать повторители. В большинстве современных сетей Ethernet вместо повторителей используются концентраторы, которые являются многопортовыми повторителями или коммутирующими устройствами, созданными на основе новых технологий.

Термин *повторитель* возник в давнюю эпоху визуальных коммуникаций, когда человек, находящийся на холме, повторял сигнал, только что полученный от человека, находящегося на предыдущем холме, для того чтобы передать его тому, кто находится на следующем холме. Повторители используются для передачи сигнала на дальние расстояния в телеграфии, телефонии, в СВЧ-связи и в оптических коммуникациях.

Назначение повторителей, показанных на рис. 5.12 и 5.13, состоит в регенерации и ресинхронизации сетевых сигналов на битовом уровне для того, чтобы они могли пройти большее расстояние по передающей среде. Повторители обычно используются в тех случаях, когда в сети имеется слишком много узлов или длины имеющегося кабеля недостаточно для достижения удаленных точек. Правило четырех повторителей для шинной топологии Ethernet 10 Мбит/с, также известное как правило 5-4-3, используется в качестве стандарта при расширении сегментов локальных сетей LAN. Это правило утверждает, что не более пяти сегментов сети могут быть соединены друг с другом с помощью четырех повторителей, но только три сегмента могут при этом иметь подключенные к ним рабочие станции (компьютеры). Хотя правило 5-4-3 справедливо для сетей с шинной топологией, для более сложных сетей с коммутаторами и звездообразной топологией оно не всегда применимо.

Концентраторы

Концентраторы по существу являются многопортовыми повторителями. Во многих случаях разница между этими двумя устройствами состоит только в количестве предоставляемых ими портов. В то время как типичный повторитель имеет только 2 порта, концентратор обычно имеет от 4 до 24 портов, как показано на рис. 5.14. Кроме того, концентраторы чаще всего используются в сетях 10BASE-T и 100BASE-T, хотя могут использоваться и в других типах сетей. Использование концентратора преобразует сетевую топологию из шинной, в которой каждое устройство непосредственно подсоединено к общей шине, в звездообразную. При использовании

концентраторов данные, поступающие на один из портов концентратора, повторяются посредством микросхем на всех остальных портах, подсоединенных к этому же сетевому сегменту, за исключением порта, с которого эти данные были отправлены.

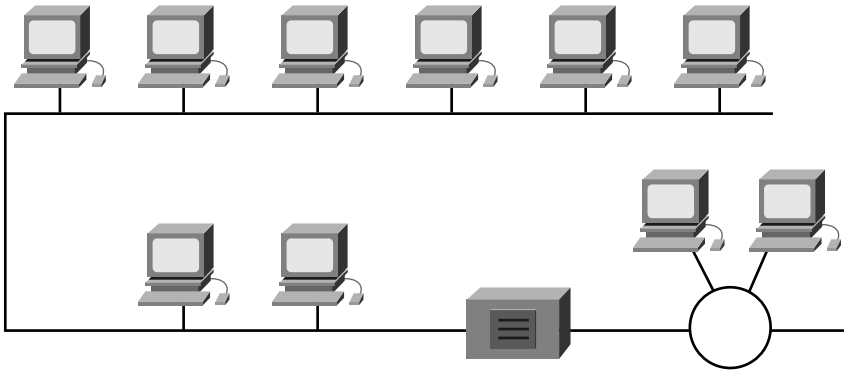


Рис. 5.12. Повторители

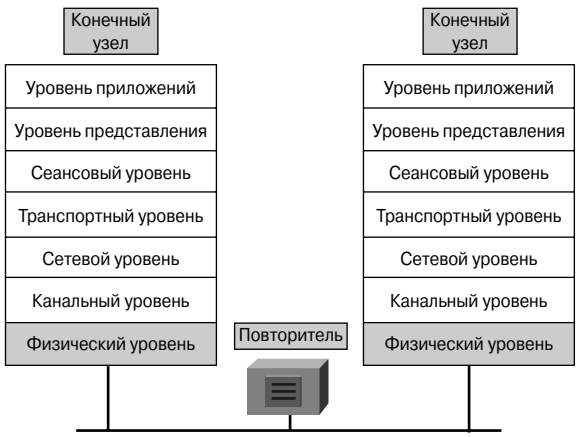


Рис. 5.13. Повторитель соединяет между собой два конечных узла

Рис. 5.14. Восьмипортовый концентратор

Концентраторы принадлежат к одному из трех указанных типов:

- **активный концентратор** должен быть подключен к источнику внешнего питания, поскольку ему нужна энергия для усиления входящего сигнала перед передачей его на внешние порты;
- **интеллектуальный концентратор** иногда называют "умным" (*smart hubs)*. В целом такие устройства функционируют как обычные концентраторы, однако имеют встроенный микропроцессор и обладают возможностями диагностики. Они дороже обычных концентраторов, однако полезны в аварийных ситуациях;
- **пассивный концентратор** выступает исключительно в качестве точки физического соединения устройств. Такой концентратор не проверяет проходящий через него трафик и не выполняет никаких действий с потоками данных; он не усиливает и не очищает сигнал. Пассивный концентратор только предоставляет доступ к общей шине и поэтому не требует наличия источника питания.

Все устройства, подсоединенные к концентратору, получают все направленные ему данные. Вследствие этого они образуют единый домен коллизий. Под коллизией понимается ситуация, в которой два устройства пытаются одновременно передавать данные.

Иногда для концентраторов используется английское название *"хаб" (hub)*.

Практическое задание 5.1.7. Выбор и приобретение концентратора и сетевой карты
В этой лабораторной работе представлен обширный прайс-лист для имеющихся на рынке сетевых компонентов. В работе предлагается ознакомиться в первую очередь с моделями концентраторов Ethernet и сетевых адаптеров.

Беспроводные коммуникации

Беспроводная среда представляет собой альтернативный способ подключения к сети LAN. При ее использовании не требуется прокладывать кабель, и поэтому компьютер легко перемещать. При беспроводном подключении можно без использования постоянного кабельного соединения передавать сигналы от одного компьютера другому с помощью радиосвязи (radio frequency — RF), лазера, инфракрасных лучей (infrared — IR), а также спутниковых сигналов или частот диапазона СВЧ. В качестве сигналов выступают электромагнитные волны, перемещающиеся в атмосфере. Беспроводным сигналам не требуется физическая среда, что делает их гибким и многовариантным способом построения сети.

Типичным приложением беспроводной связи является использование данной технологии в мобильных приложениях. Примерами такого мобильного использования технологии выступают телеработники, самолеты, спутники, космические корабли и станции.

В основе беспроводной коммуникации лежат устройства, называемые передатчиками и приемниками. Источник сигнала взаимодействует с передатчиком, который

преобразует данные в электромагнитные волны (electromagnetic — EM), которые затем детектируются приемником. Приемник преобразует волны в цифровые данные для получателя. Для двусторонней связи каждому устройству требуются как передатчик, так и приемник. Многие производители сетевого оборудования включают передатчик и приемник в один блок, называемый трансивером (приемопередатчиком), или беспроводным сетевым адаптером. Все устройства беспроводной сети LAN должны иметь соответствующий беспроводной сетевой адаптер.

Двумя наиболее часто используемыми беспроводными технологиями являются использование инфракрасных лучей (infrared — IR) и радиосвязь (radio frequency — RF). IR-технология имеет свои слабые стороны. Для нее требуется, чтобы рабочие станции и цифровые устройства находились в пределах прямой видимости передатчика. Сеть на основе технологии IR целесообразно использовать в тех случаях, когда все цифровые устройства, которым требуется соединение с сетью, находятся в одном помещении. IR-сеть может быть создана очень быстро, однако сигналы данных могут ослабляться или прерываться из-за проходящих по помещению людей или из-за повышенной влажности воздуха. Однако в настоящее время разрабатываются IR-технологии, позволяющие работать и за пределами прямой видимости.

RF-технология позволяет осуществлять связь между устройствами, находящимися в разных помещениях или даже разных зданиях. Однако использование такого типа сетей ограничено диапазоном возможных частот радиосигналов. Технология RF может использовать одну или несколько частот. Одна частота может быть подвержена внешней интерференции или маскироваться географическими препятствиями. Кроме того, одна частота легко может быть прослушана, что делает передачу данных небезопасной. Расширение спектра позволяет решить проблему безопасности при передаче данных, поскольку передача с использованием нескольких частот увеличивает защищенность в отношении шумов и усложняет перехват данных посторонними лицами.

Мосты

Иногда требуется разделить большую локальную сеть LAN на меньшие, легче управляемые сегменты. Такая стратегия позволяет ограничить поток данных через отдельную часть LAN и расширить поддерживаемую сетью географическую область, как показано на рис. 5.15. В качестве устройств, которые могут быть использованы для соединения между собой сетевых сегментов, могут быть использованы мосты, коммутаторы, маршрутизаторы и шлюзы. Коммутаторы и мосты функционируют на канальном уровне модели OSI. Функция моста состоит в определении (принятии осмысленного решения) того, требуется ли отправлять поступившие на него сигналы в другой сегмент сети. Мосты могут также быть использованы для соединения сетей, использующих различные протоколы или различные передающие среды, как, например, в случае беспроводных мостов, соединяющих сети LAN Ethernet в сеть городского масштаба.

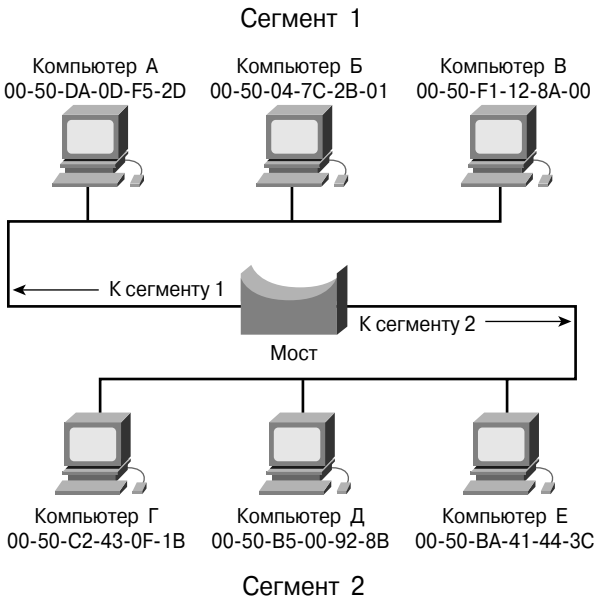
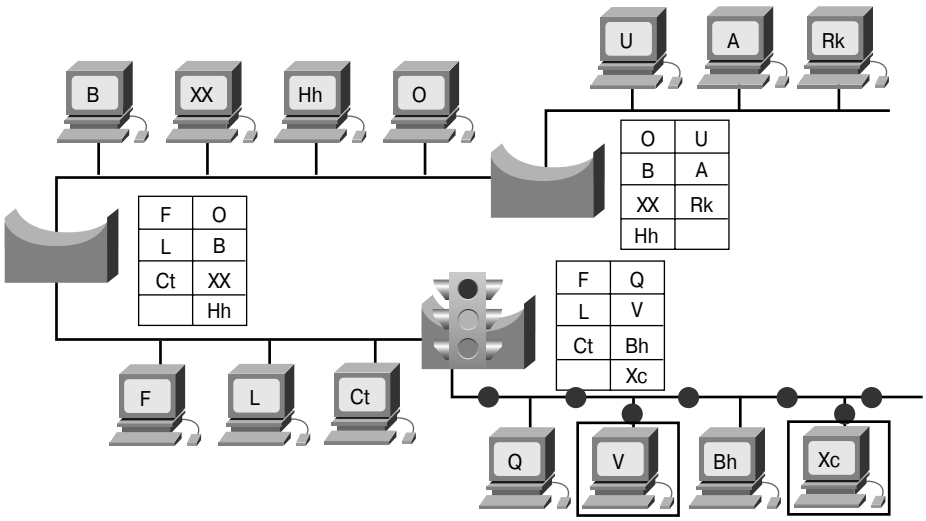


Рис. 5.15. Мосты делят сеть на сегменты

Когда мост получает фрейм, он сравнивает MAC-адрес отправителя с имеющейся у него адресной таблицей для определения того, следует ли отфильтровать этот фрейм (отбросить), разослать его лавинным способом или скопировать фрейм в другой сегмент. Принятие такого решения происходит следующим образом:

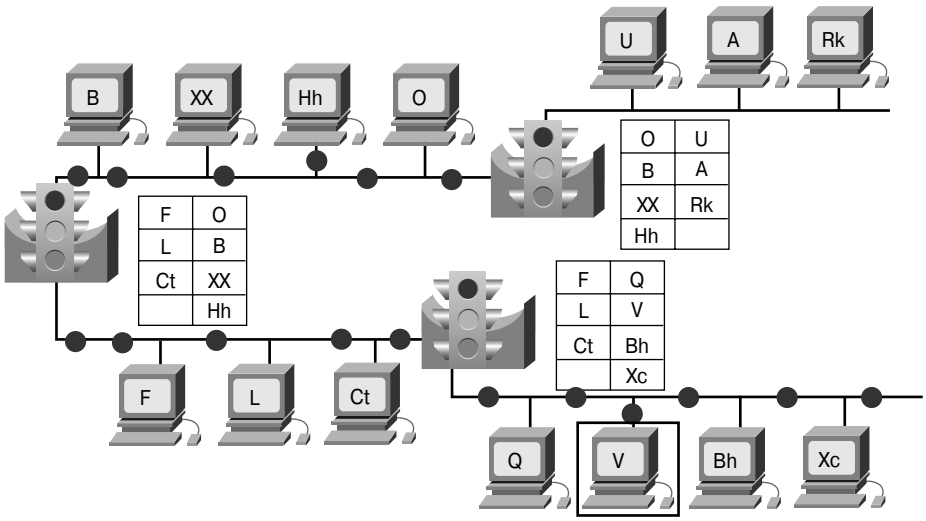
- если устройство-получатель находится в том же сегменте, из которого этот фрейм был получен, то мост предотвращает его передачу в другие сегменты, как показано на рис. 5.16. Этот процесс называется *фильтрацией (filtering)*;
- если устройство-получатель находится в другом сегменте и его адрес присутствует в адресной таблице, то мост пересылает фрейм в соответствующий сегмент, как показано на рис. 5.17;
- если устройство-получатель отсутствует в таблице адресов (т.е. "неизвестно" мосту), то мост рассылает фрейм во все сегменты за исключением того, откуда был получен фрейм. Такое поведение называют *лавинной рассылкой* сообщений.

Стратегически правильно установленный мост может значительно увеличить производительность сети.



В данном примере пакет данных отправляется с компьютера V, а пунктом назначения является компьютер Xc. Пакет поступает в пункт назначения и не рассылается широковещательно в другие сегменты сети.

Рис. 5.16. Мосты сегментируют сеть: фильтрация



В данном примере пакет данных отправляется с компьютера V, а пунктом назначения является компьютер Hh. Мост просматривает свою адресную таблицу и определяет, следует ли отправлять сигнал в другие сегменты сети.

Рис. 5.17. Мосты сегментируют сеть: пересылка

Коммутаторы

Коммутатор иногда называют многопортовым мостом. В то время как типичный мост имеет только два порта (соединяет два сетевых сегмента), коммутатор может иметь несколько портов, в зависимости от количества сетевых сегментов, которые необходимо соединить. Как и мосты, коммутаторы извлекают определенную информацию из пакетов данных, которые они получают от различных компьютеров сети. В дальнейшем эта информация используется для построения таблиц коммутации данных, которые затем используются для определения направления потоков данных, отправляемых одним из компьютеров сети другому, как показано на рис. 5.18.

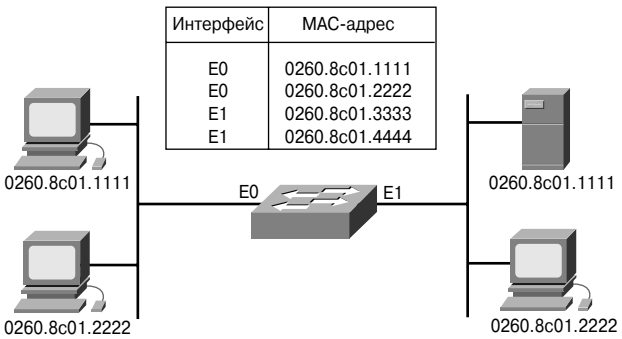


Рис. 5.18. Таблица коммутации

Хотя в работе мостов и коммутаторов есть много общего, коммутатор представляет собой более сложное устройство, чем мост. Мост определяет, направляется ли фрейм в другой сетевой сегмент, на основе MAC-адреса получателя. Коммутатор имеет несколько портов, к которым подсоединены сегменты сети. Коммутатор выбирает порт, к которому подсоединено устройство-получатель или рабочая станция. Коммутаторы Ethernet становятся все более популярными, поскольку, как и мосты, значительно повышают производительность сети (скорость передачи и полосу пропускания).

Коммутация представляет собой технологию, снижающую вероятность возникновения в сетях Ethernet LAN заторов за счет уменьшения объемов передаваемых по сети данных и увеличения полосы пропускания. Коммутаторы часто используются для замены концентраторов, поскольку не требуют изменения существующей кабельной инфраструктуры, что позволяет повысить производительность сети с минимальным количеством изменений в уже существующей сети. В настоящее время в сфере передачи данных все коммутирующее оборудование выполняет две основные операции:

- **коммутацию фреймов данных.** Под этим термином понимается процесс передачи фрейма, полученного из одной сетевой среды, в другую (выходную) среду;

- **поддержку коммутации.** Для выполнения этой функции коммутаторы строят и поддерживают таблицы коммутации и следят за возможным образованием маршрутных петель.

Коммутаторы работают с бо́льшими скоростями, чем мосты, а также могут поддерживать дополнительные и достаточно важные функции, такие, как виртуальные локальные сети VLAN (Virtual LAN).

Коммутатор Ethernet имеет много преимуществ, в частности, позволяет многим пользователям осуществлять связь параллельно за счет использования виртуальных каналов и создавать выделенные сетевые сегменты, свободные от коллизий, как показано на рис. 5.19. Такой подход позволяет максимизировать доступную полосу пропускания в общей среде. Другим преимуществом является возможность повторно использовать уже существующее аппаратное обеспечение и кабельную инфраструктуру, что делает переход к использованию коммутаторов финансово эффективным.

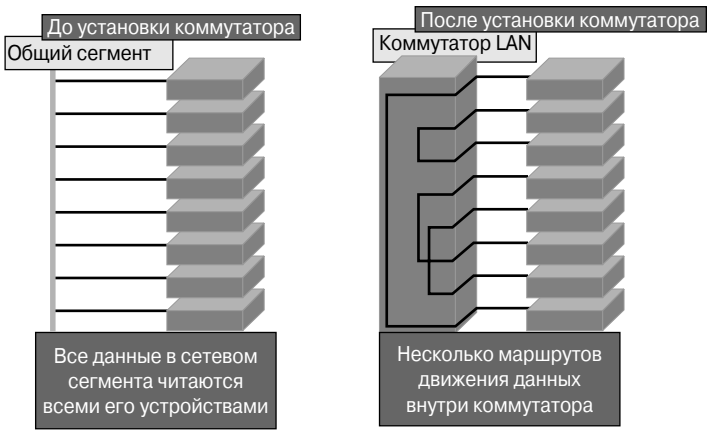


Рис. 5.19. Микросегментация сети с помощью коммутаторов

Практическое задание 5.1.10. Покупка коммутаторов сетей LAN
В этой лабораторной работе следует ознакомиться с имеющимися в продаже сетевыми компонентами и их ценами. В первую очередь следует ознакомиться с разделом о коммутаторах среды Ethernet и сетевых адаптеров NIC.

Подсоединение станций к сети

Карта сетевого интерфейса (NIC), внешний вид которой показан на рис. 5.20 и 5.21, представляет собой печатную плату, которая вставляется в гнездо на материнской плате компьютера или периферийного устройства. Она также называется сетевым адаптером. В переносных компьютерах адаптер NIC обычно имеет размеры кредитной карты. Его функция состоит в подсоединении рабочей станции к сетевой среде.

Адаптеры NIC функционируют на первом и втором уровнях эталонной модели OSI. Они рассматриваются как устройства второго уровня, поскольку каждый из них имеет уникальный код, называемый *адресом управления доступом к среде* (*Media Access Control — MAC*). Этот адрес используется для управления обменом данных между устройством и сетью. MAC-адрес каждого индивидуального адаптера NIC используется устройствами второго уровня, такими, как мосты и коммутаторы. Более подробно MAC-адреса описываются дальше в настоящей главе. Как показывает само название, адаптер NIC управляет доступом устройства к передающей среде. По этой причине адаптер NIC также работает на первом уровне, поскольку он просматривает только биты и не анализирует адресную информацию или информацию протоколов более высоких уровней. Как правило, адаптеры NIC имеют встроенные трансиверы для беспроводной связи.

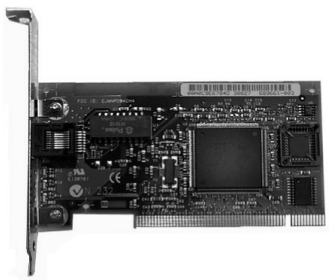


Рис. 5.20. Карта сетевого интерфейса (печатная плата)

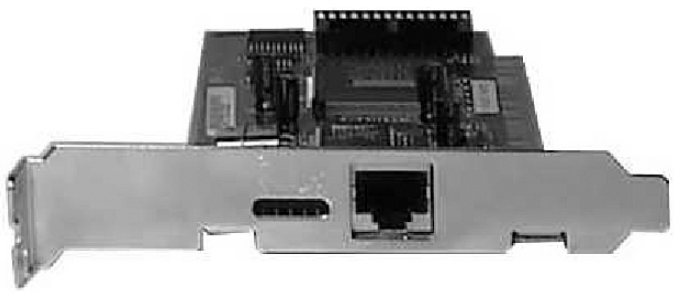


Рис. 5.21. Карта сетевого интерфейса (подключение к среде)

В некоторых случаях тип разъема на адаптере NIC не соответствует типу передающей среды, к которой он должен быть подключен. Примером такой ситуации может служить маршрутизатор Cisco серии 2500. На маршрутизаторе Ethernet-интерфейс представляет собой гнездо AUI, а к нему требуется подсоединить Ethernet-кабель UTP категории 5. Для этого используется трансивер (приемопередатчик). Трансивер среды Ethernet выполняет функцию передачи-приема (поскольку ни одна из них не обеспечивается Ethernet-интерфейсом) и в то же время преобразует один тип разъема или штекера в другой (например, подсоединяет 15-контактный интерфейс AUI к кабелю RJ-45).

На сетевых диаграммах для адаптера NIC не используется стандартный символ. При изображении устройства, подключенного к сети, подразумевается, что в нем имеется адаптер NIC или аналогичное устройство. Если на изображении сети имеется точка, то она обозначает адаптер NIC или интерфейс (порт), выполняющий функции NIC.

Взаимодействие между одноранговыми системами

В локальных сетях LAN и распределенных сетях WAN объединено большое количество соединенных друг с другом компьютеров, которые предоставляют службы своим пользователям. Для обеспечения связи сетевые компьютеры принимают на себя различные роли или функции по отношению друг к другу. Некоторые типы приложений требуют, чтобы компьютеры выступали в качестве равноправных партнеров. Другие приложения распределяют свою работу таким образом, чтобы один компьютер обслуживал несколько других, т.е. они становятся неравноправными. В обоих случаях два компьютера взаимодействуют друг с другом, используя протоколы запросов и ответов. Один компьютер посылает запрос на службу, другой компьютер его получает и отвечает на него. Компьютер, посылающий запрос, становится клиентом, а отвечающий принимает на себя роль сервера.

В *одноранговых сетях* (*peer-to-peer network*) сетевые компьютеры выступают равноправными партнерами по отношению друг к другу. Такие сети часто называются *рабочими группами (workgroups)*. Являясь равноправными партнерами, оба компьютера могут принять на себя как функции клиента, так и функции сервера. Например, в одном случае компьютер А может запросить файл у компьютера Б, который отвечает, предоставляя компьютеру А этот файл. При этом компьютер А выступает в качестве клиента, а компьютер Б — в качестве сервера. В другой ситуации компьютеры А и Б могут поменяться ролями. Например, компьютер Б делает запрос на печать компьютеру А, к которому подсоединен совместно используемый принтер, и последний, распечатывая файл, отвечает компьютеру Б, выступая в качестве сервера. Компьютеры А и Б при этом выступают в качестве равноправных или действуют как одноранговая система. В одноранговых сетях отдельные пользователи сами управляют своими ресурсами. Они могут принять решение о совместном с другими пользователями использовании определенных файлов, как показано на рис. 5.22 и рис. 5.23. Пользователи могут также потребовать введения пароля перед тем, как разрешить другим компьютерам доступ к своим ресурсам. Поскольку такие решения могут приниматься отдельными пользователями, в рассматриваемых одноранговых сетях отсутствует центральная точка управления или централизованное администрирование. Кроме того, отдельные пользователи должны самостоятельно делать резервные копии в своих системах, для того чтобы при сбое иметь возможность восстановить свои данные. В случае, когда какой-либо компьютер выступает в качестве сервера, пользователь этой станции может заметить замедление работы своей системы в моменты, когда она обрабатывает запросы других систем.

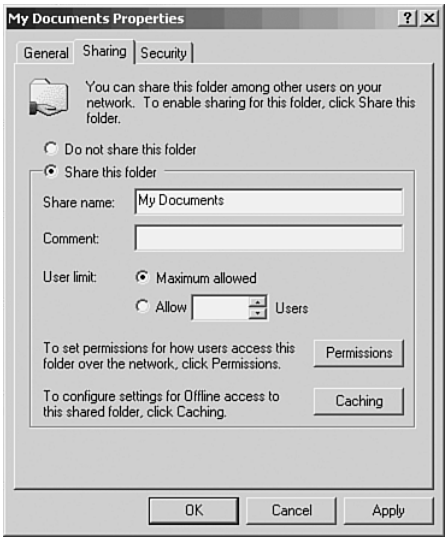


Рис. 5.22. Совместное использование файлов

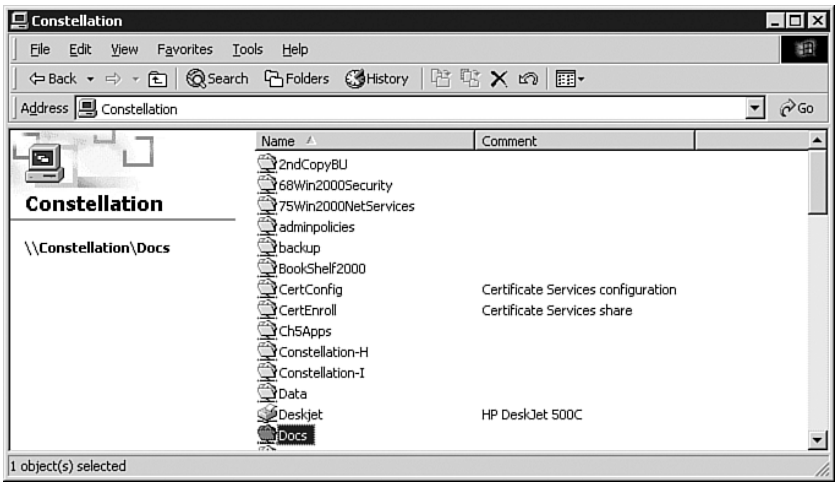


Рис. 5.23. Совместно используемые файлы

Одноранговые сети относительно легко устанавливаются и отлаживаются. При этом не требуется никакое дополнительное оборудование, кроме соответствующей операционной системы, устанавливаемой на каждом компьютере. Большинство современных операционных систем для настольных компьютеров обеспечивает поддержку одноранговых сетей. Поскольку пользователи самостоятельно управляют своими ресурсами, специальный сетевой администратор не требуется. Одноранговые сети функционируют достаточно эффективно при небольшом количестве компьютеров — как правило, не более десяти. По мере роста сети становится все труднее

координировать одноранговые связи и управлять ими. Ввиду недостаточной масштабируемости одноранговых сетей их эффективность резко падает при увеличении числа компьютеров в сети. Кроме того, тот факт, что управление доступом осуществляется индивидуально каждым пользователем, приводит к тому, что управление безопасностью сети становится затруднительным. Для преодоления ограничений, налагаемых одноранговыми сетями, может быть использована модель "клиент/сервер".

Практическое задание 5.1.12. Создание одноранговой сети
В этой лабораторной работе требуется создать простую одноранговую сеть, состоящую из двух персональных компьютеров. Необходимо правильно выбрать и установить соответствующий кабель, сконфигурировать IP-адреса и проверить работу соединения с помощью команды **`ping`**. Необходимо также создать на одном из компьютеров папку и получить к ней доступ с другого компьютера.

Сети "клиент-сервер"

В сети со структурой "клиент-сервер" сетевые службы сосредоточены на одном специально предназначенном (выделенном) компьютере, называемом сервером, который отвечает на запросы клиентов, как показано на рис. 5.24. Этот сервер является центральным компьютером, который постоянно доступен для того, чтобы отвечать на запросы клиентов относительно файловых служб, печати, предоставления приложений и других служб. Большинство сетевых операционных систем (Network Operating System — NOS) поддерживают работу сети по модели клиент-сервер. Обычно настольные компьютеры функционируют как клиенты, а один или более компьютеров, обладающие большей мощностью процессоров, большим объемом памяти и специализированным программным обеспечением, выступают в качестве серверов.

Серверы предназначены для одновременного обслуживания нескольких клиентов, как показано на рис. 5.25. До того, как клиент получит доступ к ресурсам сервера, он должен пройти идентификацию и получить авторизацию на право использования ресурсов. Такая авторизация осуществляется путем назначения каждому пользователю учетной записи (account name) и пароля, который проверяется службой аутентификации, выступающей в качестве охранной службы для предотвращения несанкционированного доступа к сети. Централизация учетных записей, обеспечения безопасности и управления доступом в сети модели "клиент-сервер" значительно упрощает работу сетевого администратора.

Концентрация на серверах сетевых ресурсов, таких, как файлы, принтеры и приложения, также облегчает резервное копирование и поддержку генерируемых ими данных. Вместо распределения этих данных на индивидуальных рабочих станциях они могут быть расположены на специализированных выделенных серверах, что облегчает получение доступа к ним. Большинство систем "клиент-сервер" также обладает дополнительными возможностями повышения производительности сети за счет добавления новых служб, повышающих эффективность сети.

Рис. 5.24. Модель сети клиент-сервер

Распределение функций в сетях "клиент-сервер" предоставляет значительные преимущества, однако вызывает некоторые дополнительные затраты. Хотя объединение ресурсов в серверных системах повышает безопасность, упрощает доступ и обеспечивает координированное управление, это также приводит к тому, что сервер становится главной возможной точкой сбоя в сети. Без сервера в рабочем состоянии сеть вообще не может функционировать. Для администрирования и поддержки серверов требуются высококвалифицированные и опытные специалисты. Такое требование увеличивает расходы на поддержку работы сети. Серверным системам также требуются дополнительное аппаратное и программное обеспечение, которое также увеличивает расходы на создание такой сети.

В табл. 5.3 и 5.4 обобщены достоинства и недостатки одноранговых сетей и сетей со структурой "клиент-сервер".

Таблица 5.3. Преимущества одноранговых сетей и сетей "клиент-сервер"

Преимущества одноранговой сети	Преимущества сети "клиент-сервер"
Требует меньших финансовых затрат	Имеет более высокий уровень безопасности и масштабируемости
Не требует серверного программного обеспечения операционной системы NOS	Облегчает администрирование крупных сетей за счет централизации
Не требуется специальный сетевой администратор	Резервное копирование всех данных выполняется в одном месте

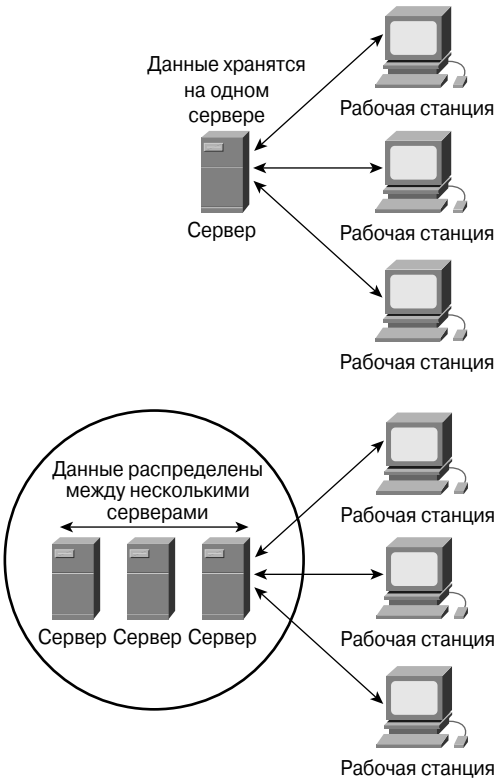


Рис. 5.25. Ресурсы сервера

Таблица 5.4. Недостатки одноранговых сетей и сетей "клиент-сервер"

Недостатки одноранговой сети	Недостатки сети "клиент-сервер"
С трудом поддается расширению и с увеличением количества станций становится малоуправляемой	Требует сетевого программного обеспечения NOS, такого, как Windows NT/2000/XP, Novell NetWare или UNIX
Каждого пользователя требуется обучить решению административных задач	Для станций-серверов требуется дорогостоящее аппаратное обеспечение
Низкий уровень безопасности	Требуется профессиональный администратор
Совместное использование ресурсов всеми станциями негативно влияет на производительность сети	Имеется одна основная, критически важная точка сбоя, и если в сети есть только один сервер, то при его выходе из строя данные всех пользователей становятся недоступны

Практическое задание 5.1.13a. Создание сети на основе концентратора
В этой лабораторной работе требуется создать простую сеть, в которой два персональных компьютера соединены друг с другом с помощью концентратора. Для этого необходимо правильно выбрать и подсоединить соответствующие кабели, сконфигурировать IP-адреса рабочих станций и протестировать соединения с помощью команды **`ping`**.

Практическое задание 5.1.13b. Создание сети на основе коммутатора
В этой лабораторной работе требуется создать простую сеть, в которой два PC соединены друг с другом с помощью Ethernet-коммутатора. Для этого необходимо правильно выбрать и подсоединить соответствующие кабели, сконфигурировать IP-адреса рабочих станций и протестировать соединения с помощью команды **`ping`**.

Кабельные соединения распределенных сетей

Для подсоединения локальной сети к другим удаленным сетям иногда необходимо использовать службы распределенных сетей WAN (Wide-Area Network — WAN). Службы WAN предоставляют различные методы соединения между собой локальных сетей, однако их кабельные стандарты отличаются от стандартов локальных сетей (LAN), поэтому пользователь должен различать разные кабельные соединения для того, чтобы правильно выбрать тип, который требуется ему для подключения к определенным службам. В этом разделе рассматриваются типы кабелей и кабельных соединений, используемых для соединений между собой коммутаторов и маршрутизаторов в сетях LAN или WAN. В этом разделе также обсуждаются кабельные соединения для последовательных портов, для соединений посредством интерфейса базовой скорости (Basic Rate Interface — BRI) цифровой сети с комплексным обслуживанием (Integrated Services Digital Network — ISDN), соединений абонентских цифровых каналов (Digital Subscriber Line — DSL), а также для установки консольных соединений.

Физический уровень распределенной сети

Многие физические реализации предусматривают передачу данных по сети WAN. Потребности в службах WAN-сетей зависят от расстояния между оборудованием и службами, от скорости передачи и характера самой службы. На рис. 5.26 приведен список канальных и физических реализаций, которые поддерживаются наиболее известными в настоящее время WAN-сетями. Тип физического уровня, выбираемый пользователем, зависит от расстояний, скорости передачи и типа интерфейса, к которому необходимо осуществить подсоединение.

Последовательные соединения служат для поддержки служб WAN-сетей, таких, в частности, как выделенные линии, на которых используются протокол двухточечных соединений (Point-to-Point Protocol — PPP) и технология Frame Relay. Скорость передачи по таким соединениям изменяется в интервале от 2400 бит/с до уровня линии T1 (1,544 Мбит/с). Другие WAN-службы, такие, как каналы ISDN, позволяют устанавливать соединения по требованию (dial-on-demand) или обеспечивают

службу резервного удаленного доступа (dialbackup). Интерфейс BRI сети ISDN состоит из двух каналов-носителей по 64 Кбит/с (B-каналы), которые используются для передачи данных и одного дельта-канала (D-канал) со скоростью 16 Кбит/с, который служит для сигнализации и управления соединением. Для передачи данных по B-каналу обычно используется протокол PPP. Все более возрастающий спрос на широкополосные (высокоскоростные) службы в домашних условиях повысил популярность каналов DSL и кабельных модемов. Скорость службы DSL может достигать уровня T1/E1 по существующей телефонной линии. Кабельные службы, функционирующие по существующему коаксиальному телевизионному кабелю, также предлагают высокоскоростные соединения со скоростями на уровне DSL, а иногда и превосходящими их.

Интерактивная презентация: стандарты физического уровня распределенной сети
В этой презентации необходимо идентифицировать компоненты физического уровня сети WAN.

Высокоуровневый протокол управления каналом корпорации Cisco (High-level Data Link Control — HDLC)	Протокол PPP	Протокол Frame Relay	Соединение BRI сети ISDN (с протоколом PPP)	DSL-модем	Кабельный модем
EIA/TIA-232 EIA/TIA-449 X.21 V.24 V.35			RJ-45 *Примечание*: расположение контактов порта BRI сети ISDN отличается от их расположения в сети Ethernet	RJ-11 *Примечание*: работает по телефонной линии	F-интерфейс *Примечание*: работает по линии кабельного TV

Рис. 5.26. Стандарты WAN-сетей на физическом уровне

Последовательные соединения распределенных сетей WAN

Последовательной передачей называется метод передачи данных, при котором биты данных передаются последовательно по одному каналу. Такой способ передачи противопоставляется параллельной передаче, при которой одновременно передаются несколько битов. При дальней связи сети WAN используют последовательную передачу. Для передачи энергии, представленной битами данных, последовательные каналы используют специальный электромагнитный или оптический диапазон. Частоты (частота — это количество циклов в секунду, Герц) выступают в качестве

диапазона или спектра коммуникации. Например, сигналы, передаваемые по голосовой телефонной линии, используют до 3 кГц (килогерц, или тысяч герц). Ширина частотного диапазона называется *полосой пропускания (bandwidth*).

Другим способом описать полосу пропускания является указание объема данных в битах в секунду, которые может передавать последовательный канал. В табл. 5.5 сравниваются физические стандарты последовательных соединений EIA/TIA-232, EIA/TIA-449, v.35, X.21 и EIA-530 WAN.

Таблица 5.5. Сравнение физических стандартов

Скорость передачи данных (бит/с)	Расстояние (м) EIA/TIA-232	Расстояние (м) EIA/TIA-449, V.35, X.21, EIA-530
2400	60	1250
4800	30	625
9600	15	312
19,200	15	156
38,400	15	78
115,200	3,7	—
T1 (1,544 Мбит/с)	—	15

Для подключения к последовательным службам WAN может быть использовано несколько типов физических соединений. Выбор типа последовательного кабеля для маршрутизатора зависит от физической реализации, выбранной пользователем, или от физической реализации, используемой провайдером. На рис. 5.27 показаны несколько типов разъемов последовательных каналов. Последовательные порты и разъемы используются для подсоединения устройств конечного пользователя к устройствам провайдера службы. Следует отметить, что последовательные порты маршрутизаторов Cisco используют фирменное 60-контактное гнездо (т.н. “smart serial” — интеллектуальный последовательный разъем) меньшего размера, которое позволяет реализовать два последовательных соединения на одной карте WAN-интерфейса. Тип разъема на другом конце кабеля определяется провайдером службы или требованиями конечного устройства, однако типичным является разъем стандарта V.35.

Если соединение установлено непосредственно с провайдером службы или с устройством, которое обеспечивает синхронизацию (clocking), например, с модулем CSU/DSU (Channel Service Unit/Data Service Unit — модуль обслуживания канала и данных), маршрутизатор будет выступать в качестве конечного (терминального) оборудования (Data Terminal Equipment — DTE), и для подключения к каналу или службе понадобится DTE-кабель. Обычно именно такая схема подключения используется в сетях. Тем не менее, иногда возникает необходимость получать синхроимпульсы от местного маршрутизатора; в таком случае необходимо использовать DCE-кабель, и устройство будет выступать в качестве аппаратуры передачи данных (Data Communications Equipment — DCE) или телекоммуникационного оборудования, т.е. оборудования обслуживания канала. В лабораторных работах (и в тестовых условиях),

когда один маршрутизатор подключен непосредственно к другому, одно устройство будет DTE-модулем, а другое — DCE, и для подключения их друг к другу понадобится кабель DTE-DCE.

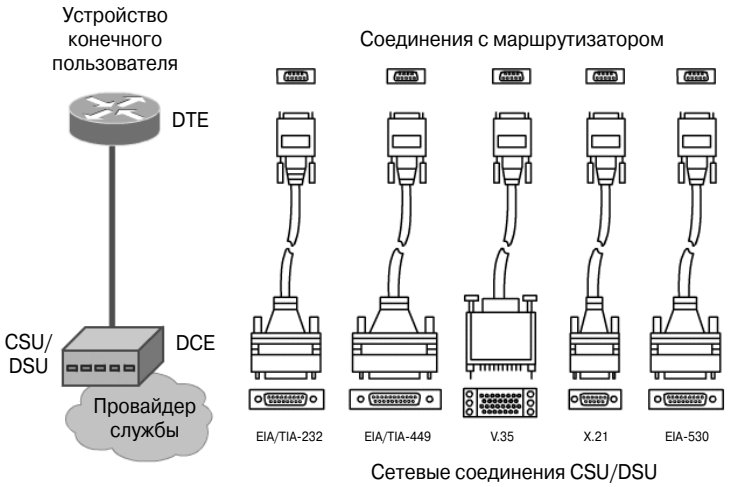


Рис. 5.27. Различные варианты последовательных соединений WAN

Маршрутизаторы и последовательные соединения

Кроме выбора типа кабеля, необходимо определить, какого типа разъемы требуются для сети пользователя: разъемы терминального оборудования (Data Terminal Equipment — DTE) или телекоммуникационного (Data Communications Equipment — DCE). Модуль DTE представляет собой устройство пользователя в конечной точке канала WAN. Под DCE-модулем подразумевается устройство, на котором пользовательские данные DTE-устройства преобразовываются в приемлемую форму для устройств, обеспечивающих службы WAN. Как показано на рис. 5.28, если осуществляется непосредственное подсоединение к провайдеру службы или к устройству, осуществляющему синхронизацию сигнала (такому, например, как модуль CSU/DSU), то маршрутизатор является устройством DTE, и необходимо использовать последовательный кабель DTE. Такая ситуация типична при использовании маршрутизаторов.

ВНИМАНИЕ!

Синхронизацией называется согласование во времени передачи данных между устройствами. В последовательном соединении WAN-сети синхронизацию передачи данных осуществляет модуль CSU/DSU.

Однако в некоторых случаях функции DCE выполняет маршрутизатор, как показано на рис. 5.29. Например, при непосредственном лабораторном соединении маршрутизаторов (back-to-back), т.е. когда на обоих концах соединения находятся

маршрутизаторы, один из них выполняет функции DTE-устройства, а другой — DCE-устройства, осуществляя синхронизацию.

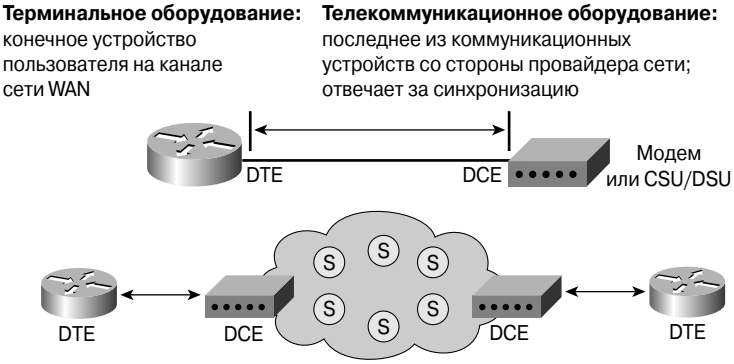


Рис. 5.28. Последовательное соединение: DTE и DCE

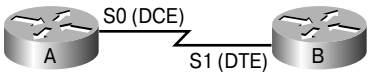


Рис. 5.29. Непосредственное лабораторное последовательное соединение маршрутизаторов

Для создания последовательного соединения в маршрутизаторах есть фиксированные, или модульные, порты. Тип используемого порта влияет на синтаксис, который будет позднее использоваться при конфигурировании каждого интерфейса. На рис. 5.30 показан маршрутизатор с фиксированными последовательными портами (интерфейсами). Каждому порту присваивается имя (метка), отражающее его тип и номер, например, **`serial 0`** (нулевой последовательный интерфейс). При конфигурировании фиксированного интерфейса необходимо указывать интерфейс, используя соглашение о типе и номере порта.

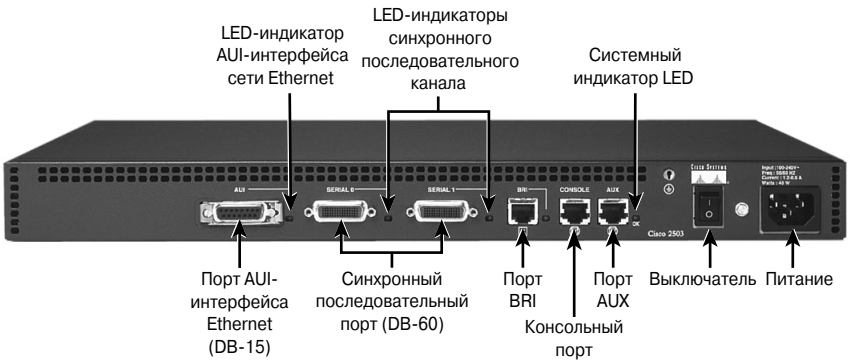


Рис. 5.30. Фиксированные интерфейсы

На рис 5.31 показан маршрутизатор с модульными последовательными портами. Обычно каждому порту присваивается имя, указывающее **тип**, **разъем** (гнездо, в которое вставляется модуль) и **номер порта**. При конфигурировании порта на модульной карте пользователю предлагается указать интерфейс, используя команду в формате "**`тип/номер разъема/номер порта`**", например, **`serial 1/0`**; в этом обозначении указан тип интерфейса (последовательный, serial), номер разъема, в котором установлен модуль последовательного интерфейса (разъем с номером 1), и конкретный порт на модуле последовательного интерфейса (порт с номером 0).

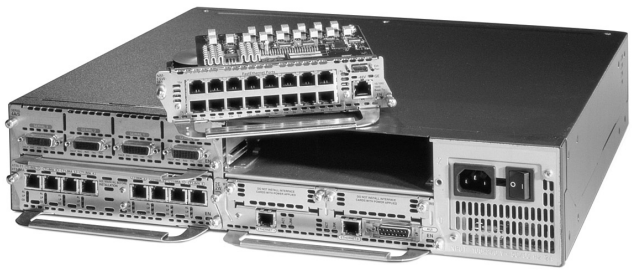


Рис. 5.31. Порты модульного последовательного интерфейса

Практическое задание 5.2.3a. Соединение LAN-интерфейсов маршрутизаторов

В этой лабораторной работе требуется идентифицировать интерфейсы Ethernet или Fast Ethernet-маршрутизатора. Затем следует выбрать кабели для маршрутизаторов и концентраторов или коммутаторов и подсоединить их.

Практическое задание 5.2.3b. Создание базовой WAN-сети с использованием маршрутизаторов

В этой лабораторной работе требуется соединить между собой две простые локальные сети, каждая из которых состоит из рабочей станции и коммутатора (или концентратора), в результате чего образуется WAN-сеть с соединением маршрутизатор-маршрутизатор.

Практическое задание 5.2.3c. Поиск и устранение неисправностей в соединениях между устройствами

В этой лабораторной работе требуется создать простую маршрутизируемую распределенную сеть, к которой подключены два ПК, два коммутатора или концентратора и два маршрутизатора. В ней также нужно сконфигурировать IP-адреса на персональных компьютерах и при необходимости найти и устранить неисправности в работе сети: неправильные соединения, нерабочие кабели или обнаружить неправильно указанные адреса.

Маршрутизаторы и соединения BRI сети ISDN

При использовании интерфейса BRI цифровой сети с комплекнсым обслуживанием (ISDN) могут быть использованы два типа интерфейсов: BRI-S/T и BRI-U. В службе BRI сети ISDN интерфейс пользователя (U) представляет собой электрический интерфейс для соединения на основе витой пары пользователя с сетевым терминирующим устройством первого типа (Network Termination 1 — NT1). Терминальный интерфейс (T) представляет собой электрический интерфейс между устройством NT1 и устройством NT2, в качестве которого обычно выступает частная телефонная станция (Private Branch Exchange — PBX, мини-АТС). Под системным (System — S) интерфейсом понимается электрический интерфейс между устройством NT1 и устройством ISDN, таким, как компьютер или ISDN-телефон. При использовании интерфейса BRI T-интерфейс электрически идентичен S-интерфейсу, поэтому эти два интерфейса обычно объединены в одном интерфейсе, который обозначается как S/T-интерфейс.

Чтобы определить, какой интерфейс требуется в конкретной ситуации, необходимо выяснить, имеется ли устройство NT1 или, возможно, оно предоставляется провайдером. Устройство NT1 является промежуточным между маршрутизатором и ISDN-коммутатором провайдера службы (сетевая среда), и используется для подсоединения четырехпроводной линии потребителя к обычному двухпроводному абонентскому каналу. В Северной Америке устройство NT1 обычно обеспечивается самим потребителем, а в остальных странах — предоставляется провайдером. Устройство NT1 является преобразователем однопарной дуплексной медной линии провайдера связи в двухпарную линию потребителя с раздельными передающими и приемными контактами. Такое устройство позволяет одновременно использовать два раздельных независимых устройства в цепи, например, ISDN-телефон и ISDN-маршрутизатор.

ВНИМАНИЕ!

Важно, чтобы кабель, идущий от порта BRI сети ISDN, был подключен к гнезду ISDN или к коммутатору ISDN. В порту BRI технологии ISDN используются напряжения, которые могут серьезно повредить устройства, несовместимые с сетью ISDN.

Дополнительная информация: кабельные соединения между маршрутизатором и ISDN-сетью

Если устройство NT1 должно быть обеспечено самим пользователем, то может быть использован BRI-порт сети ISDN с U-интерфейсом. U-интерфейс имеет встроенное устройство типа NT1. Если используется внешнее устройство NT1, или устройство NT1 используется провайдером службы, то маршрутизатору требуется S/T-интерфейс сети ISDN. Поскольку маршрутизаторы могут иметь различные типы интерфейсов ISDN, требуемый тип интерфейса должен быть учтен при приобретении маршрутизатора. Некоторые маршрутизаторы имеют как U-интерфейс, так и S/T-интерфейс. Тип разъема ISDN на маршрутизаторе может быть определен по этикетке порта. На рис. 5.32 показаны различные типы портов интерфейса ISDN.

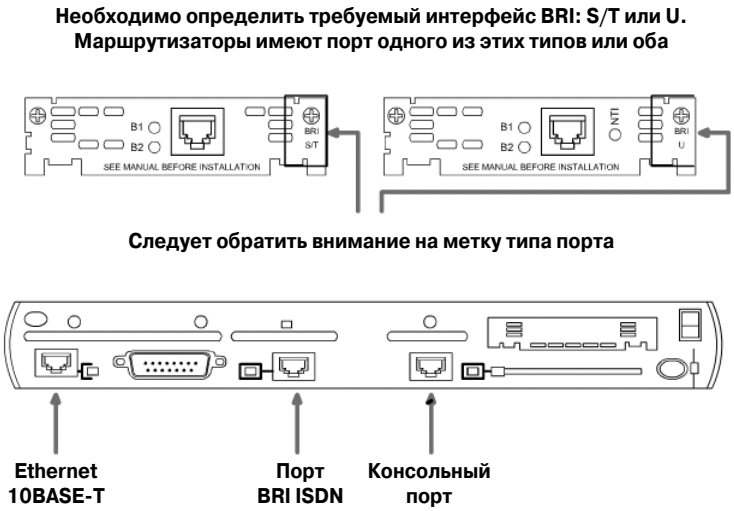


Рис. 5.32. Подсоединение кабелей к маршрутизаторам для соединений сети ISDN

Для подсоединения порта BRI сети ISDN на маршрутизаторе к устройству провайдера службы нужно использовать прямой кабель UTP категории 5 с разъемами RJ-45. Следует отметить, что расположение контактов кабелей портов BRI сети ISDN отличается от расположения контактов для среды Ethernet. В табл. 5.6 описано назначение контактов S/T-интерфейса порта BRI сети ISDN.

Таблица 5.6. Контакты S/T-интерфейса BRI сети ISDN

Контакт	Сигнал
1	Не используется
2	Не используется
3	Передача (Tx+)
4	Прием (Rx+)
5	Прием (Rx-)
6	Передача (Tx-)
7	Не используется
8	Не используется

Маршрутизаторы и соединения DSL

Соединение DSL представляет собой модемную технологию, которая позволяет осуществлять недорогую высокоскоростную цифровую передачу по уже имеющейся телефонной линии на основе витой пары. Использование технологии DSL является эффективным решением для многих коммерческих приложений, таких, как передача файлов или получение доступа ко внутренней корпоративной сети. Асимметричный цифровой абонентский канал (Asymmetric Digital Subscriber Line — ADSL) используется чаще всего и является представителем обширного семейства технологий, в общем виде обозначаемых как *xDSL*.

Маршрутизаторы с фиксированной конфигурацией серии Cisco 800 обеспечивают высокую степень безопасности, имеют небольшую стоимость, надежны и являются эффективным вложением средств благодаря развитому программному обеспечению IOS Cisco, специально разработанному для малых офисов и телеработников. Как показано на рис. 5.33, ADSL-маршрутизатор Cisco 827-4V имеет один ADSL-интерфейс, который используется для подключения к сети Internet или к корпоративной сети LAN через цифровой абонентский канал DSL.

ВНИМАНИЕ!

Если необходимо подключить телефонное оборудование, которое не поддерживает технологию DSL, к DSL-службе, то рекомендуется установить фильтр во избежание интерференции между голосовыми и службами передачи данных.

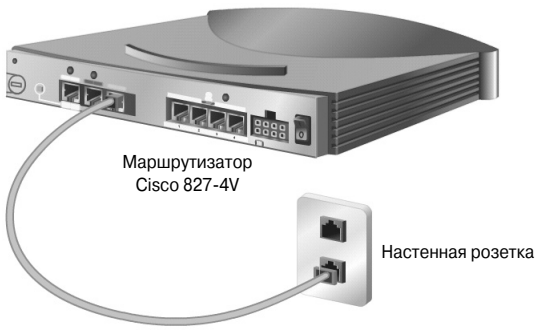


Рис. 5.33. Маршрутизатор Cisco 827-4V

Дополнительная информация: подключение маршрутизатора к DSL-линии

Для подсоединения канала ADSL к порту ADSL необходимо выполнить простые действия, описание которых приводится ниже.

Этап 1. Подсоединить телефонный кабель к порту ADSL маршрутизатора.

Этап 2 Подсоединить другой конец телефонного кабеля к внешней стенной розетке (разъему).

Для подсоединения маршрутизатора к службе DSL необходим телефонный кабель с разъемами RJ-11. Канал DSL функционирует по обычной телефонной линии. Как показано в табл. 5.7, он использует только два контакта разъема RJ-11.

Таблица 5.7. Контакты S/T-интерфейса BRI сети ISDN

Контакт	Сигнал
1	Не используется
2	Не используется
3	Передача (Tx)
4	Прием (Rx)
5	Не используется
6	Не используется

Маршрутизаторы и кабельные сети

Кабельные модемы позволяют осуществлять двухстороннюю высокоскоростную передачу данных по тому же коаксиальному кабелю, который используется для кабельного телевидения. Некоторые провайдеры кабельных служб обещают скорости, в шесть и более раз превосходящие скорости выделенных линий T1. По мере возрастания спроса на широкополосные службы соединения с помощью кабельных модемов становятся все более популярными. Маршрутизатор кабельного доступа Cisco uBR905 обеспечивает высокоскоростной доступ к сети по системе кабельного телевидения домашним пользователям, а также малым и домашним офисам (Small Office, Home Office — SOHO).

ВНИМАНИЕ!

Коаксиальный радиочастотный кабель подсоединяется к антеннам общего пользования или распределительным узлам кабельного телевидения. Большинство систем кабельного телевещания в качестве своих проводных систем также использует коаксиальный кабель. На главных магистральных линиях, идущих от провайдера кабельных служб, могут использоваться оптоволоконные кабели, однако на участках между коробкой распределения и конечным пользователем используется только коаксиальный кабель.

В маршрутизатор модели uBR905 встроен интерфейс коаксиального кабеля (F-разъем), который может быть подсоединен к кабельной системе. Для соединения между собой маршрутизатора и кабельной системы используется коаксиальный кабель и F-разъем. Коаксиальный кабель может принадлежать к типу 59 (RG-59) или RG-6, хотя рекомендуется использование кабеля марки RG-6. Для подсоединения маршрутизатора кабельного доступа Cisco uBR905 к кабельной системе необходимо выполнить действия, описанные ниже.

Этап 1. Убедиться в том, что маршрутизатор отключен от источника питания.

Этап 2. Найти радиочастотный коаксиальный кабель, идущий от настенной розетки кабельного телевидения.

Этап 3. Установить, если требуется, кабельный или направленный ответвитель для разделения телевизионных сигналов и компьютерных. При необходимости следует установить также высокочастотный фильтр для предотвращения интерференции между телевизионными и компьютерными сигналами.

Этап 4. Подсоединить коаксиальный кабель к F-разъему маршрутизатора, как показано на рис. 5.34. Вручную затянуть кольцо разъема, удостоверившись, что напряжение затягивания соответствует мускульному усилию пальцев, а затем подтянуть зажим еще на 1/6 оборота с помощью гаечного ключа.

Этап 5. Удостовериться, что все остальные разъемы коаксиального кабеля — промежуточных делителей, удвоителей и других заземленных блоков — надежно затянуты (чтобы обеспечить уверенный контакт) по маршруту от распределительного ответвления до маршрутизатора Cisco uBR905 согласно инструкциям четвертого этапа.

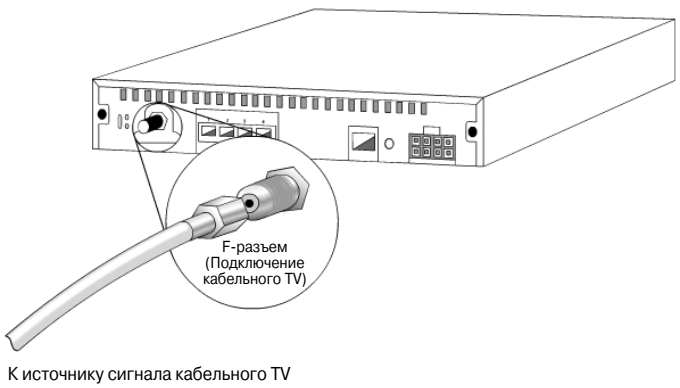


Рис. 5.34. F-разъем

ВНИМАНИЕ!

Не следует слишком старательно затягивать кольцо разъема, поскольку его можно таким образом сломать. Также не рекомендуется использовать какие-либо рычаги либо гаечные ключи с ограничением по моменту, поскольку с помощью такого ключа не всегда удается повернуть кольцо зажима именно на 1/6 окружности, после того как оно было закручено вручную.

Установка консольных соединений

Для первоначального конфигурирования устройств Cisco необходимо обеспечить непосредственное соединение с оборудованием. Для оборудования Cisco прямое управление обеспечивается посредством *консольного порта* (*console port*). Консольный порт позволяет осуществлять мониторинг и конфигурировать концентратор, коммутатор или маршрутизатор корпорации Cisco. Кабель, который используется между терминалом и консольным портом, называется *консольным, или инвертированным, кабелем (rollover cable)*; на его концах используются разъемы RJ-45, как показано на рис. 5.35.

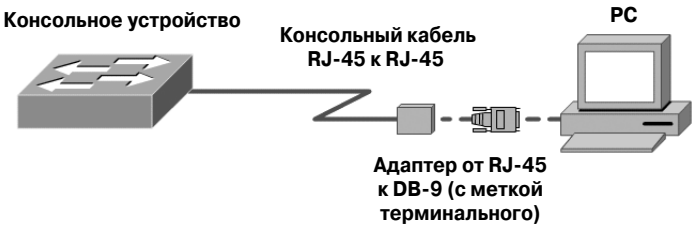


Рис. 5.35. Консольное подключение к устройству

Инвертированный кабель, также известный как консольный, имеет иную распайку контактов, чем сквозной или перекрещенный кабели с разъемами RJ-45, используемые в сети Ethernet или для подключения к BRI-порту сети ISDN. У этого типа кабеля контакты соединены следующим образом:

контакт 1 подключен к контакту 8,

контакт 2 подключен к контакту 7,

контакт 3 подключен к контакту 6,

контакт 4 подключен к контакту 5,

контакт 5 подключен к контакту 4,

контакт 6 подключен к контакту 3,

контакт 7 подключен к контакту 2,

контакт 8 подключен к контакту 1.

Для создания соединения между терминальным оборудованием и консольным портом устройства Cisco необходимо выполнить действия, описание которых приводится ниже.

Этап 1. Соединить устройства с помощью консольного кабеля. Для подключения, возможно, потребуются адаптеры от разъема RJ-45 к-DB-9 или от разъема RJ-45 к-DB-25 для персонального компьютера или терминала.

Этап 2. Сконфигурировать приложение эмуляции терминала, задав следующие общие установки для портов оборудования (порта COM):

- скорость равна 9600 бит/с;
- используются 8 битов данных (8 data bits);
- проверка четности отключена (no parity);
- используется 1 стоповый бит (1 stop bit);
- используется аппаратное управление потоком (hardware flow control).

ВНИМАНИЕ!

Вспомогательный (auxiliary — AUX) порт используется для удаленного управления устройством с помощью модема. Порт AUX перед использованием должен быть сконфигурирован с помощью консольного порта. Порт AUX также конфигурируется со стандартными для оборудования корпорации Cisco установками: 9600 бит/с, 8 битов данных, без четности, с одним стоповым битом и аппаратным управлением потоком. Для вспомогательного порта может быть установлена скорость передачи до 115200 бит/с, но при подключении с помощью модема реальная скорость не будет превышать 33600 бит/с из-за ограничений за счет импульсно-кодовой модуляции сигнала.

Презентация: консольный кабель
В этой презентации показан консольный кабель.

Практическое задание 5.2.7. Подсоединение консоли к маршрутизатору или коммутатору
В этой лабораторной работе необходимо подсоединить ПК к маршрутизатору или коммутатору, установить консольный сеанс связи и получить доступ к интерфейсу пользователя.

Резюме

В этой главе были изложены следующие ключевые темы, касающиеся сетевых технологий:

- сетевой адаптер NIC предоставляет возможность персональному компьютеру обмениваться информацией с сетью;
- тремя основными средами локальных сетей LAN являются сети технологий Ethernet, Token Ring и FDDI;
- термин *Ethernet* часто используется по отношению ко всем сетям множественного доступа CSMA/CD, соответствующим Ethernet-спецификациям;
- семейство LAN-реализаций технологии Ethernet включает в себя четыре основные категории: Ethernet и IEEE 802.3, Fast Ethernet, Gigabit Ethernet, Ethernet 10G или 10000 Мбит/с Ethernet;
- перекрещенный кабель используется для соединения между собой однотипных устройств (коммутатор с коммутатором, маршрутизатор с маршрутизатором, ПК с ПК или концентратор с концентратором);

- прямой кабель используется для соединения друг с другом разнотипных устройств (например, коммутатор с маршрутизатором, коммутатор с ПК, концентратор с маршрутизатором или концентратор с ПК);
- существуют два основных типа сетей LAN: одноранговые и сети "клиент-сервер";
- в сетях WAN используется последовательная передача данных;
- маршрутизатор обычно выполняет функции DTE-устройства, и для подсоединения к DCE-устройству, такому, как CSU/DSU, ему требуется последовательный кабель DTE;
- порт BRI цифровой сети с комплексным обслуживанием (ISDN) бывает двух видов: S/T и U. Для подсоединения порта BRI сети ISDN к устройству провайдера службы используется прямой кабель UTP категории 5;
- для подсоединения маршрутизатора к службе DSL используются телефонный кабель и разъем RJ-11;
- для подсоединения маршрутизатора к кабельной службе используются коаксиальный кабель и F-разъем;
- для подсоединения терминала к консольному порту маршрутизатора используется консольный кабель.

Обратите внимание на относящиеся к данной главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Они помогут вам закрепить основные понятия и термины, изложенные в этой главе.

Ключевые термины

RJ-45 — это разъем, которым обычно заканчивается кабель типа витой пары.

Активный концентратор (active hub) — концентратор такого типа должен быть подключен к источнику питания (в настенную розетку), поскольку ему требуется питание для усиления входящего сигнала перед передачей его на другие порты.

Интеллектуальный концентратор (intelligent hub) — иногда такой концентратор называют "умным". Устройства данного типа обычно функционируют как активные концентраторы, однако имеют дополнительные микропроцессоры и обладают функциями диагностики. Они дороже активных концентраторов и имеют полезные функции обнаружения неисправностей.

Интерфейс подключаемых (сетевых) устройств (Attachment Unit Interface — AUI) — интерфейс 15-контактного физического разъема между сетевой картой компьютера и кабелем среды Ethernet.

Коммутатор (Switch) — это устройство, иногда называемое многопортовым мостом. В то время как обычный мост, как правило, имеет только два порта (т.е. соединяет два сетевых сегмента), коммутатор может иметь несколько портов, в зависимости от того, сколько сетевых сегментов требуется соединить.

Конвертер гигабитового интерфейса (Gigabit Interface Converter — GBIC) представляет собой устройство ввода/вывода, подключаемое к порту Gigabit Ethernet и допускающее замену без выключения системы.

Одноранговая сеть (peer-to-peer network) — это сеть, в которой компьютеры выступают по отношению друг к другу как равноправные партнеры. При необходимости каждый из них может принимать на себя как функции сервера, так и функции клиента.

Перекрещенный кабель (crossover cable) — это кабель, в котором перекрещена пара, для того чтобы правильно подать, передать и получить сигналы между однотипными устройствами.

Повторитель (Repeater) — устройство, которое регенерирует и ресинхронизирует сетевые сигналы на битовом уровне, что позволяет передавать их на большее расстояние в передающей среде.

Прямой кабель (straight-through cable) — это кабель, в котором сохранен порядок следования контактов на обоих концах. Если провод подсоединен к контакту с номером 1 на одном конце кабеля, то и на другом конце он будет подсоединен к аналогичному контакту 1.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые ниже вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. Что из перечисленного является спецификацией 802.3u?

а) 10BASE-F.

б) 10BASE-T.

в) 100BASE-TX.

г) 1000BASE-CX.

2. Что из перечисленного является наиболее подходящим выбором для Ethernet-соединений?

а) Использование технологии Ethernet со скоростью 10 Мбит/с в качестве соединения между сервером и сетью LAN.

б) Использование соединения Gigabit Ethernet в качестве канала на уровне пользователя для обеспечения высокой производительности.

в) Использование соединения Fast Ethernet в качестве канала между уровнем пользователя и сетевыми устройствами для агрегирования потоков данных от каждого Ethernet-сегмента по каналу доступа.

г) Ничего из перечисленного.

3. Какой орган стандартизации создал спецификации для кабелей и разъемов, используемых в Ethernet-технологиях?

а) ISO.

б) ANSI.

в) TIA/EIA.

г) IETF.

4. Какое из приведенных утверждений неправильно описывает разъем для подсоединения к передающей среде?

а) RJ-45 представляет собой восьмиконтактный разъем, используемый главным образом в качестве терминатора коаксиального кабеля.

б) AUI представляет собой 15-контактный разъем, используемый для соединения между собой адаптера NIC и кабеля Ethernet.

в) GBIC представляет собой трансивер, преобразующий постоянные электрические токи в оптические сигналы и наоборот.

г) Ни одно из вышеприведенных утверждений.

5. В каком из перечисленных случаев потребуется перекрещенный (crossover) кабель?

а) Создание магистральных каналов между коммутаторами.

б) Соединение маршрутизаторов с коммутаторами.

в) Подсоединение концентраторов к коммутаторам.

г) Ни в одном из вышеперечисленных.

6. Какая из перечисленных технологий не является одним из видов беспроводных соединений?

а) Сотовая связь.

б) Широкополосная радиосвязь.

в) Связь в инфракрасном диапазоне.

г) Расширение спектра.

7. Что из нижеперечисленного не является реализацией распределенной сети WAN?

а) DSL.

б) ISDN.

в) Frame Relay.

г) Ethernet.

8. Какой тип передачи данных используется в распределенных сетях WAN?

а) Параллельная.

б) Последовательная.

в) Одиночная.

г) Ни один из вышеперечисленных.

9. Какое из приведенных определений наилучшим образом описывает понятие DCE?

а) Устройство пользователя в конечной точке сети.

б) Оборудование, которое служит источником данных или их получателем.

в) Физические устройства, такие, как трансляторы протоколов и мультиплексоры.

г) Устройства, которые являются конечным сетевым оборудованием интерфейса “пользователь-сеть”.

10. Какая из передающих сред используется для подсоединения порта BRI сети ISDN к устройству провайдера службы?

а) Прямой кабель UTP категории 5.

б) Перекрещенный кабель UTP категории 5.

в) Коаксиальный кабель.

г) Оптоволоконный кабель.

11. Какой тип разъема используется для соединений DSL?

а) RJ-45.

б) RJ-11.

в) F-разъем.

г) DB-9.

12. Какой тип разъема используется для подсоединения маршрутизатора к телевизионной кабельной системе?

а) RJ-45.

б) RJ-11.

в) F-разъем.

г) AUI.

13. Какой тип кабеля используется для подсоединения терминала к консольному порту?

а) Прямой.

б) Консольный.

в) Перекрещенный.

г) Коаксиальный.

ГЛАВА 6

Основы технологии Ethernet

В этой главе...

- кратко описана история технологии Ethernet и стандарты и принципы именования технологий IEEE;
- указано, на каких уровнях эталонной модели OSI работает технология Ethernet;
- описан формат фрейма 802.3;
- описано управление доступом к среде передачи (Media Access Control — MAC) и MAC-адресация;
- описан метод доступа к среде CSMA/CD;
- описана процедура установки соединения;
- рассмотрен дуплексный метод передачи данных;
- рассказано, как идентифицировать компьютеры и интерфейсы;
- рассмотрен процесс фреймирования на втором уровне эталонной модели;
- описана структура фреймов Ethernet;
- рассмотрена синхронизация в технологии Ethernet;
- описаны межфреймовые интервалы и таймеры;
- рассмотрен процесс обработки ошибок;
- рассмотрены три типа коллизий;
- указаны основные источники ошибок в среде Ethernet;
- описаны процедура контроля ошибок и контрольная сумма фрейма (FCS);
- описана процедура автоматического согласования параметров канала в технологии Ethernet.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

технология Ethernet, с. 304,

множественный доступ с контролем несущей и обнаружением коллизий, с. 305,

Институт инженеров по электротехнике и электронике, с. 306,

максимальный блок передачи, с. 319,

технология token ring, с. 322,

технология fddi, с. 322,

без установки соединения, с. 325,

симплексная передача, с. 325,

Fast Ethernet, с. 307,
Gigabit Ethernet, с. 307,
10-Gb Ethernet, с. 307,
подуровень управления доступом к среде, с. 309,
подуровень управления логическим каналом, с. 309,
IEEE 802.2, с. 309,
IEEE 802.3, с. 309,
MAC-адрес, с. 312,
уникальный идентификатор организации, с. 312,
концевик, с. 313,
полудуплексная передача, с. 325,
дуплексная передача, с. 326,
задержка распространения, с. 327,
простой протокол управления сетью, с. 331,
сбойный пакет, с. 337,
удлиненный фрейм, с. 338,
ошибка выравнивания, с. 340,
нарушение границ фрейма, с. 340,
заголовок, с. 312,
фрейм-призрак, с. 340.

Технология *Ethernet* в ее различных формах представляет собой наиболее широко используемую технологию локальных сетей (Local-Area Network — LAN). Она была предназначена для заполнения технологического разрыва между низкоскоростными сетями большой протяженности и специализированными сетями масштаба небольшого помещения, в которых данные передаются с большими скоростями на очень короткие расстояния.

Технология Ethernet хорошо подходит для приложений, в которых по среде локальной сети спорадически передаются большие объемы информации с высокими скоростями. Эта технология была предназначена для совместного использования ресурсов на уровне локальной рабочей группы. При ее разработке ставилась цель достичь простоты технологии, невысокой стоимости, совместимости, равного доступа к ресурсам, малой задержки и высокой скорости передачи.

В этой главе описана история технологии Ethernet и стандартов Ethernet, разработанных IEEE. В ней также рассмотрен принцип функционирования сети Ethernet, описаны формат фреймов Ethernet и процедура обработки ошибок, рассмотрены различные типы коллизий в сетях Ethernet. В главе даны определения понятий коллизионного и широковещательного доменов. В последней части описаны сегментация сети и устройства, используемые для создания сетевых сегментов.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в данной главе.

Основы технологии Ethernet

Локальными сетями LAN называются высокоскоростные сети передачи данных, характеризуемые низким уровнем ошибок и охватывающие относительно небольшую географическую область (до нескольких километров в диаметре). LAN-сети соединяют между собой рабочие станции, периферийные устройства, терминалы и другие устройства, находящиеся в одном здании или в некоторой ограниченной географически области.

В настоящее время Ethernet является доминирующей во всем мире технологией локальных сетей LAN. Бо́льшая часть потоков данных, передаваемых по сети Internet, начинает свое движение по Ethernet-соединению и заканчивается на нем. Со времени своего появления технология Ethernet развивалась в направлении удовлетворения все большего спроса на высокоскоростные сети LAN. После появления новой передающей среды — оптоволоконного кабеля — технология Ethernet была адаптирована к ней и начала использовать ее преимущества: огромную ширину полосы пропускания и низкий уровень ошибок в оптоволоконных каналах. Теперь тот же базовый протокол, по которому в 1973 году данные передавались со скоростью 3 Мбит/с, осуществляет передачу со скоростью 10 Гбит/с.

Успех технологии Ethernet стал результатом ее простоты, надежности, легкости поддержки Ethernet-сетей, способности включать в себя новые технологии, а также невысокой стоимости установки и модернизации. С появлением технологии Gigabit Ethernet то, что начиналось как технология локальных сетей, распространилось на расстояния, соответствующие стандартам городских (metropolitan-area) и даже распределенных (wide-area) сетей. В последующих разделах приведен обзор технологии Ethernet, включая историю Ethernet, рассмотрены соглашения о названиях версий Ethernet и форматы фреймов Ethernet.

Введение в технологию Ethernet

Первоначальная идея технологии Ethernet возникла в связи с необходимостью решить проблему того, как сделать возможным использование двумя или более пользователями одной и той же передающей среды без наложения их сигналов. Эта проблема одновременного доступа нескольких пользователей к общей среде передачи изучалась в начале 70-х годов в университете штата Гавайи. Для того чтобы сделать возможным для нескольких станций Гавайских островов согласованный доступ к общему диапазону радиочастот в атмосфере, была разработана система, получившая название Alohanet. Первоначальная технология, на которой базируется сегодняшний Ethernet, была беспроводной. Эта работа позднее стала основой знаменитого MAC-механизма среды Ethernet, известного *как множественный доступ с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access/Collision Detection — CSMA/CD*). Метод CSMA/CD более подробно обсуждается далее в этой главе.

Первоначальная версия технологии Ethernet была первой в мире локальной сетью LAN. Она была создана более 30 лет назад Робертом Меткалфом (Robert Metcalfe) и его коллегами в корпорации Xerox. Первый стандарт Ethernet был опубликован консорциумом компаний Digital Equipment Company, Intel и Xerox (DIX) в 1980 году.

Меткалф хотел, чтобы Ethernet стал совместно используемым стандартом, преимуществами которого пользовались бы все желающие. Поэтому консорциум DIX сделал новый стандарт открытым, т.е. доступным любой компании. В те времена в компьютерной индустрии такое происходило нечасто. Первые аппаратные и программные продукты, разработанные с использованием стандарта Ethernet, поступили на рынок в начале 80-х годов XX в. В то время технология Ethernet позволяла передавать данные со скоростью 10 Мбит/с по толстому (диаметр примерно равен толщине мизинца) коаксиальному кабелю на расстояния до 2-х км. Технология Ethernet сразу получила успех и признание.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers — IEEE) является профессиональной организацией, определяющей сетевые стандарты. В 1985 году комитет стандартов IEEE по локальным и городским сетям опубликовал свои стандарты для сетей LAN. Стандарты IEEE для LAN-технологий в настоящее время преобладают и являются наиболее известными стандартами локальных сетей во всем мире. Их названия начинаются с номера 802. Основанный на технологии Ethernet стандарт LAN-сетй получил название 802.3. Институт IEEE хотел обеспечить совместимость и гармоничное взаимодействие своих стандартов с эталонной моделью OSI международной организации ISO. Стандарт IEEE подразделяет канальный уровень модели OSI на два подуровня: управления доступом к среде передачи (Media Access Control — MAC) и управления логическим каналом (Logical Link Control — LLC).

В результате такого подхода в стандарт 802.3 были внесены незначительные изменения по сравнению с первоначальным стандартом Ethernet. Между спецификациями DIX Ethernet и 802.3 имеются некоторые различия. Однако эти различия столь незначительны, что любая плата сетевого интерфейса Ethernet (Network Interface Card — NIC) может отправлять и получать пакеты и фреймы как стандарта Ethernet, так и 802.3. По существу спецификации Ethernet и IEEE 802.3 представляют собой один и тот же стандарт. Следует, однако, помнить, что официальным стандартом Ethernet IEEE в настоящее время является 802.3.

В середине 80-х годов XX в. полосы пропускания Ethernet, равной 10 Мбит/с, была более чем достаточно для компьютеров того времени. Однако к началу 90-х годов персональные компьютеры стали работать значительно быстрее, и пользователи начали выражать неудовлетворение заторами в сети, возникавшими вследствие малой полосы пропускания Ethernet-среды сетей LAN. В 1995 г. институт IEEE объявил о создании нового стандарта Ethernet — 100 Мбит/с. Вслед за этим в 1998-1999 гг. последовали стандарты Gigabit Ethernet (со скоростью передачи 1 миллиард битов в секунду). В июне 2002 года институт IEEE одобрил стандарты Ethernet 10 Гбит/с. Эти современные стандарты по-прежнему представляют собой модифицированную первоначальную технологию Ethernet (802.3).

Все новые Ethernet-стандарты в своей основе совместимы с первоначальным стандартом Ethernet. Пакет технологии Ethernet (фрейм) может выйти с адаптера персонального компьютера со скоростью 10 Мбит/с, помещен маршрутизатором в оптоволоконный канал Ethernet 10 Гбит/с и в конечном итоге передан в адаптер Ethernet 100 Мбит/с. До тех пор, пока пакет не покидает сети Ethernet разных типов,

он остается неизменным. Этим объясняется большой успех технологии Ethernet — она легко допускает масштабирование сетей, построенных по этой технологии. Это означает, что полоса пропускания сети может быть неоднократно расширена без внесения изменений в базовую Ethernet-технологию.

В первоначальную технологию Ethernet неоднократно вносились дополнения с целью включения новых передающих сред и повышения скорости передачи. Важно, однако, понимать, что основы первоначальной технологии Ethernet при этом оставались неизменными. Все стандарты Ethernet 802.3 принадлежат к одному и тому же семейству. Между этими стандартами имеются различия, однако их значительно меньше, чем общих для них характеристик. Наличие таких общих характеристик, идущих от оригинальной технологии Ethernet, означает, что все протоколы семейства 802.3 совместимы друг с другом.

Обозначения IEEE для различных версий технологии Ethernet

Термин *Ethernet* применяется по отношению ко всему семейству сетевых технологий, включающему в себя оригинальную технологию Ethernet, технологии *Fast Ethernet*, *Gigabit Ethernet* (или Gig-E) и *10-Gb Ethernet* (или 10-G). Стоимость Ethernet-интерфейсов может находиться в диапазоне от 10 до 100 000 долларов США. Скорости передачи могут принимать значения 10, 100, 1000 и 10 000 Мбит/с. В этом разделе подробно рассматриваются первоначальная технология Ethernet (10BASE-T), технологии Fast Ethernet (100BASE-TX и 100BASE-FX), Gigabit Ethernet (1000BASE-T и 1000BASE-X), а также Ethernet со скоростью передачи 10 Гбит/с. Две характеристики Ethernet остаются неизменными во всех версиях: базовый формат фрейма и IEEE-подуровни второго уровня эталонной модели OSI.

В случае, когда технологию Ethernet необходимо расширить для добавления нового типа передающей среды или новых функций, Институт IEEE выпускает новые дополнения к стандарту 802.3. Новые дополнения получают одно- или двухбуквенное обозначение, например, для Fast Ethernet используется обозначение 802.3u. Дополнению также задается аббревиатура (называемая идентификатором). Ниже приведены примеры таких дополнений.

- 10BASE2 — IEEE 802.3a.
- 10BASE5 — IEEE 802.3.
- 100BASE-T — IEEE 802.3i.
- 1000BASE-TX — IEEE 802.3X.

Как мы видим, аббревиатура состоит из следующих частей:

- числа, указывающего скорость передачи в мегабитах;
- слова BASE, указывающего на использование внутриполосной (базовой) сигнализации;
- числа (2 или 5), указывающего максимальную длину сегмента коаксиального кабеля (длина 185 м округлена до 200 м, на что указывает цифра 2);

- одной или более букв алфавита, указывающих на используемый тип передающей среды (F — оптоволоконный кабель (fiber optical cable), T — медная неэкранированная витая пара (copper unshielded twisted pair)).

Внутриполосная сигнализация представляет собой простейший метод сигнализации. При ее использовании вся полоса пропускания передающей среды используется для передачи полезного сигнала. Сигнал, представляющий данные (уровни напряжения в кабеле UTP или интенсивность светового сигнала в оптоволоконном кабеле), передается непосредственно по передающей среде. Другого специального сигнала (называемого несущим сигналом или несущей) при этом не требуется. В технологии Ethernet используется базовая сигнализация.

Альтернативный метод сигнализации, называемый широкополосной (broadband signaling) в технологии Ethernet не используется. При широкополосной сигнализации сигнал, представляющий данные, никогда не подается непосредственно в среду передачи. Вместо этого аналоговый сигнал, называемый несущим сигналом или просто несущей, модулируется сигналом данных. Затем полученный модулированный несущий сигнал передается по среде передачи. Широкополосная сигнализация используется, в частности, в радиопередаче и в кабельном телевидении.

Институт IEEE, как и международная организация по стандартизации (International Organization for Standardization — ISO), является органом разработки стандартов. От производителей сетевого оборудования не требуется, однако, полностью выполнять все спецификации всех стандартов. Институт IEEE ставит перед собой следующие цели:

- поставлять инженерную информацию, необходимую для разработки устройств, отвечающих стандартам Ethernet;
- не ограничивать производителей в новых технических разработках.

При создании новой небольшой LAN-сети или модернизации уже существующей все оборудование можно приобрести у одного производителя с хорошей репутацией. В этом случае можно быть уверенным в полной совместимости всех приобретенных устройств. Однако в том случае, когда пользователь имеет дело с крупной сетью, состоящей из множества небольших сетей LAN технологии Ethernet с оборудованием, приобретенным у нескольких разных производителей, возникает совершенно иная ситуация. Обеспечение надежной совместной работы оборудования от различных производителей представляет собой весьма важную и иногда достаточно трудоемкую задачу. К сожалению, не существует промышленного или правительственного агентства, которое могло бы протестировать устройство и гарантировать его полное соответствие стандарту IEEE. Однако такое положение вещей является серьезным доводом в пользу самостоятельного изучения промышленных стандартов. Фактически лишь собственные знания и знания коллег являются основой для принятия решений при приобретении оборудования и проектировании сети.

Интерактивная презентация: стандарты серии 802 Института IEEE.
Выполнение заданий этой презентации позволит закрепить и систематировать знания о стандартах 802 Института IEEE.

Технология Ethernet и эталонная модель OSI

Стандарты LAN-сетей определяют характеристики физической среды и разъемы, используемые для подсоединения устройств на физическом уровне эталонной модели OSI. Стандарты LAN также определяют способ коммуникации устройств на канальном уровне. Дополнительно стандарты LAN определяют зависящий от конкретного протокола тип инкапсуляции данных, который позволяет соответствующим образом их обрабатывать по мере продвижения потоков данных между различными уровнями эталонной модели OSI. Несмотря на существенные различия в технологиях нижних уровней, протоколы и средства верхних уровней от них не зависят. Для выполнения этих функций канальный уровень технологии Ethernet Института IEEE имеет два подуровня:

- *подуровень управления доступом к среде (Media Access Control — MAC*) (802.3). Как указывает само название, MAC-подуровень определяет способ передачи фреймов в физическую передающую среду. На этом подуровне решаются вопросы физической адресации всех устройств, определения сетевой топологии и дисциплины канала;
- *подуровень управления логическим каналом (Logical Link Control — LLC*) (802.2). Как показывает само название, подуровень LLC отвечает за логическую идентификацию различных типов протоколов и последующую инкапсуляцию согласно им. Код типа протокола или идентификатор точки доступа к службе (Service Access Point — SAP) выполняют логическую идентификацию ресурса. Тип LLC-фрейма, используемый конечной станцией, зависит от того, какой идентификатор ожидается протоколом более высокого уровня (таким, например, как протокол IP). Хотя *IEEE 802.2* представляет собой стандартный тип *инкапсуляции* (*encapsulation*), используются также и другие типы, такие, как Ethernet II (используемый в первую очередь в сетях LAN Ethernet на основе протоколов TCP/IP). Они обсуждаются далее в этой главе.

Как показано на рис. 6.1, стандарт *IEEE 802.3* определяет физический уровень (первый уровень) и MAC-часть канального (первого) уровня.

На рис. 6.2 изображены разнообразные технологии первого уровня модели OSI и нижняя половина второго уровня. В этой книге основное внимание уделено технологии Ethernet сетей LAN. Первый (физический) уровень эталонной модели OSI описывает интерфейс устройств со средой передачи, сигнализацию, перемещение битовых потоков по среде передачи, компоненты, передающие сигналы в передающую среду, и различные топологии сетей LAN. Физический уровень играет ключевую роль в коммуникации между отдельными компьютерами, однако его функций недостаточно для работы сети. Каждая из этих функций имеет свои ограничения. Эти ограничения преодолеваются на втором уровне.

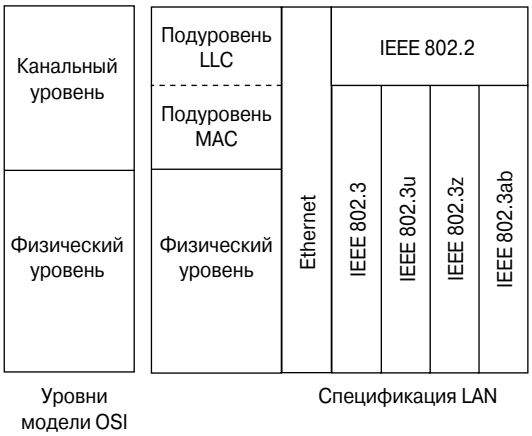


Рис. 6.1. Стандарт Ethernet и эталонная модель OSI

Рис. 6.2. Спецификации сетей LAN и эталонная модель OSI

Как показано в табл. 6.1, для каждого ограничения первого уровня имеется соответствующее решение на втором уровне.

Подуровни LLC и MAC второго уровня являются действующими и полезными соглашениями, которые делают технологию совместимой, а связь между компьютерами — возможной. MAC-подуровень управляет физическими компонентами, которые будут использоваться для передачи информации. Как и другие уровни, подуровень LLC остается относительно независимым от физического оборудования, которое будет использоваться в процессе коммуникации. Подуровень LLC позволяет

поддерживать несколько протоколов третьего уровня, таких, как IP и IPX, а также различные типы фреймов.

На рис. 6.3 проиллюстрировано соответствие между различными версиями технологии Ethernet, первым уровнем и частью второго уровня модели OSI. Хотя существуют и иные версии технологии Ethernet, приведенные на этом рисунке используются наиболее часто и находятся в центре рассмотрения в нашей книге.

Таблица 6.1. Проблемы первого уровня, решаемые на втором

Ограничения первого уровня	Решение на втором уровне
Первый уровень не может осуществлять связь с верхними уровнями	Второй уровень осуществляет связь с верхними уровнями через подуровень LLC
Первый уровень не может идентифицировать отдельные компьютеры	Второй уровень идентифицирует отдельные компьютеры с помощью MAC-схемы адресации
Первый уровень оперирует только потоками битов	На втором уровне создаются фреймы для организации или группировки битов (в этом процессе группа битов приобретает определенное значение)
Первый уровень не может принять решение о том, какой компьютер из группы компьютеров, пытающихся передавать двоичные данные в данный момент, будет первым осуществлять передачу	Для принятия этого решения второй уровень использует MAC-подуровень

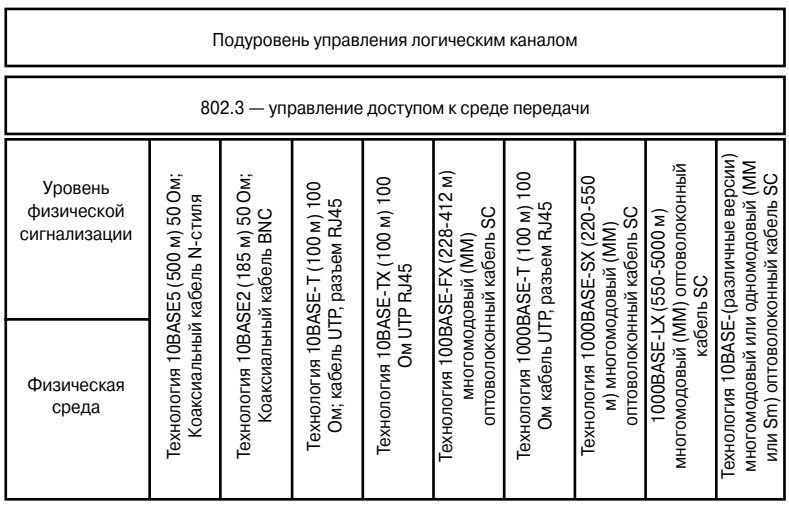


Рис. 6.3. Соответствие технологий Ethernet и модели OSI

MAC-адресация

Для того чтобы в сети Ethernet стала возможной локальная доставка фреймов, необходима определенная система адресации, т.е. присвоения имен компьютерам и интерфейсам. Каждый компьютер имеет уникальный способ самоидентификации. Никакие два физических адреса в сети не должны быть одинаковыми. Физические адреса, называемые адресами *управления доступом к передающей среде (Media Access Control — MAC-адрес)*, записаны в сетевом адаптере NIC. Для MAC-адреса используются и другие названия: аппаратный адрес, NIC-адрес, адрес второго уровня и Ethernet-адрес.

MAC-адреса в сети Ethernet используются для уникальной идентификации отдельных устройств. Каждое устройство (ПК, маршрутизатор, коммутатор и т.д.), имеющее Ethernet-интерфейс к сети LAN, должно иметь MAC-адрес, в противном случае другие устройства не смогут обмениваться с ним данными. MAC-адрес имеет длину 48 битов и записывается в виде 12-ти шестнадцатеричных цифр. Первые шесть шестнадцатеричных цифр, задаваемых IEEE, идентифицируют производителя или продавца устройства и, таким образом, включают в себя *уникальный идентификатор организации (Organizationally Unique Identifier — OUI*). Остальные шесть шестнадцатеричных цифр включают в себя серийный номер интерфейса или другое значение, задаваемое конкретным производителем. MAC-адреса иногда называют прошитыми (Burned-In Address — BIA), поскольку они записаны в постоянной памяти (Read-Only Memory — ROM) интерфейса или устройства и копируются в оперативную память (Random-Access Memory — RAM) при инициализации сетевого адаптера NIC. На рис. 6.4 показан формат MAC-адреса.

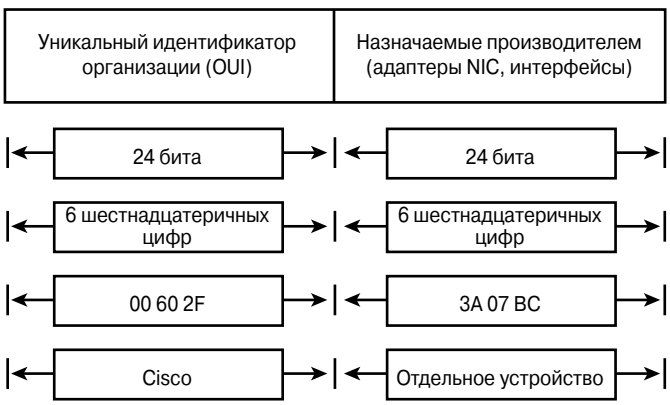


Рис. 6.4. Формат MAC-адреса

Без MAC-адресов сеть LAN представляла бы собой лишь группу изолированных компьютеров, и доставка Ethernet-фреймов была бы невозможной. Вследствие этого на канальном уровне к данным верхних уровней добавляются *заголовок (header*), содержащий MAC-адрес устройства, и *концевик (trailer*). Заголовок и концевик содержат

управляющую информацию, предназначенную для канального уровня устройства, которому направляется фрейм. Данные верхних уровней инкапсулируются в заголовок и концевик канального уровня.

LAN-сети спецификаций Ethernet и 802.3 являются широковещательными. Это означает, что все станции сети видят все проходящие по сети фреймы, и каждая станция должна исследовать каждый фрейм, для того чтобы выяснить, не является ли она требуемым пунктом назначения этого фрейма.

В сети Ethernet в случае, когда устройству требуется отправить данные другому устройству, оно может открыть маршрут коммуникации к другому устройству, используя свой MAC-адрес. Когда устройство-отправитель посылает данные в сеть, эти данные включают в себя MAC-адрес требуемого пункта назначения. По мере того, как эти данные перемещаются по сетевой среде, адаптер NIC каждого устройства, к которому они поступают, проверяет, не совпадает ли его MAC-адрес с адресом пункта назначения, содержащимся во фрейме данных. Если такого соответствия нет, то адаптер отбрасывает этот фрейм. Если же такое соответствие имеется, то адаптер NIC проверяет адрес получателя в заголовке фрейма, для того чтобы удостовериться в правильности адресации пакета. При поступлении данных на требуемую станцию ее адаптер делает их копию, удаляет заголовок и концевик и передает их компьютеру для обработки протоколами более высокого уровня, такими, как IP и TCP.

Фреймирование на втором уровне

Закодированные потоки битов в физической среде представляют собой огромное технологическое достижение, однако их недостаточно для осуществления коммуникации. Превращение этих битовых потоков во фреймы позволяет получать из них существенную информацию, которая не может быть получена из самих по себе закодированных битовых потоков. Дополнительная информация, которая может содержаться во фреймах, включает:

- сведения о том, какие компьютеры осуществляют связь друг с другом;
- сведения о том, когда начинается связь между двумя индивидуальными компьютерами и когда она заканчивается;
- она обеспечивает распознавание ошибок, которые могут произойти в процессе коммуникации;
- она содержит указания, чья очередь “говорить” в “диалоге” между двумя компьютерами;
- сведения о том, где во фрейме расположены собственно полезные данные.

После того как определен способ идентификации отдельных компьютеров, можно перейти к процессу создания фреймов. Создание фреймов происходит в процессе инкапсуляции данных на втором уровне эталонной модели OSI. Фрейм представляет собой модуль данных протокола второго уровня. На рис. 6.5 проиллюстрированы понятия бита и фрейма.

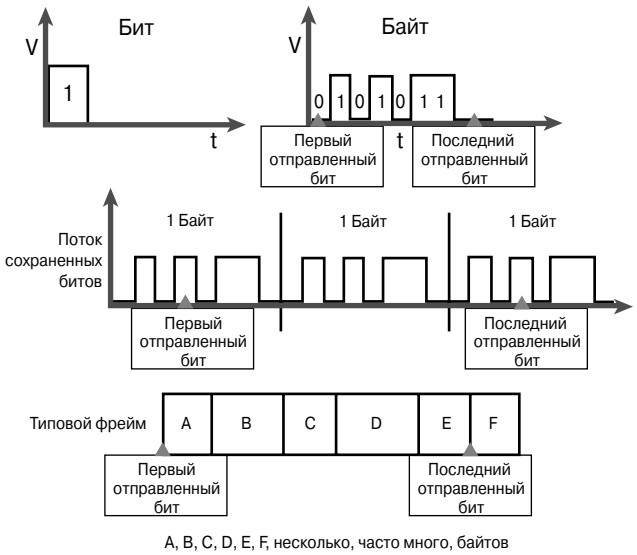


Рис. 6.5. Переход от битов к фреймам

При работе с битами наиболее наглядным представлением является график зависимости напряжения от времени. Однако обычно приходится иметь дело с более крупными порциями данных, а также с адресами и управляющей информацией, в результате чего изображение всей этой информации в виде графика из-за большого ее объема было бы ненаглядным и весьма неудобным. Другим типом представления может быть диаграмма формата фрейма, которая строится на основе зависимостей напряжения от времени. Такую диаграмму можно читать слева направо, как обычное изображение на осциллографе. Диаграмма формата фрейма отображает группы битов (поля); при этом с различными полями связываются определенные функции.

Различными стандартами описываются многие типы фреймов. Отдельный фрейм в общем случае состоит из частей, называемых *полями (fields*), каждое из которых, в свою очередь, состоит из байтов (рис. 6.6). Во фрейме канального уровня обычно присутствуют следующие поля:

- поле начала фрейма (Frame Start);
- поле адреса (Address field);
- поле длины/типа/управляющее (Length/Type/Control field);
- поле данных (Data field);
- поле контрольной последовательности фрейма (Frame Check Sequence — FCS).

Рис. 6.6. Так выглядит формат фрейма в самом общем случае

Ниже различные поля фреймов описываются более подробно.

Дополнительная информация: поля фрейма

Поле начала фрейма

После того как компьютеры подключены к физической среде передачи, для каждого из них должен существовать способ привлечь внимание всех остальных, для того чтобы широковещательно передать некоторое сообщение, например, такое: “Внимание! В сеть поступает фрейм!”. В различных технологиях для этого используются различные процедуры, однако, независимо от типа используемой технологии, все фреймы имеют начальную сигнальную последовательность байтов.

Поле адреса

Все фреймы содержат идентификационную информацию, такую, как адрес компьютера-отправителя (MAC-адрес) и адрес компьютера-получателя (MAC-адрес).

Поля длины и типа фрейма

Большинство фреймов имеют специализированные поля. В некоторых технологиях поле длины фрейма (Length field) указывает точную длину фрейма. В некоторых других имеется поле типа фрейма (Type field), указывающее протокол 3-го уровня, осуществляющий запрос. Во многих технологиях такие поля отсутствуют.

Поле данных

Целью отправки фреймов является передача данных более высокого уровня (в конечном итоге данных приложения пользователя) от компьютера-отправителя компьютеру-получателю. Пакет данных, который необходимо при этом доставить, включает само передаваемое сообщение (данные пользователя). Для того чтобы фрейм имел определенную минимальную длину, иногда в него добавляются байты-заполнители, не несущие смысловой нагрузки. В стандартных фреймах IEEE в поле данных включаются также байты подуровня управления логическим каналом (Logical Link Control — LLC). Следует помнить о том, что подуровень LLC добавляет управляющую информацию к данным сетевого протокола в пакет 3-го уровня для облегчения доставки пакета в пункт назначения. Таким образом, второй уровень взаимодействует с более высокими уровнями через подуровень LLC.

Поле контрольной последовательности фрейма

Все фреймы (а также содержащиеся в них биты, байты и поля) вследствие различных причин в процессе передачи могут повреждаться и к моменту поступления к получателю содержать ошибки. Поле контрольной последовательности фрейма (Frame Check Sequence — FCS) содержит значение, вычисленное на основе данных фрейма при его отправке компьютером-отправителем. При получении фрейма компьютер-получатель вновь вычисляет это значение и сравнивает его со значением FCS, содержащимся во фрейме. Если эти два значения не совпадают, то фрейм квалифицируется как ошибочный и отбрасывается.

Значение контрольной последовательности фрейма обычно вычисляется с помощью алгоритма проверки циклической избыточности (Cyclic Redundancy Check — CRC), который выполняет полиномиальные вычисления над данными фрейма.

Структура фрейма Ethernet

На MAC-подуровне для всех скоростей передачи Ethernet (10/100/1 000/10 000 Мбит/с) структура фрейма практически одинакова. В версии полудуплексного Gigabit Ethernet 1000BASE-T и в "W"-версиях 10 Гбит/с Ethernet есть некоторые особенности, связанные с синхронизацией, требующие изменений в обработке MAC-уровнем промежутков между фреймами, однако во всех остальных аспектах эти технологии аналогичны технологиям с другими скоростями. Однако на физическом уровне почти все версии Ethernet существенно отличаются друг от друга, и каждая скорость имеет свои собственные правила проектирования архитектуры сети.

Ethernet-фреймы спецификации IEEE 802.3

Кроме рассмотренного выше типа фрейма 802.2, существует более простой тип фрейма 802.3, разработанный Институтом IEEE. Что касается спецификации 802.2, то в современных локальных Ethernet-сетях она используется достаточно редко. На рис. 6.7 показан базовый формат Ethernet-фрейма спецификации IEEE 802.3.

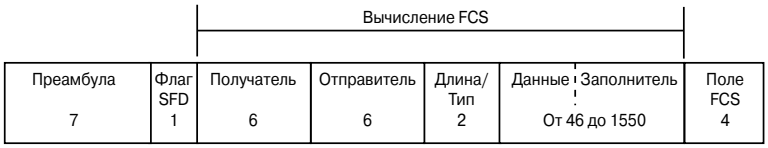


Рис. 6.7. Структура фрейма Ethernet спецификации 802.3 Института IEEE

В табл. 6.2 для каждого поля Ethernet-фрейма 802.3 приведены размер в октетах и название поля.

Таблица 6.2. Поля фрейма Ethernet IEEE 802.3

Размер поля в октетах	Поле фрейма
7	Преамбула
1	Флаг начала фрейма (Start Frame Delimiter — SFD)
6	MAC-адрес получателя
6	MAC-адрес отправителя
2	Поле длина/тип (используется как длина фрейма, если в шестнадцатеричной записи значение поля меньше 0600, в противном случае представляет собой тип протокола)
46 to 100	Данные и/или биты заполнения
4	Контрольная последовательность фрейма (Frame Check Sequence — FCS, циклическая контрольная сумма CRC)

Дополнительная информация: фрейм Ethernet II

В DIX-версии технологии Ethernet, которая была разработана до принятия в качестве стандарта Ethernet-версии IEEE 802.3, поле преамбулы (Preamble) и поле флага начала фрейма (Start Frame Delimiter — SFD) были объединены в одно, хотя двоичное представление было тем же. Поле длины/типа (Length/Type) в ранних версиях IEEE содержало только длину фрейма, а в DIX-версии — только его тип. Эти два варианта использования поля были объединены в новой версии стандарта IEEE, которая вышла позже, поскольку оба варианта широко использовались в сетевой индустрии. Ранний формат фрейма DIX Ethernet, также известный как Ethernet Version 2 (Ethernet версии 2), или Ethernet II, представляет собой тип фрейма, наиболее часто используемый в локальных Ethernet-сетях на базе стека протоколов TCP/IP.

На рис. 6.8 показан формат фрейма Ethernet II.

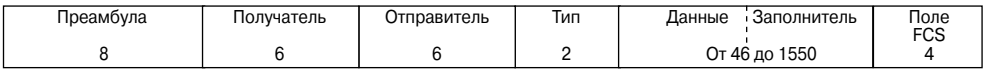


Рис. 6.8. Формат фрейма Ethernet II

В табл. 6.3 для каждого поля фрейма Ethernet II приведены номер октета и название.

Таблица 6.3. Поля фрейма Ethernet II

Размер поля в октетах	Поле фрейма
8	Преамбула (у 802.3 SFD заканчивается цифрами 10101011)
6	MAC-адрес получателя
6	MAC-адрес отправителя
2	Поле типа (Type Field), если длина заголовка меньше 46 октетов, то к нему добавляются биты заполнения, чтобы общая длина была равна требуемой
От 46 до 1500	Данные и/или биты заполнения
4	Контрольная последовательность фрейма (Frame Check Sequence — FCS, циклическая контрольная сумма CRC)

Как показано в табл. 6.3, поле типа фрейма (Type field) в стандарте Ethernet II включено в текущее определение фрейма 802.3. После получения фрейма принимающая станция должна определить, какой протокол верхнего уровня присутствует в поступившем фрейме. Сначала она пытается сделать это, анализируя поле длины/типа фрейма. Если это состоящее из двух октетов значение равно или больше шестнадцатеричного числа 600, то фрейм интерпретируется согласно указанному коду типа Ethernet II. Если же это значение меньше шестнадцатеричного числа 600, то фрейм интерпретируется как фрейм 802.3, и значение этого поля рассматривается как длина фрейма. Для определения дальнейших действий требуется дополнительный анализ. Начиная с этого момента, исследуются первые четыре октета поля данных (Data field) фрейма 802.3. Значение, извлеченное из этих первых четырех октетов, обычно проверяется на наличие двух уникальных значений; если они отсутствуют, то предполагается, что фрейм инкапсулирован подуровнем управления логическим каналом (Logical Link Control (LLC) и декодируется соответственно указанной LLC-инкапсуляции, описанной в спецификации 802.2. Одним из таких проверяемых значений является шестнадцатеричное число AAAA, которое указывает на инкапсуляцию 802.2/802 протокола доступа к подсети (Subnetwork Access Protocol — SNAP). Другим проверяемым значением является шестнадцатеричное число FFFF, которое может указывать на необработанную “raw” инкапсуляцию протокола IPX корпорации Novell (Internetwork Packet Exchange — протокол межсетевого пакетного обмена).

Поля Ethernet-фрейма

Ниже описано большинство требуемых или разрешенных полей фрейма Ethernet 802.3. Структура фрейма Ethernet 802.3 проиллюстрирована рис. 6.8.

- **Преамбула (Preamble)**. Это поле содержит набор чередующихся нулей и единиц, которые использовались для временной синхронизации в асинхронной реализации технологии Ethernet со скоростью передачи 10 Мбит/с и в более медленных. Высокоскоростные версии технологии Ethernet являются синхронными, поэтому эта информация синхронизации избыточна, однако сохраняется для совместимости с предыдущими версиями. Преамбула имеет длину семь октетов и представляется следующим бинарным набором: 10101010 10101010 10101010 10101010 10101010 10101010 10101010.
- **Флаг начала фрейма (Start Frame Delimiter — SFD)**. Это поле имеет длину один октет и отмечает конец информации синхронизации. Оно представляется двоичным значением 10101011. В старой DIX-версии технологии Ethernet этот октет был последним в восьмиоктетной преамбуле. Хотя в ней первые восемь октетов были описаны иначе, чем в версии Ethernet Института IEEE, вышеупомянутое значение и его использование были такими же. Следует также отметить, что информация синхронизации, представленная в преамбуле и поле SFD, отбрасывается и не принимается в расчет, когда речь идет о минимальном и максимальном размерах фрейма.
- **Адрес получателя (Destination Address)**. Это поле содержит шестиоктетный MAC-адрес получателя. Адрес получателя может быть адресом одноадресатной рассылки (отдельный узел), многоадресатной рассылки (группа узлов) или широковещательным (рассылка всем узлам).
- **Адрес отправителя (Source Address)**. Это поле содержит шестиоктетный MAC-адрес отправителя. Предполагается, что адрес отправителя может быть только одноадресатным идентификатором передающей Ethernet-станции. Однако все чаще применяются виртуальные протоколы, которые иногда используют конкретный MAC-адрес для идентификации виртуального объекта.

  В старых спецификациях технологии Ethernet MAC-адреса могли состоять из двух или шести октетов, при условии, что этот размер был одинаковым для всех станций *широковещательного домена (broadcast domain*). Двухоктетная адресация была явным образом исключена параграфом 3.2.3 версии стандарта 802.3, принятой в 1998 году, и с тех пор в Ethernet-версии 802.3 не поддерживается.

- **Длина/Тип (Length/Type)**. Если это значение меньше десятичного числа 1536 (или шестнадцатеричного 0600), то оно указывает длину фрейма. Интерпретация поля как длины используется в тех случаях, когда уровень LLC обеспечивает идентификацию протокола.
  - **Тип фрейма (тип Ethernet)**. Поле типа фрейма (Type) указывает протокол более высокого уровня, которому будут переданы данные после окончания обработки на уровне Ethernet.
  - **Длина фрейма (длина IEEE 802.3)**. Поле длины фрейма указывает количество байтов данных, которые следуют за этим полем. Если это значение равно или больше десятичного числа 1536 (или шестнадцатеричного 0600), то оно указывает тип протокола, и в этом случае содержимое поля данных (Data field) декодируется согласно указанному протоколу. Список основных протоколов для Ethernet (Ethertype protocols) приводится в спецификации RFC 1700, начиная со страницы 168.
- **Данные и биты заполнения (Data and Pad field)**. Это поле может иметь произвольную длину, не превосходящую максимально допустимый размер фрейма. *Максимальный блок передачи (Maximum Transmission Unit — MTU)* для технологии Ethernet составляет 1500 октетов, и объем данных не должен превосходить это значение. На содержимое этого поля не накладываются никакие условия. Заполнитель произвольного вида вставляется сразу после данных пользователя в том случае, когда пользовательских данных недостаточно для достижения фреймом минимальной длины. Согласно параметрам структуры фрейма, длина поля данных должна находиться в интервале от 46 до 1500 октетов. В действительности спецификация Ethernet не налагает это условие. От фрейма требуется, чтобы его длина была не менее 64 октетов и не более 1518 октетов, а размер поля данных строго не задан. Пользователю предлагается самостоятельно вычислить размер поля данных путем вычитания из полного размера фрейма длину всех остальных полей. Если используются требуемые в настоящее время шестиоктетные MAC-адреса, то размер поля данных будет находиться в диапазоне от 46 (при необходимости добавляется заполнитель) до 1500 октетов.
- **Данные (IEEE 802.3)**. После того как обработка фрейма на физическом и канальном уровнях завершена, данные передаются протоколу более высокого уровня, который должен быть определен в поле данных фрейма. Если данных фрейма недостаточно для того, чтобы он имел минимальный размер 64 байта, то добавляются байты заполнителя, с тем чтобы фрейм имел длину как минимум 64 байта.
- **Контрольная последовательность фрейма (Frame Check Sequence — FCS)**. Эта последовательность содержит четырехбайтовое значение циклического избыточного кода (Cyclical Redundancy Check — CRC), которое вычисляется посылающим фрейм устройством, а затем повторно вычисляется получающим этот фрейм устройством для проверки того, не был ли фрейм поврежден в процессе передачи. В это четырехоктетное поле помещается результат выполнения

алгоритма проверки CRC. Передающая станция вычисляет контрольную сумму для передаваемого фрейма, а полученное значение вставляется за полем данных (или за битами заполнения). Приемная станция (станции) выполняет те же вычисления и сравнивает новую контрольную сумму с находящейся в конце пересылаемого фрейма. Если эти два значения совпадают, фрейм считается полноценным. Для вычисления контрольной суммы используются значения всех полей, начиная с поля адреса получателя и заканчивая полем данных, как показано на рис. 6.7. Преамбула, показанная на рис. 6.8, показывает, что поле SFD и поле расширения (Extension) при вычислении не используются. Поле FCS является единственным Ethernet-полем, которое передается в неканоническом порядке (сначала передается самый старший двоичный разряд).

Поскольку повреждение даже одного бита в любом месте, начиная от поля адреса получателя до поля FCS, приводит к неравенству контрольных сумм, при вычислении контрольной суммы используется и она сама. Вследствие этого невозможно отличить случай повреждения поля контрольной суммы от случая повреждения любого предшествующего поля, используемого при вычислении FCS.

Принцип работы сети Ethernet

В тех случаях, когда нескольким станциям (узлам) необходимо получить доступ к физической среде и к другим сетевым устройствам, могут быть использованы различные методы управления доступом. В этом разделе кратко описаны различные стратегии получения доступа и подробно рассмотрен метод управления доступом, применяемый в сетях Ethernet, — CSMA/CD (Carrier Sense Multiple Access with Collision Detection — множественный доступ с контролем несущей и обнаружением конфликтов).

Следует отметить, что, несмотря на огромную историческую важность и большое практическое значение метода CSMA/CD на начальной стадии развития технологии Ethernet, в настоящее время его значение несколько уменьшается по двум причинам:

- при использовании кабеля UTP с четырьмя парами имеются отдельные пары для передачи (Tx) и приема (Rx), что потенциально делает медный кабель UTP свободным от коллизий и позволяет работать в дуплексном режиме, в зависимости от того, размещен ли он в совместно используемой среде (в сети с концентраторами) или в коммутируемой ;
- аналогичная логика применима и к оптоволоконным каналам, в которых используются отдельные оптические маршруты: отдельный кабель для передачи и отдельный — для приема.

Новая версия технологии Ethernet — 1000BASE-TX, Gigabit Ethernet, при использовании медного кабеля использует все четыре пары одновременно, что вызывает постоянную коллизию. В прежних типах сетей Ethernet такая постоянная коллизия

сделала бы сеть неработоспособной. Однако в версии 1000BASE-TX сложная система соединений позволяет нейтрализовать состояние постоянной коллизии, возникающее из попытки получать по кабелю UTP максимально возможный объем данных.

Управление доступом к передающей среде

Под управлением доступом к среде (Media Access Control — MAC) понимаются протоколы, которые в совместно используемой среде (коллизионном домене) определяют, какому компьютеру предоставить право передавать данные. Подуровни MAC и LLC описываются IEEE-версией второго уровня. MAC и LLC являются подуровнями второго уровня. Существуют два общих типа MAC-подуровня:

- детерминистический (существует очередность предоставления доступа);
- недетерминистический (право передачи предоставляется первому обратившемуся по принципу "первым пришел — первым обслужен"(first come, first served)).

Технологии Token Ring и FDDI являются детерминистическими, а Ethernet/802.3 — недетерминистической (также называется вероятностной).

Детерминистические MAC-протоколы

Детерминистические MAC-протоколы при предоставлении права на передачу используют очередность, иногда шутливо называемую "передачей хода". Примером детерминистического протокола может служить протокол передачи маркера Token Ring. В некоторых американских индейских племенах существовал обычай во время собраний передавать "говорящую палочку". Тот, кому она передавалась, получал право говорить. Когда этот человек заканчивал свою речь, он передавал палочку другому.

В этой аналогии совместно используемой средой был воздух, данными — слова говорящего, а протоколом — обладание "говорящей палочкой". Такую палочку можно было бы назвать маркером. Описанная ситуация аналогична сети, использующей протокол канального уровня Token Ring. В сети Token Ring отдельные станции образуют кольцо, как показано на рис. 6.9. По такому кольцу циркулирует специальный маркер. Если какой-то станции требуется передать данные, она захватывает маркер, в течение определенного времени передает данные, а затем передает маркер в кольцо, где он может быть перехвачен другой станцией.

Недетерминистические MAC-протоколы

Недетерминистические MAC-протоколы используют механизм доступа согласно принципу "первым пришел — первым обслужен" (first-come, first-served — FCFS). Примером недетерминистического MAC-протокола является метод множественного доступа CSMA/CD.

При использовании этой технологии общего доступа среда Ethernet позволяет сетевым устройствам конкурировать за право передачи. Станции в сети, использующей метод CSMA/CD, прослушивают сеть и ожидают момента, когда она будет свободна

для передачи данных. Однако если две станции начинают передачу одновременно, то происходит коллизия (столкновение), и попытки передачи обеих станций оказываются безуспешными. Все станции сети также узнают об этой коллизии и ожидают, когда канал передачи освободится. Передающие станции, в свою очередь, ожидают в течение некоторого случайным образом выбираемого промежутка времени перед попыткой повторной передачи, что уменьшает вероятность повторной коллизии.

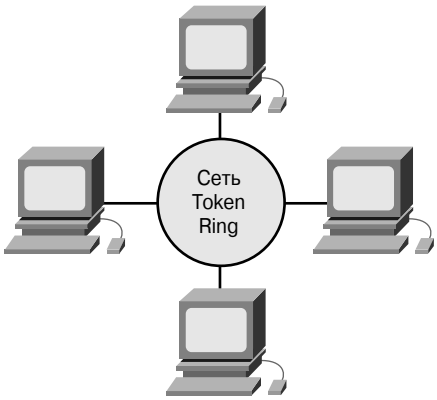


Рис. 6.9. Сеть Token Ring

Три топологии сети Ethernet и их MAC-протоколы

Тремя основными технологиями второго уровня являются Token Ring, FDDI и Ethernet. Из этих трех технологий Ethernet используется гораздо чаще остальных, однако все три иллюстрируют различные подходы к реализации локальных сетей LAN. Они определяют элементы второго уровня (например, LLC, имена, метод создания фреймов и MAC-подуровень), а также компоненты сигнализации на первом уровне и характеристики передающей среды. Ниже дается характеристика этих трех технологий.

- *Технология Ethernet* представляет собой логическую шинную топологию (информация проходит по линейной шине).
- *Технология Token Ring* представляет собой логическую кольцевую топологию (иными словами, информация перемещается по кольцу) и физическую звездообразную (соединения образуют звезду).
- *Технология FDDI* представляет собой логическую кольцевую (информационный поток перемещается по кольцу) и физическую топологию двойного кольца (соединения образуют двойное кольцо).

MAC-подуровень и обнаружение коллизий

Среда Ethernet представляет собой широковещательную технологию совместного доступа. Используемый в среде Ethernet метод доступа CSMA/CD выполняет три функции:

- передачу и получение пакетов данных;
- декодирование пакетов данных и проверку действительности содержащихся в них адресов перед передачей их более высоким уровням модели OSI;
- обнаружение ошибок в пакетах данных или в работе сети.

При использовании метода доступа CSMA/CD сетевые устройства, имеющие данные для передачи, находятся в режиме "прослушивание сети перед передачей" (listen-before-transmit mode), иначе называемом "контролем несущей" (Carrier Sense — CS). В технологии Ethernet совместного доступа такой подход означает, что когда устройству требуется передать данные, оно должно предварительно удостовериться в том, что сетевая среда свободна для передачи. После того как устройство проверило, что в сетевой среде нет сигналов, оно начинает передавать данные. Передавая данные в виде сигналов, устройство продолжает прослушивание среды для того, чтобы быть уверенным в том, что другие устройства не ведут передачу одновременно с ним. Если две станции ведут передачу одновременно, возникает коллизия, как показано на рис. 6.10. После окончания передачи устройство возвращается в режим прослушивания сети. В традиционной технологии Ethernet при совместном использовании среды передачи в каждый конкретный момент передавать данные может только одно устройство. В коммутируемой среде Ethernet это утверждение становится неверным, что подробно описывается в главе 8, "Ethernet-коммутация".

Сетевые устройства способны обнаруживать возникновение коллизии, поскольку она сопровождается увеличением амплитуды сигнала в сетевой среде. Такая функция называется обнаружением коллизий (Collision Detect — CD). Когда возникает коллизия, каждое устройство, которое в данный момент осуществляет передачу, продолжает ее в течение короткого промежутка времени для того, чтобы коллизию могли увидеть все устройства в сети. Когда все устройства увидели, что в сети произошла коллизия, передающие устройства вызывают алгоритм, известный как алгоритм *возврата* (*backoff*). После того как все передающие устройства осуществили возврат и воздержались от передачи в течение некоторого случайно выбранного (и, следовательно, разного у всех устройств) промежутка времени, любое устройство может попытаться вновь получить доступ к среде передачи. При возобновлении передачи устройства, которые были вовлечены в произошедшую коллизию, не имеют приоритета в передаче данных. Процесс передачи в сети, использующей метод доступа CSMA/CD, обобщенно показан на рис. 6.11.

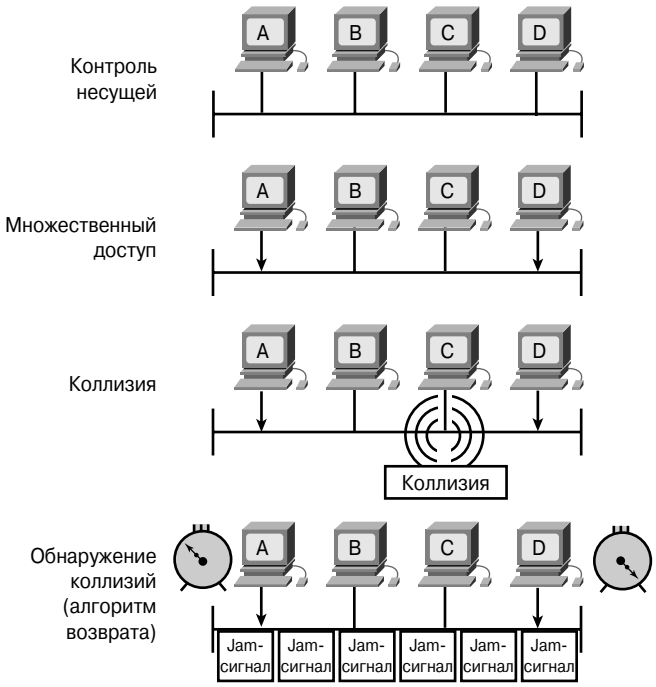


Рис. 6.10. Метод доступа CSMA/CD

Ethernet представляет собой широковещательную технологию передачи данных. Это означает, что все устройства в сети могут "видеть" все фреймы, проходящие мимо них в сетевой среде. Однако не все устройства обрабатывают эти данные. Только устройство, MAC-адрес которого совпадает с MAC-адресом получателя, находящимся во фрейме, копирует этот фрейм в свой буфер. В технологии Ethernet адреса протоколов третьего уровня, таких, как IP или IPX, не просматриваются и не используются. Если MAC-адреса совпадают, то фрейм копируется в буфер и передается на третий уровень для проверки соответствия IP- или IPX-адреса получателя адресу устройства.

После того как устройство проверило MAC- и IP-адрес, содержащиеся в данных, пакет проверяется на наличие в нем ошибок. Если они обнаруживаются, пакет отбрасывается. Устройство-получатель не информирует об этом отправителя, независимо от того, прибыл ли пакет благополучно или нет. По этой причине Ethernet называется сетевой структурой *без установки соединения* (*connectionless*) и *негарантированной доставкой* (*best-effort delivery*).

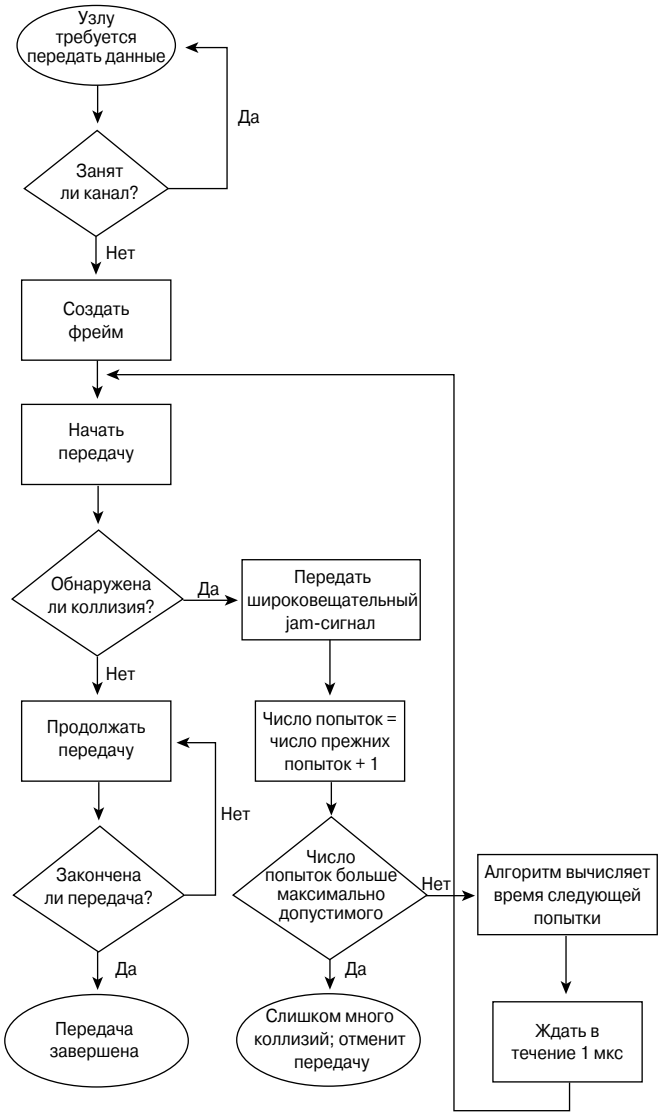


Рис. 6.11. Процесс получения доступа к сетевой среде по методу CSMA/CD

Дополнительная информация: симплексный, полудуплексный и дуплексный режимы

Каналы передачи данных могут функционировать в одном из трех режимов: симплексном, полудуплексном и дуплексном. Различие между ними состоит в возможных направлениях передачи сигнала.

Симплексная передача (simplex transmission), как указывает само название, является самым простым режимом. Она также называется односторонней (однонаправленной), поскольку сигналы

перемещаются только в одном направлении, как автомобили на улице с односторонним движением. Примерами симплексной связи могут служить радио- или телепередачи, как показано на рис. 6.12.

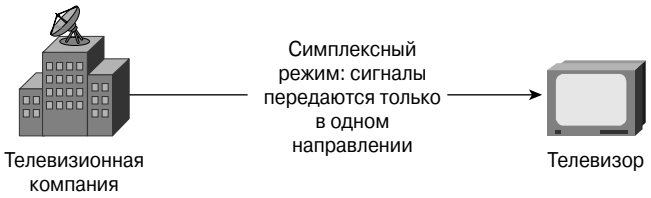


Рис. 6.12. Симплексная передача

Полудуплексная передача (*half-duplex transmission*) представляет собой усовершенствованную симплексную передачу, поскольку сигналы могут передаваться в обоих направлениях. Однако, хотя передача и может осуществляться в обоих направлениях, но она происходит не одновременно, как показано на рис. 6.13. Полудуплексная технология Ethernet, определенная в первоначальной спецификации Ethernet 802.3, использует только один провод, по которому сигнал может передаваться в обоих направлениях. Однако в каждый момент времени передача данных от передающей станции принимающей может происходить только в одном направлении. При этом для предотвращения коллизий используется протокол CSMA/CD, а в случае коллизии происходит повторная передача.

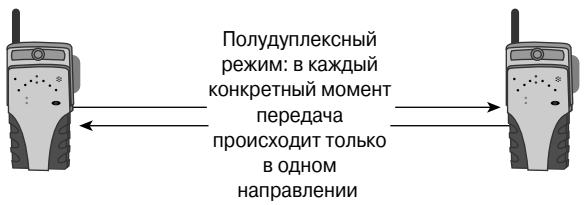


Рис. 6.13. Полудуплексная передача

Дуплексная передача (full-duplex), как показано на рис. 6.14, функционирует как улица с двусторонним движением. Потоки автомобилей могут двигаться в обоих направлениях одновременно. Дуплексная передача стала возможной благодаря применению технологии с коммутацией, которая подробно описана в главе 8, “Ethernet-коммутация”. Дуплексная технология с использованием коммутации значительно увеличивает производительность сети, поскольку данные одновременно передаются и принимаются. Дуплексный Ethernet использует две пары проводов, которые позволяют станции-получателю и станции-отправителю одновременно обмениваться данными. Фактически в сети дуплексного Ethernet-режима коллизии вообще не происходят, поскольку технология коммутации при необходимости для двух устройств обменяться данными создает между двумя станциями виртуальный канал типа “точка-точка”, или “микросегмент”. Предполагается, что дуплексный Ethernet позволяет достичь стопроцентной эффективности использования канала в обоих направлениях. Это означает, что в дуплексном режиме Ethernet 10 Мбит/с предоставляют пользователю 20 Мбит/с. Коммутатор 100 Мбит/с в дуплексном режиме потенциально обеспечивает станции полосу пропускания 200 Мбит/с.

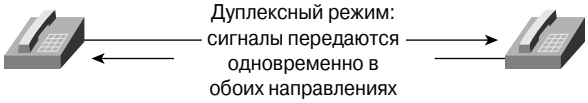


Рис. 6.14. Дуплексная передача

Синхронизация в сетях Ethernet

При создании технологии Ethernet предполагалось, что она будет функционировать в структуре с общей шиной; на техническом языке это выражает тот факт, что каждая станция "слышит" все проходящие по сети сообщения практически в один и тот же момент времени. Формально такой метод доступа называется CSMA/CD. Упрощенно это означает следующее: в случае, когда две станции обнаруживают, что они ведут передачу одновременно, они прекращают ее и ожидают в течение некоторого времени перед повторной передачей.

Базовые правила и спецификации для нормального функционирования сети Ethernet несложны, хотя в некоторых реализациях физического уровня уровень сложности возрастает. Несмотря на принципиальную простоту технологии Ethernet, при возникновении проблемы в такой сети часто оказывается весьма сложным поиск источника возникшей проблемы. Поскольку структура Ethernet использует общую шину (которая может быть названа одной распределенной точкой возможных сбоев), сфера возможного сбоя охватывает все станции сети, принадлежащие сегменту в коллизионном домене. При использовании повторителей этот сегмент может включать в себя станции ближайших сегментов, число которых может достигать четырех.

Согласно требованиям спецификации, любая станция в сети Ethernet, которой требуется передать данные, сначала прослушивает канал, для того чтобы убедиться в том, что другие станции не ведут в данный момент передачу. Если сигнал в кабеле отсутствует, станция немедленно начинает передачу. Однако поскольку сигналу требуется, хотя и небольшое, время для прохождения по кабелю (т.н. *задержка распространения — propagation delay*), а каждый повторитель на маршруте вносит свою долю задержки при пересылке фрейма с одного своего порта на другой, становится возможной ситуация, когда более одной станции начинают передачу практически одновременно. В этом случае возникает коллизия.

Если подсоединенная станция работает в дуплексном режиме, она может пересылать и получать данные одновременно, и коллизий не будет. При работе в дуплексном режиме меняется также подход к синхронизации и пропадает потребность в канальных интервалах (timeslot) при передаче данных. Дуплексный режим позволяет проектировать более крупные сети, поскольку пропадает ограничение синхронизации, связанное с обнаружением коллизий.

При работе в дуплексном режиме и при отсутствии коллизий отправляющая данные станция передает 64 бита информации временно*й* синхронизации, которая в целом часто называется преамбулой. Такая информация включает в себя:

- MAC-адреса получателя и отправителя;
- некоторую другую информацию заголовка;
- полезную нагрузку (передаваемые данные);
- контрольную сумму (FCS), используемую для проверки того, что данные не были повреждены в процессе передачи.

Станции, получающие фрейм, вновь вычисляют контрольную сумму FCS для проверки целостности получаемого сообщения и передают неповрежденные данные на более высокий уровень используемого стека протоколов.

В версии Ethernet 10 Мбит/с и более медленных, которые используют асинхронный режим передачи, каждая принимающая станция использует 8 октетов дополнительной информации для синхронизации своего принимающего канала с поступающими данными, а затем отбрасывает эти октеты. Версия 100 Мбит/с и более высокоскоростные реализации Ethernet используют синхронный режим, поэтому в действительности информация синхронизации вообще не нужна. Однако для совместимости преамбула и флаг SFD сохранены и в более поздних версиях. Вся информация, следующая за блоком SFD в конце информационного модуля синхронизации, передается на более высокий уровень. При этом заново вычисляется контрольная сумма и сравнивается с контрольной суммой, находящейся в конце полученного фрейма. Если фрейм не поврежден, он должен интерпретироваться в соответствии с правилами протокола, указанного в поле длины или типа (Length/Type) или протокола LLC-уровня, указанного первыми восемью октетами данных.

В версиях стандарта Ethernet 1998 и 2000 годов в базовую структуру Ethernet было внесено большое количество изменений. Одним из значительных изменений было явное включение в стандарт двухоктетных адресов, хотя неявно они присутствовали и во всех предыдущих версиях. В случае указания в поле спецификации 802.3 длина/тип (Length/Type) длины (Length) было задано точное максимальное значение этого поля (длина/тип), равное 1536 (шестнадцатеричное число 600), в то время как ранее оно предполагалось равным максимальной величине модуля данных MTU, равной 1500 (шестнадцатеричное число 5DC).

Для всех скоростей передачи в Ethernet-сети, равных или меньших 1000 Мбит/с, стандарт требует, чтобы время передачи было не меньшим величины канального интервала. Величина канального интервала для Ethernet 10 Мбит/с и 100 Мбит/с составляет 512 битовых интервалов (64 октета). Канальный интервал для Ethernet 1000 Мбит/с составляет 4096 битовых интервалов (512 октетов, включая расширение). Для технологии Ethernet со скоростью передачи 10 Гбит/с канальный интервал не определен, поскольку в этой версии не допускается полудуплексный режим работы.

Длительность канального интервала определяется тем, что максимальное время задержки при самом длинном циклическом маршруте по максимальной длине кабеля, используемого в самой обширной сетевой структуре, и все задержки распространения в аппаратном обеспечении максимальны; при обнаружении коллизий используется 32-битовый сигнал переполнения. Иными словами, канальный интервал просто должен быть больше того времени, которое теоретически требуется фрейму для того, чтобы переместиться от одной самой удаленной точки наибольшего коллизионного домена Ethernet до другой, самой удаленной, испытать коллизию с другим передаваемым фреймом в самый последний момент, осколком фрейма вернуться к передававшей его станции и быть зарегистрированным как поврежденный в результате коллизии. Для надежной работы системы необходимо, чтобы первая станция узнавала о произошедшей коллизии до того, как она закончит отправку фрейма наименьшего возможного размера. Для того чтобы сеть Ethernet 1000 Мбит/с могла

функционировать в полудуплексном режиме при отправке небольших фреймов, было добавлено поле расширения (Extension), просто для того, чтобы передатчик был занят в течение времени, которое требуется, чтобы фрагмент претерпевшего коллизию фрейма вернулся назад. Это поле присутствует только в полудуплексных каналах 1000 Мбит/с; оно позволяет увеличить длину фрейма минимального размера (64 октета) до той, которая нужна для удовлетворения требований продолжительности канального интервала. Биты расширения отбрасываются принимающей станцией.

Для иллюстрации изложенного выше рассмотрим следующий пример: в сети Ethernet 10 Мбит/с для передачи одного бита на MAC-подуровне требуется 100 наносекунд (нс). На скорости 100 Мбит/с для передачи бита требуется 10 нс, а на скорости 1000 Мбит/с — только 1 нс. В табл. 6.4 приведены значения битовых интервалов для различных версий Ethernet.

Таблица 6.4. Битовые интервалы для различных версий Ethernet

Скорость передачи (Мбит/с)	Битовый интервал (нс)
10	100
100	10
1000 (1 Гбит/с)	1
10 000 (10 Гбит/с)	0,1

В качестве приближенной оценки при вычислении задержки распространения в кабеле UTP принимается значение 8 дюймов (20,3 см) за одну наносекунду. Для кабеля UTP длиной 100 м такая величина означает, что для прохождения сигнала в сети 10BASE-T расстояния в 100 м требуется менее 5 битовых интервалов (4,92 битового интервала). Для вычисления соответствующего значения при использовании скоростей 100 Мбит/с и 1000 Мбит/с достаточно лишь передвинуть десятичную точку, что дает значения соответственно 49,2 битовых интервалов для 100 Мбит/с и 492 битовых интервалов — для 100 Мбит/с.

Для того чтобы метод CSMA/CD правильно работал в сети Ethernet, отправляющая станция должна узнать о коллизии до того, как она закончила передачу фрейма минимального размера. При скорости передачи данных в 100 Мбит/с синхронизация в системе едва успевает сработать при длине кабеля 100 м. В сети со скоростью передачи 1000 Мбит/с требуются специальные и весьма неэффективные меры, поскольку отправляющая станция успевает передать весь фрейм минимального размера до того, как первый бит достигнет конца первого стометрового отрезка кабеля UTP. Такой пример ясно показывает, почему в сетях Ethernet со скоростью передачи данных 10 Гбит/с полудуплексный режим не разрешен.

Межфреймовый зазор и алгоритм возврата

В табл. 6.5 приведены значения минимального зазора между двумя несталкивающимися пакетами, также называемого межфреймовым зазором — от последнего бита поля FCS первого фрейма до первого бита преамбулы второго фрейма.

Таблица 6.5. Межфреймовый зазор

Скорость передачи	Межфреймовый зазор (битовых интервалов)	Требуемое время (мкс)
10 Мбит/с	96	9,6
100 Мбит/с	96	0,96
1 Гбит/с	96	0,096
10 Гбит/с	96	0,0096

В сети Ethernet со скоростью передачи 10 Мбит/с после того, как какая-либо станция отправила фрейм, все станции должны ожидать в течение как минимум 96 битовых интервалов (9,6 мкс), до того как они смогут начать передачу своих фреймов. В высокоскоростных версиях Ethernet межфреймовый зазор остается тем же — 96 битовых интервалов. Однако время, соответствующее этому количеству битовых интервалов, становится меньшим, как показано в табл. 5.6. Такой интервал также называется межфреймовым зазором, межфреймовым интервалом, межпакетным зазором и предназначен для того, чтобы медленные станции успели обработать предыдущий фрейм и подготовиться к приему следующего.

Таблица 6.6. Параметры канального интервала

Скорость	Канальный интервал[1] (битовых интервалов)	Временной интервал (мкс)
10 Мбит/с	512	51,2
100 Мбит/с	512	5,12
1 Гбит/с	4096	4,096
10 Гбит/с	Не применяется	—

Однако ожидается, что повторитель регенерирует все 64 бита информации синхронизации (преамбулу и SFD) в начале каждого фрейма, несмотря на потенциальную возможность потери части начальных битов преамбулы для замедления синхронизации. Таким образом, вследствие вынужденного введения битов синхронизации некоторое уменьшение межфреймового зазора не только возможно, но и ожидается. Некоторые наборы микросхем Ethernet-интерфейсов чувствительны к уменьшению межфреймового интервала, и если оно происходит, то они могут "пропустить" некоторые фреймы. При увеличении вычислительной мощности настольного компьютера (передающей станции) он легко может переполнить сегмент Ethernet пересылаемыми данными и начать повторную передачу до того, как истечет время межфреймовой задержки. На протяжении нескольких лет некоторые производители сознательно в определенной степени нарушали требования межфреймового зазора для улучшения тестовых результатов при сравнительных испытаниях своих продуктов и продукции конкурентов. По большей части такие хитрости с межфреймовым интервалом не приводили к серьезным проблемам, однако потенциально они возможны.

[1] *Канальные интервалы используются только в полудуплексных соединениях Ethernet. — Прим. ред.*

После того как произошла коллизия и все станции освобождают кабель от сигнальной нагрузки (каждая из них ожидает в течение полного интервала), станции, фреймы которых участвовали в коллизии, должны ожидать дополнительное, и в принципе, бо́льшее время до попытки повторной передачи столкнувшихся фреймов. Период ожидания намеренно рассчитывается практически случайным образом для того, чтобы две станции не использовали один и тот же промежуток времени перед повторной передачей, в противном случае результатом стали бы новые коллизии. Частично требуемое поведение достигается путем расширения интервала, из которого выбирается случайным образом время повторной передачи при каждой попытке пересылки фрейма. Период ожидания измеряется в величинах, кратных значению канального интервала.

Дополнительная информация: повторная передача фрейма

Время повторной передачи выбирается в соответствии со следующим принципом:

$0 \le r < 2^k$,

где r — случайная величина, которая кратна канальному интервалу, а k — число попыток повторной передачи (его максимальное значение равно 10). Время возврата определяется по формуле:

r × длительность канального интервала.

Максимальное количество попыток повторной передачи равно 16, хотя количество возвратов остается равным 10 для нескольких последних попыток. Указанное выше произведение задает минимальный период ожидания для попытки повторной передачи. Для станции вполне приемлемо, хотя и не требуется, ввести дополнительную задержку, которая уменьшит передаваемое ей количество данных.

В качестве примера рассмотрим ситуацию, когда после пятой последовательной коллизии и безуспешной попытки передать фрейм 10BASE-T время ожидания для станции будет случайным числом из диапазона $0 \le r < 32$ канальных интервалов. После неудачной попытки первой передачи время задержки согласно приведенной выше формуле будет случайным числом, кратным 51,2 микросекунды в диапазоне от нуля до 1638,4.

Если MAC-подуровень после 16-ти попыток не может отправить фрейм, он прекращает их и генерирует сообщение об ошибке, передаваемое протоколу более высокого уровня. Такие случаи достаточно редки и происходят только в условиях чрезвычайных нагрузок в сети или при наличии проблем физического уровня.

Существует лишь одна специальная ситуация, в которой даже после 16-ти попыток подобные сбои происходят достаточно часто — эта ситуация обычно наблюдается в коммутируемых каналах. Она называется захватом пакета, или эффектом пакетного истощения. Если два устройства (коммутаторы, станции или и те, и другие), работающие в полудуплексном режиме, одновременно пытаются передать крупные блоки данных, происходит коллизия. Какая бы станция ни “выиграла” право первой повторной передачи, с каждой последующей коллизией она будет иметь все большую вероятность получения права передачи. Предположим, произошла вторая коллизия. Первая станция, которая могла передавать свой первый фрейм, снова выбирает случайный промежуток времени между нулевым и первым временными интервалами, в то время как вторая станция теперь выбирает между нулевым, первым, вторым и третьим временными интервалами. Весьма вероятно, что первая станция вновь получит меньшее время задержки и право на передачу. Вполне вероятно, что первая станция выиграет право на повторную передачу в течение 16-ти последовательных попыток у второй станции. В этом случае вторая станция прекратит попытки передачи и отбросит фрейм. У нее также появится запись об ошибке, связанная с избыточным количеством попыток. Этот тип ошибок обычно обнаруживается с использованием управляющих средств, таких, как *простой протокол*

управления сетью (Simple Network Management Protocol — SNMP), который посылает запросы порту коммутатора. Часто бывает, что к порту, на котором происходит такая ошибка, подсоединено всего лишь одно устройство. Поскольку потоки передаваемых данных в сетях Ethernet по самой своей природе имеют неравномерный характер (всплески), такая ситуация может возникнуть на порту, который имеет сравнительно небольшую среднюю нагрузку.

Обработка ошибок

Чаще всего (и обычно без серьезных последствий) состояние ошибки в сети Ethernet возникает в результате коллизии. Коллизии являются механизмом разрешения конфликтов за право доступа к сети. Несколько коллизий обеспечивают для сетевых узлов достаточно простой, удобный и не вызывающий большой служебной нагрузки способ разрешения споров за сетевые ресурсы. В ситуации, когда сеть не может функционировать соответствующим образом из-за различных проблем, коллизии могут стать существенной помехой ее эффективной работе. Коллизии возможны только в полудуплексных сегментах.

При возникновении коллизий тратится рабочее время сети в двух аспектах.

- Прежде всего теряется часть полосы пропускания, равная сумме первоначально передаваемых данных, и сигнал коллизии (т.н. jam-сигнал, или сигнал затора). Такое явление называется *задержкой потребления*; оно затрагивает все сетевые узлы. Задержка потребления значительно уменьшает пропускную способность сети. Вслед за каждой успешной или неудачной попыткой передачи для всех станций сети наступает период простоя (период возврата), называемый межфреймовым зазором (или межфреймовым интервалом), который также влияет на пропускную способность сети.
- Второй аспект задержки связан с алгоритмом возврата после коллизии. Задержки возврата обычно незначительны.

Большое число коллизий происходит очень рано во фрейме, часто еще до флага SFD. О коллизиях, имевших место до флага начала фрейма (SFD), обычно не сообщается более высоким уровням, как если бы коллизии вообще не происходили. Как только обнаруживается коллизия, отправляющая станция (станции) передает 32-битовый jam-сигнал, который навязывает состояние коллизии всем станциям.

На рис. 6.15 две станции прослушивают сеть, для того чтобы убедиться в том, что кабель свободен, и начать передачу. Стандарт 802.3 устанавливает ограничения на время задержки сигнала каждым компонентом системы в самом худшем случае. Максимальная задержка при передаче сигнала в прямом и обратном направлениях в коллизионном домене при скорости передачи данных 10 Мбит/с составляет 512 битовых интервалов; это значение определяет минимальный размер фрейма. Первой начинает передачу станция 1 и успевает передать большую часть данных до того, как будет обнаружена коллизия. Станция 2 до обнаружения коллизии успевает отправить лишь несколько битов.

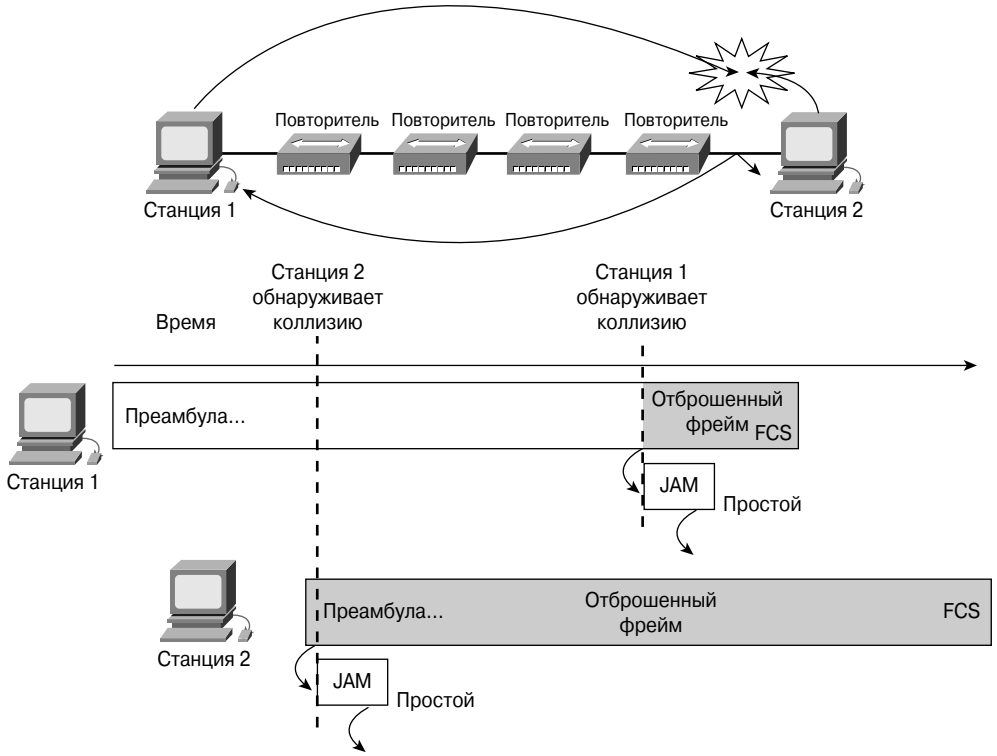


Рис. 6.15. Типичная обработка ошибок в коллизионном домене, который работает со скоростью 10 Мбит/с

Рассмотрим пример, показанный на рис. 6.15, более подробно. Станция 1 может передать значительную часть фрейма еще до того, как сигнал достигнет последнего сегмента кабеля. Станция 2 не успевает получить первый бит передачи до начала своей собственной передачи. Станция 2 может послать только несколько битов до того, как адаптер NIC обнаружит коллизию. Сразу после ее обнаружения станция 2 прекращает текущую передачу и подставляет на место передаваемых данных 32-битовый jam-сигнал. После этого станция 2 полностью прекращает передачу. Во время коллизии и передачи jam-сигналов, которые испытывает станция 2, фрагменты фреймов, поврежденных во время коллизии, движутся в обратном направлении по коллизионному домену в направлении станции 1. Станция 2 заканчивает передачу 32-битового jam-сигнала и после этого переходит в режим молчания до того момента, когда фрагменты коллизии достигнут станции 1. При этом станция 1, по-прежнему не зная о коллизии, продолжает передачу. Когда, наконец, фрагменты коллизии достигают станции 1, она также прерывает текущую передачу и подставляет 32-битовый jam-сигнал вместо оставшейся части передаваемого фрейма. После отправки 32-битового jam-сигнала станция 1 также прекращает все передачи.

Jam-сигнал может состоять из любых двоичных данных, поскольку он не является соответствующей контрольной суммой для уже переданной части фрейма. Наиболее часто в качестве jam-сигнала используется простое чередование единиц и нулей: 1, 0, 1, 0..., такое же, как и в преамбуле. При просмотре с помощью анализатора протоколов такой сигнал представляется как шестнадцатеричное число 5 или A-последовательность. Поврежденные частично переданные фрагменты (сообщения) часто называются фрагментами коллизии или, иногда, сленговым термином "карлики" (карликовыми фреймами). В отличие от запоздалых коллизий, обычные коллизии имеют длину менее 64 октетов и из-за этого не могут пройти тест минимальной длины и тест контрольной суммы FCS.

Типы коллизий

Коллизии обычно происходят в том случае, когда две или более станций, находящихся в одном коллизионном домене, одновременно ведут передачу. Коллизии регистрируются счетчиками событий большинством диагностических инструментов, однако они могут быть зарегистрированы и отдельно, как одиночные или множественные коллизии, когда коммутатор или другая станция опрашиваются протоколом SNMP. Понятие "одиночная коллизия" относится к тому случаю, когда при первой попытке передачи фрейма произошла коллизия, однако следующая попытка была успешной. Множественная коллизия означает, что успешной отправке фрейма предшествовали несколько неудачных попыток. Второй случай отличается от случая отложенной передачи, поскольку при откладывании передачи коллизия не происходит. Отложенная передача означает, что при попытке станции или коммутатора передать фрейм среда была занята, и потребовалось ожидать своей очереди на передачу. При неоднократных безуспешных попытках передать фрейм возможна ситуация, когда он вообще не будет передан; при этом сообщается, что отправка отменена из-за избыточного числа коллизий.

Результаты коллизий — фрагменты фреймов и поврежденные фреймы, длина которых меньше 64 октетов и которые имеют недействительную контрольную сумму, часто называются коллизионными фрагментами. Некоторые анализаторы протоколов и сетевые мониторы называют эти фрагменты "карликами", однако такой термин не совсем точен.

Основными типами ошибок фреймов в сетях Ethernet, которые могут быть зарегистрированы в сеансе работы анализатора протоколов, являются:

- локальная коллизия;
- удаленная коллизия;
- запоздалая коллизия.

Три типа коллизий показаны на рис. 6.16. В последующих разделах кратко рассмотрены эти типы ошибок фреймов.

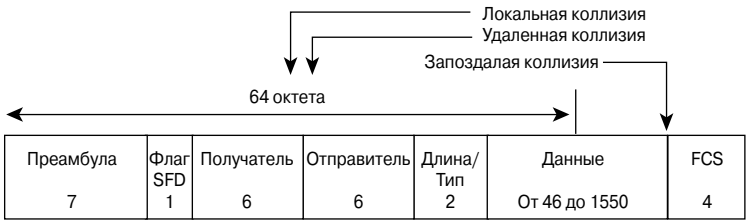


Рис. 6.16. Типы коллизий: локальная, удаленная и запоздалая

Дополнительная информация: локальные, удаленные и запоздалые коллизии

Локальные коллизии

Локальная коллизия в коаксиальном кабеле (10BASE2 или 10BASE5) происходит в том случае, когда проходящий по кабелю сигнал “встречается” с сигналом от другой станции. При этом волны сигналов накладываются друг на друга, в результате чего некоторые части сигнала взаимно погашаются, а другие удваиваются. Удвоение сигнала приводит к тому, что его напряжение превышает допустимый максимум. Такое состояние регистрируется всеми станциями локального кабельного сегмента как коллизия. В мониторах адаптеров NIC имеется специальная цепь, которая следит за возникновением состояния избыточного напряжения. Порогом избыточного напряжения является значение приблизительно в 1,5 В, измеряемое в коаксиальном кабеле. На рис. 6.17 показаны сигнал и коллизия в сети 10BASE2/10BASE5, которые зарегистрированы цифровым запоминающим осциллографом.

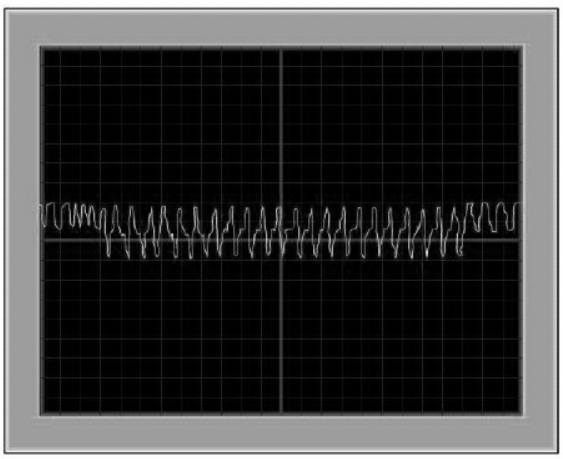


Рис. 6.17. Локальная коллизия в сети 10BASE2/10BASE5

На рис. 6.17 начало графика отображает обычные данные манчестерского кода. Через несколько периодов сигнала амплитуда волны удваивается — это начало коллизии, когда две волны накладываются друг на друга. Перед самым окончанием графика амплитуда возвращается к нормальному значению — в этот момент станция, которая первой обнаружила коллизию, прекращает передачу, а jam-сигнал от второй станции все еще наблюдается.

В кабеле UTP (таком, как 10BASE-T, 100BASE-TX или 1000BASE-T) коллизия в локальном сегменте обнаруживается только тогда, когда станция, передающая данные по паре передачи TX

(transmit), одновременно обнаруживает сигнал на принимающей паре RX (receive). Поскольку эти два сигнала проходят по разным парам, характерного изменения амплитуды сигнала не происходит (см. рис. 6.17). Коллизии в кабеле UTP распознаются только в том случае, когда станция работает в полудуплексном режиме. В этом отношении единственное различие между полудуплексным и дуплексным режимами состоит в том, разрешено ли одновременное использование передающей и принимающей пар. Если станция не ведет передачу, то она не может обнаружить локальную коллизию. Однако возможно и противоположное явление: дефект кабеля, такой, как избыточные наводки, может привести к тому, что станция воспримет свою собственную передачу как коллизию.

Удаленные коллизии

Характерными для удаленных коллизий являются фреймы, которые имеют длину меньше минимальной, недействительную контрольную сумму FCS, но не проявляют себя характерными для локальных коллизий симптомами — избыточным напряжением или одновременной передачей и приемом. Такой тип коллизий обычно возникает из-за столкновения фреймов на дальнем конце соединения, использующего повторители. Повторитель не может пересылать далее сигналы с избыточным напряжением и не может вызвать у станции одновременную активность обеих пар: принимающей RX и передающей TX. Для того чтобы обе пары станции были активны, она должна передавать данные, а это может привести к локальной коллизии. В сетях с кабелем UTP такая коллизия — наиболее часто наблюдаемый тип коллизий. Почти все средства мониторинга сетей, регистрирующие коллизии, такие, как программные анализаторы протоколов и средства удаленного мониторинга (Remote Monitoring — RMON), будут обнаруживать только удаленные коллизии, поскольку они являются пассивными прослушивающими устройствами.

Запоздалые коллизии

После того как передающей станцией были переданы первые 64 октета данных, обычная коллизия произойти уже не может. До этого момента будут превышены теоретические максимумы времени распространения данных по сети. Коллизии, которые происходят после передачи первых 64 октетов данных, называются запоздалыми. Наиболее важное различие между такими коллизиями и теми, которые происходят до передачи первых 64 октетов, состоит в том, что Ethernet-адаптер NIC автоматически повторяет передачу попавшего в коллизию фрейма, но не делает этого для фрейма, который попал в коллизию позднее. В том, что касается адаптера NIC, проблем не возникает, поскольку верхние уровни стека протоколов делают вывод, что фрейм был утерян. Кроме повторной передачи, станция, обнаружившая позднюю коллизию, обрабатывает ее точно так же, как и обычную коллизию.

Кроме одного случая, стандарт 802.3 позволяет станции попытаться повторно передать фрейм, попавший в позднюю коллизию, но не требует этого. Версия Gigabit Ethernet явным образом запрещает повторную передачу фреймов, попавших в позднюю коллизию.

Поздняя удаленная коллизия имеет место в том случае, когда истекло время канального интервала и коллизия происходит на дальнем участке работы повторителя. Однако, поскольку повторитель не позволяет наблюдать симптомы локальной коллизии, проявляющиеся как избыточное напряжение или одновременные передача и прием, для обнаружения такой поздней коллизии и сообщения о ней станции, осуществляющей мониторинг, на дальнем сегменте должно присутствовать соответствующее аппаратное обеспечение. Догадаться о том, что на дальнем участке работы повторителя произошла удаленная запоздалая коллизия, можно также путем анализа нескольких последних октетов поврежденного фрейма с целью нахождения последовательностей битов, характерных для jam-сигнала. Обычно такой тип коллизии обнаруживается в локальном сегменте просто как ошибка контрольной суммы FCS.

Ошибки в сетях Ethernet

Зачем изучать ошибки в сетях Ethernet? Ответ прост: поскольку Ethernet является доминирующей технологией локальных сетей (LAN), глубокое понимание характера и причин типичных ошибок имеет огромную ценность как для понимания работы Ethernet-сетей, так и для устранения в них ошибок и неисправностей.

В то время как локальные и удаленные коллизии рассматриваются как нормальный режим работы сети Ethernet, запоздалые коллизии квалифицируются как ошибки. Наличие ошибок в сети Ethernet всегда предполагает дальнейшее исследование характера работы сети. Уровень возникшей проблемы определяет, насколько срочным является вмешательство администратора для устранения возникших ошибок. Некоторое количество ошибок, произошедших за несколько часов работы сети, указывает на проблему невысокого приоритета. Если же за несколько минут произошли тысячи ошибок, требуется срочное вмешательство.

В качестве ошибок в работе сети Ethernet рассматриваются следующие ситуации:

- происходит одновременная передача от нескольких станций до того, как истекло время канального интервала;
- происходит одновременная передача от нескольких станций после того, как истекло время канального интервала;
- чрезмерно длительная передача или передача неразрешенной длительности (ошибка типа jabber, или сбойный пакет; длинный фрейм или ошибочный размер фрейма);
- слишком короткая передача (короткий фрейм, фрагмент коллизии или фрейм-карлик);
- передача фрейма с повреждением (ошибка в контрольной сумме FCS);
- недостаточное или избыточное количество переданных фреймов (ошибка выравнивания — alignment error);
- несоответствие действительного и сообщенного количество октетов во фрейме (ошибка в размере фрейма);
- необычно длинная преамбула jam-событие (несуществующий фрейм — ghost или ошибочный бессмысленный пакет).

Каждая из указанных выше ситуаций должна быть рассмотрена отдельно. Фреймы, которые содержат ошибки, часто, но не всегда, отбрасываются. Нормальные коллизии включены в этот список только для полноты, но в действительности как ошибки не рассматриваются. В следующих разделах кратко описаны некоторые ошибки в сетях Ethernet.

Сбойные пакеты

Определение термина *сбойный пакет (jabber)* в стандарте 802.3 приведено в нескольких местах. Такой пакет представляет собой передачу станцией сигнала в течение времени, равного 20 000–50 000 битовых интервалов. Однако большинство

диагностических средств предполагают, что получен сбойный фрейм, даже когда обнаружена передача блока, большего разрешенной для среды длины, но, тем не менее, она значительно меньше значений из диапазона 20 000–50 000 битовых интервалов. Таким образом, данное выше определение становится расплывчатым, поскольку регистрирующее устройство может рассматривать 1518-октетный фрейм с добавленным тегом сети VLAN и как имеющий разрешенную, и как превышающий стандартную длину. Кроме того, в определении не сказано, имеет ли сбойный пакет (jabber) правильную или ошибочную контрольную сумму FCS. Большинство сбойных пакетов правильнее называть длинными фреймами.

Удлиненные фреймы

Удлиненный фрейм (long frame) — это фрейм, имеющий длину больше разрешенной, однако при этом учитывается возможное наличие тега. Вопрос о том, имеет ли фрейм правильную контрольную сумму FCS, в данном случае не рассматривается. Именно такой вид ошибки обычно имеется в виду, когда говорится об обнаружении в сети сбойного пакета (jabber). На рис. 6.18 показан удлиненный фрейм, длина которого превосходит 1518 октетов.

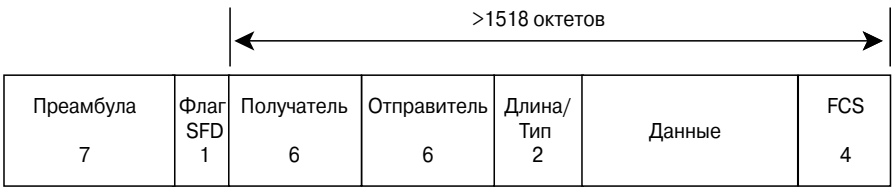


Рис. 6.18. Удлиненный фрейм

Как и сбойный пакет, так и удлиненные фреймы имеют длину больше максимального разрешенного размера фрейма. Однако сбойный пакет (jabber), как правило, имеет значительно бо́льшую длину. Если фрейм спецификации 802.1q имеет тег, он обычно не рассматривается как фрейм больше разрешенной длины. Стандартом IEEE 802.1Q определяется использование, функционирование и администрирование топологий виртуальных локальных сетей (VLAN) в инфраструктуре сети LAN, использующей мосты. Стандарт IEEE 802.1Q разработан для решения проблемы разбиения крупной сети на более мелкие с тем, чтобы широковещательные потоки данных и потоки данных многоадресатной рассылки не захватывали бо́льшую полосу пропускания, чем это необходимо.

Укороченные фреймы

Под *укороченным фреймом* понимается фрейм, имеющий размер меньше минимального разрешенного — 64 октета, и имеющий правильную последовательность контрольной суммы. Некоторые анализаторы протоколов и сетевые мониторы называют такие фреймы карликовыми, однако этот термин следует признать неточным. Как правило, короткие фреймы не обнаруживаются клиентскими устройствами, и их присутствие не обязательно означает некорректную работу сети.

Короткие фреймы формируются обычным образом (за исключением одного аспекта) и имеют правильную контрольную сумму, однако их длина меньше минимального разрешенного размера в 64 октета.

На рис. 6.19 показан короткий фрейм, имеющий длину менее 64 октетов.

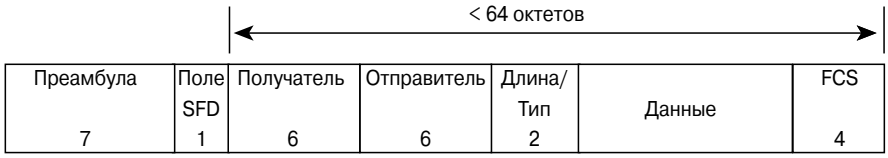


Рис. 6.19. Укороченный фрейм

Карликовые фреймы

Термин *фрейм-карлик* (или карликовый фрейм) является неточным сленговым термином и означает набор данных, имеющий размер меньший, чем разрешено в стандарте. Он может применяться и по отношению к коротким фреймам, имеющим правильную контрольную сумму FCS. Как правило, такое определение применяется по отношению к фрагментам коллизий. Стандарт Ethernet описывает атрибут управления протокола SNMP, называемый "карликом", который имеет размер больше 74 битовых интервалов, но меньше минимального размера фрейма (64 октета при скоростях 10/100 Мбит/с, минимальный размер при полудуплексной передаче составляет 517 октетов при скорости 1000 Мбит/с), и при этом не является результатом локальной коллизии.

Ошибки контрольной суммы FCS

Если у полученного фрейма имеется ошибка в контрольной сумме (ошибка контрольной суммы, или CRC-ошибка), то это означает, что у него по крайней мере один бит отличается от того, который был передан изначально. Если фрейм имеет FCS-ошибку, то, вероятно, информация в заголовке правильная (адреса и т.д.), однако контрольная сумма, вычисленная принимающей станцией, не соответствует значению контрольной суммы, вычисленной отправляющей станцией и находящейся в заключительной части фрейма. Доверять точности адреса, содержащегося лишь в одном фрейме, было бы, вероятно, рискованным, однако если большое количество фреймов имеет один и тот же адрес, то велика вероятность, что такой адрес все же будет правильным.

Большое количество FCS-ошибок от одной станции указывает на неисправность адаптера NIC, ошибочные или поврежденные программные драйверы или на дефекты кабельного канала, соединяющего эту станцию с сетью. Если FCS-ошибки связаны с несколькими станциями, то такая ситуация обычно указывает на неисправность кабельных соединений, несоответствующую версию драйвера сетевого адаптера, неисправный порт концентратора или большое количество вносимых в кабельную систему шумов. Ошибки контрольной суммы регистрируются в том случае, когда хотя бы один бит в передаваемых данных отличается от полученных. При вычислении

новой контрольной суммы принимающей станцией и сравнении ее с контрольной суммой в поле FCS эти два значения не совпадают. В таком случае фрейм отбрасывается.

Ошибка выравнивания

Если граница сообщения фрейма не совпадает с границей октета (т.е. во фрейм помещается не целое число октетов), то такое явление называется *ошибкой выравнивания (alignment error)*. Т.е. вместо правильного количества бинарных битов, которые должны образовать полные октетные группы, имеется несколько дополнительных битов (менее восьми), которые не образуют полный октет. Такой фрейм усекается до ближайшей границы октета, а если не совпадают контрольные суммы, то посылается сообщение об ошибке. Ошибка выравнивания часто вызывается дефектными программными драйверами или коллизией и, как правило, сопровождается несовпадением контрольных сумм. Другими причинами могут быть ошибки операций ввода/вывода, которые вызываются ошибками в программном обеспечении. Если ошибка выравнивания не исправляется, она может вызвать критическую ситуацию в сети. Обычно программное обеспечение само исправляет свои ошибки, однако сбои вызывают внезапную резкую загрузку центрального процессора маршрутизатора.

Нарушение границ фрейма

Появление фрейма, у которого установлено правильное значение в поле длины фрейма (Length field), но не соответствующее количеству октетов в поле данных (Data field), называется *нарушением границ фрейма (range error)*. Эта ошибка также возникает в том случае, когда поле длины фрейма содержит значение, меньшее минимального разрешенного размера поля данных (Data field) при отсутствии заполнителя. Аналогичная ошибка в границе фрейма появляется, когда поле длины фрейма содержит значение, большее максимально разрешенного.

Фреймы-призраки

Корпорация Fluke Networks предложила употреблять термин *фрейм-призрак (ghost)* по отношению к обнаруживаемой в кабеле внешней энергии (шуму), которая выглядит как фрейм, но у которой отсутствует действительный флаг SFD. Для того чтобы быть квалифицированным как “призрак”, этот “фрейм” должен иметь длину не менее 72-х октетов (включая преамбулу), в противном случае он будет классифицирован как удаленная коллизия.

Из-за особой природы фреймов-призраков важно отметить, что результаты тестов в значительной степени зависят от того, в какой части сегмента произведено измерение.

Некоторые типы шумов вводят в заблуждение узлы сетевого сегмента, в результате чего последние считают, что они получают полноценный фрейм. Однако фрейм так и не приходит, поэтому никакие данные для обработки сетевому адаптеру не передаются. Через некоторое время прием данных адаптером прекращается, и он возобновляет передачу своих собственных сообщений. Различные сетевые интерфейсы по-разному реагируют на такие ситуации, и стандартами не определяется, как и

когда должен адаптер NIC реагировать на такой "шумящий" сегмент. Повторители обычно распространяют такие шумовые сигналы в другие сегменты коллизионного домена.

Одним из симптомов присутствия фреймов-призраков является замедление работы сети или полное ее прекращение без видимых причин. При этом файловые серверы практически не загружены, устройства мониторинга сети показывают небольшой уровень загрузки сети, однако пользователи жалуются на медленную работу или даже на простой сети. Этот симптом может быть географически ограничен, т.е. один конец большого (или протяженного) сегмента сети кажется работающим нормально, в то время как на другом конце работа сети резко замедляется или вообще прекращается.

Причинами появления фреймов-призраков обычно является либо короткое замыкание кабеля на заземление, либо другие проблемы с кабелями. Фреймы-призраки заставляют некоторые повторители вести себя так, как если бы они получали фрейм. Поскольку повторители реагируют только на напряжение переменного тока, протекающего по кабелю, ни один полноценный фрейм не может пройти к другим портам. Однако повторитель передает эту энергию на свои остальные порты. Передаваемый фрейм-призрак может выглядеть как шаблон jam-сигнала или даже как очень длинная преамбула.

Большинство средств мониторинга сети не распознает фреймы-призраки по той же причине, по какой они не распознают коллизии при передаче преамбулы — они полностью полагаются на реакцию микросхемной логики сетевых адаптеров. Программные анализаторы протоколов, многие аппаратные анализаторы протоколов и карманные диагностические средства, такие, как большинство средств RMON, не сообщают о таких событиях.

Автоматическое согласование параметров соединения в сетях Ethernet

По мере того как скорости передачи в сетях Ethernet возрастали от 10 к 100 и далее до 1000 Мбит/с, возрастала необходимость обеспечения совместной работы всех этих технологий, вплоть до необходимости непосредственного соединения интерфейсов со скоростями 10, 100 и 1000 Мбит/с.

Для решения этих задач был разработан процесс, названный автосогласованием (autonegotiation) скоростей и дуплексности соединения. В частности, во время ввода в практику технологии Fast Ethernet стандарт включал в себя метод автоматического конфигурирования конкретного интерфейса таким образом, чтобы он соответствовал скорости и возможностям партнера по каналу. Процесс определял, каким образом два партнера по каналу могут автоматически согласовать конфигурацию, которая обеспечит им наибольший общий уровень производительности. Дополнительное преимущество такого подхода состоит в том, что при этом затрагивается только самая нижняя часть физического уровня.

Технология 10BASE-T требует, чтобы каждая станция каждые 16 миллисекунд (мс) передавала канальный импульс, если она в этот момент не передает иное сообщение.

Автоматическое согласование включает в себя сигнал, который называется нормальным канальным импульсом (Normal Link Pulse — NLP). Если отправляется группа таких импульсов, она называется пакетом импульсов быстрого соединения (Fast Link Pulse (FLP) burst). Каждый пакет FLP отправляется с таким же временны*м* интервалом, что и одиночный импульс NLP, для того чтобы устаревшие устройства версии 10BASE-T нормально работали при приеме группы импульсов. На рис. 6.20 показаны временны*е* характеристики импульсов NLP и FLP.

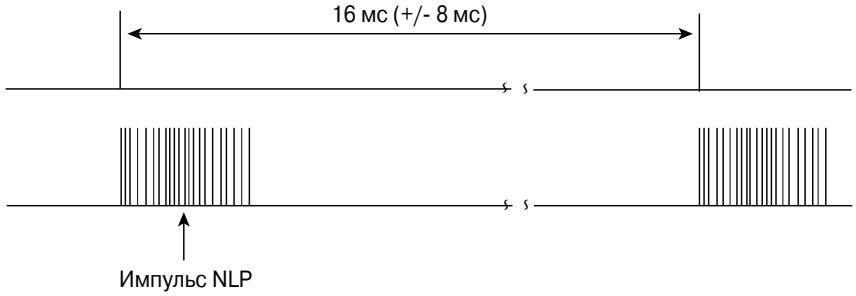


Рис. 6.20. Сравнение временных параметров импульсов NLP и FLP

В технологии 10BASE-T передача происходит с использованием сигнализации с напряжением +1 и —1 В при двухвольтовом дифференциальном пиковом сигнале. NLP-сигнализация использует только диапазон от 0 до +1 В. Длительность одиночного NLP-импульса составляет 100 нс. На рис. 6.21 показаны два типа NLP-импульсов. Импульс слева имеет очень острый пик и четкую форму — он получен от интерфейса, способного работать на скорости 1000 Мбит/с. Импульс справа поступил от устройства старой версии, поддерживающего только скорости 10/100 Мбит/с и не требующего особой четкости сигнала.

Рис. 6.21. Импульсы NLP

Автоматическое согласование осуществляется путем передачи пакета канальных импульсов 10BASE-T каждому партнеру канального соединения. В таких пакетах содержится информация о возможностях передавшей этот пакет станции. После того как обе станции проанализируют предложение своего партнера, они переключаются на общую конфигурацию, соответствующую максимальной производительности, и устанавливают в канале эту скорость и соответствующий режим передачи. Если по какой-либо причине связь прерывается и канал выходит из строя, то сначала оба

партнера пытаются восстановить связь на прежней согласованной скорости. Если это не удается или со времени обрыва канала прошло слишком много времени, то процесс автосогласования начинается сначала. Канал может выйти из строя по внешним причинам, таким, как дефект кабеля, или из-за того, что один из узлов выполняет перезагрузку.

На рис. 6.22 показан реальный пакет автоматического согласования FLP.

Рис. 6.22. Пакет автоматического согласования параметров канала FLP

Пакет FLP состоит из 33-х импульсов, представляющих 16-битовое кодовое слово, которое перемежается с 17-ю импульсами синхронизации. Импульсы в пакете разделены временны*ы*ми промежутками длительностью 62,5 мс (±7 мс). Между всеми импульсами синхронизации находятся позиции для импульсов данных. Если позиция импульса данных присутствует, она интерпретируется как бинарная единица. Отсутствие импульса данных в промежутке между двумя импульсами синхронизации интерпретируется как бинарный ноль. Как показано на рис. 6.23, 17 импульсов синхронизации присутствуют всегда. 16 импульсов данных присутствуют только в том случае, если они представляют бинарную единицу, и отсутствуют, если представляют бинарный ноль в кодированном 16-битовом слове данных. Импульсы, интерпретированные как бинарные единицы данных, затенены.

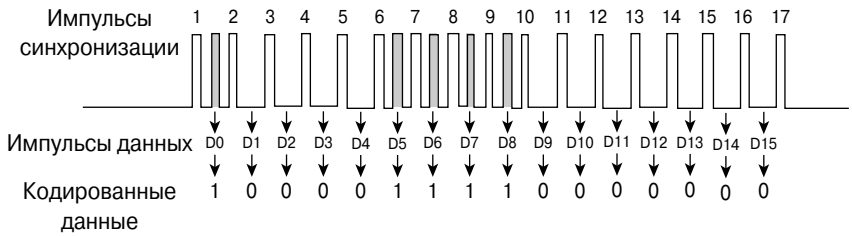


Рис. 6.23. Интерпретация импульса автоматического согласования параметров канала

После того как прошло автоматическое согласование, может быть добавлена дополнительная информация с использованием понятия страницы. Под страницами понимаются дополнительные биты, представляющие более сложные параметры канала и самого процесса согласования.

После того как устройство декодировало слово канального кода, предложенное партнером по каналу, оно подтверждает получение первичного слова путем отправки как минимум трех пакетов импульсов FLP с установленным битом подтверждения (Acknowledge). После того как оба партнера по каналу подтвердили получение слова канального кода FLP таким образом, они либо переходят к следующей странице, либо принимают обсужденную конфигурацию как окончательную и пытаются установить канал с соответствующими параметрами. Партнеры по каналу могут

послать произвольное количество дополнительных страниц после первоначальной страницы базовой конфигурации и любое количество дополнительных страниц, связанных с базовой страницей.

Установка канала и согласование дуплексного или полудуплексного режима

Партнеры по каналу имеют право пропустить процесс согласования конфигураций, которые они могут предложить, однако не имеют права включать в предложение в качестве своих конфигурации, которые они не способны поддерживать. Такой подход позволяет сетевому администратору принудительно установить на портах выбранную скорость и дуплексный режим, не отключая процесс автосогласования.

Для большинства реализаций Ethernet автоматическое согласование является необязательной опцией. Gigabit Ethernet требует использования механизма автоматического согласования, однако пользователь может его отключить. Первоначально автоматическое согласование было определено для реализаций Ethernet, использующих кабель UTP.

Когда станция, участвующая в автоматическом согласовании, в первый раз пытается установить канал, предполагается, что у нее изначально есть наборы микросхем 10BASE-T, которые используются для того, чтобы попытаться сразу установить канал (т.е. стандартно предполагается, что как минимум самая низкоскоростная технология поддерживается). Поэтому если в соединении присутствует сигнализация 10BASE-T и станция поддерживает технологию 10BASE-T, то она пытается установить канал без согласования параметров. Если с использованием сигнализации возможно установление высокоскоростного канала или получены пакеты импульсов FLP, то станция продолжает работать по другой технологии. Если же партнер по каналу не пересылает пакеты импульсов FLP, а вместо этого передает сигналы NLP, то автоматически делается вывод о том, что это устройство является станцией 10BASE-T. Во время такого первоначального периода тестирования в отношении других технологий по передающему маршруту посылаются пакеты импульсов FLP. Стандарт не позволяет параллельно пытаться обнаружить другие технологии (т.е. параметры канала устанавливаются однозначно и непротиворечиво[2]).

Если канал установлен посредством параллельного процесса согласования канала, то требуется, чтобы он был полудуплексным. Существуют только два метода установки дуплексного канала:

- посредством выполнения полной процедуры автоматического согласования;
- путем принудительной установки администратором дуплексного режима для обоих партнеров по каналу.

[2] *У некоторых недорогих концентраторов могут возникать проблемы с согласованием параметров канала; в таком случае соединение не будет функционировать должным образом, и счетчик коллизий и ошибок на интерфейсе, который подключен к концентратору, будет быстро расти. — Прим. ред.*

Если у одного из партнеров принудительно установлен дуплексный режим, а другой партер параллельно обнаруживает во время попытки автоматического согласования другое состояние, то обязательно возникнет несоответствие режимов дуплексности, что приведет к коллизиям и ошибкам в таком канале. Если на одном из концов канала принудительно установлен дуплексный режим, то он должен быть установлен и на другом конце[3]. Исключением из этого правила является лишь технология 10 Гбит/с Ethernet, которая не поддерживает полудуплексных соединений.

Многие производители реализуют свое аппаратное обеспечение таким образом, чтобы устройство последовательно проходило через различные возможные состояния (режимы). Сначала это устройство в течение некоторого времени передает пакеты импульсов FLP для автоматического согласования канала, затем конфигурирует само себя для поддержки технологии Fast Ethernet и в течение некоторого периода времени пытается создать канал, а в заключение просто прослушивает его. Некоторые производители не предусматривают никаких попыток передачи для установки канала до тех пор, пока устройство не получит пакет FLP или какую-либо иную сигнальную схему. В состоянии пассивного прослушивания портативный компьютер способен экономить энергию аккумулятора, сохраняя работоспособность, хотя такой режим не поддерживается стандартом.

Дуплексный режим в сетях Ethernet

Существуют два режима работы соединений: полудуплексный и дуплексный. В совместно используемых средах поддержка полудуплексного режима является обязательной. Все коаксиальные сети по природе своей полудуплексные и не могут работать в дуплексном режиме. Структуры, использующие кабель UTP или оптоволоконный кабель, могут работать в полудуплексном режиме, но он является административно устанавливаемым. Все реализации технологии 10 Гбит/с используют только дуплексный режим.

В полудуплексном режиме в каждый конкретный момент времени передавать может только одна станция. В коаксиальных реализациях при попытке передачи второй станцией сигналы накладываются друг на друга и стакиваются, в результате чего они искажаются. В кабеле UTP и в оптоволоконном кабеле передача обычно идет по отдельным парам, поэтому в них отсутствует возможность столкновения и искажения сигналов.

В спецификациях Ethernet установлены правила разрешения конфликтных ситуаций, возникающих в тех случаях, когда две или более станций пытаются вести передачу одновременно.

В дуплексном канале “точка-точка” обе станции имеют право в любое время вести передачу, независимо от того, передает ли данные в это же время другая станция. Автоматическое согласование позволяет избежать большинства ситуаций, в которых одна из станций канала “точка-точка” ведет передачу в полудуплексном режиме, а

[3] *Устанавливать дуплексность и скорость передачи вручную рекомендуется только в исключительных случаях. — Прим. ред.*

другая работает в дуплексном режиме. Существуют только два метода установки дуплексного соединения при скоростях ниже, чем у технологии Gigabit Ethernet:

- за счет автоматического согласования;
- за счет принудительной установки дуплексного режима администратором.

Если одна из станций ведет автоматическое согласование, а другая по каким-либо причинам в нем не участвует, то первая станция должна выбрать полудуплексный режим. Таким образом, если на одном конце канала принудительно устанавливается какой-либо режим, то обязанностью персонала, обслуживающего сеть, является установка такого же режима и на другом конце канала. В противном случае в сети будет наблюдаться искусственно завышенный уровень ошибок и пониженная производительность. Несоответствие режимов дуплексности является, вероятно, наиболее частой ошибкой в коммутируемых сетях.

Установка приоритетов

В том случае, когда партнеры по каналу имеют возможность использовать несколько общих возможных технологий, для выбора одной из предлагаемых конфигураций используется приводимый ниже список. Иными словами, в случае возможности использования версий Ethernet 10/100/1000 Мбит/с на основе медного кабеля желательно автоматически соглашаться на наилучший из имеющегося списка вариант соединения интерфейсов. В списке параметров конфигурации они расположены в порядке приоритетности, при этом в первой позиции находится конфигурация с наивысшим приоритетом (приоритет уменьшается снизу вверх):

- 100 BASE-T дуплексный режим;
- 100 BASE-T полудуплексный режим;
- 100 BASE-TX дуплексный режим;
- 100 BASE-TX полудуплексный режим;
- 10 BASE-T дуплексный режим;
- 10 BASE-T полудуплексный режим.

Оптоволоконные реализации технологии Ethernet не включены в этот список, поскольку электроника и оптика интерфейса не позволяют легко менять конфигурацию. Предполагается, что конфигурация такого интерфейса фиксирована. Если два интерфейса способны выполнять автоматическое согласование, то они уже используют одну и ту же реализацию технологии Ethernet, хотя при этом возможен выбор из нескольких конфигураций с различными вариантами режимов дуплексности и различными вариантами выбора ведущего устройства для синхронизации.

Резюме

В этой главе были рассмотрены такие ключевые вопросы:

- Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers — IEEE) является профессиональной организацией, разрабатывающей сетевые стандарты. Стандарты IEEE для локальных сетей наиболее широко известны стандартами LAN и в настоящее время общеприняты;
- Институт IEEE подразделяет канальный уровень эталонной модели OSI на два отдельных подуровня: подуровень управления доступом к передающей среде (Media Access Control — MAC) и подуровень управления логическим каналом (Logical Link Control — LLC);
- в сетях Ethernet используются MAC-адреса устройств, которые являются физическими адресами, хранящимися в сетевом адаптере NIC каждого устройства;
- разбиение данных на фреймы позволяет передавать существенную управляющую информацию, которая не может быть передана простым кодированием битовых потоков;
- двумя основными методами доступа к передающей среде являются детерминистический (передача происходит по очереди) и недетерминистический (первым передается первый поступивший фрейм);
- в сетях Ethernet используется метод множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD);
- при полудуплексном режиме (Half-duplex transmission) передача сигналов возможна в любом направлении, но не в обоих одновременно. В дуплексном режиме возможны одновременно передача данных по каналу и их прием;
- использование общей для всех устройств сети среды передачи может вызвать затор в сети, который резко снижает эффективность ее работы;
- наиболее типичной (и обычно некритической) ошибкой передачи в сетях Ethernet являются коллизии;
- основными типами ошибок передачи фреймов в сетях Ethernet, которые могут быть выявлены в сеансе работы анализатора протоколов, являются локальные, удаленные и запоздалые коллизии;
- ошибками в сетях Ethernet также считаются сбойные пакеты (jabber), удлиненные, укороченные фреймы, фреймы-карлики, ошибки контрольной суммы, ошибки выравнивания и ошибки, связанные с выходом за границы фрейма.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, которые изложены в данной главе.

Ключевые термины

IEEE (Институт инженеров по электротехнике и электронике — Institute of Electrical and Electronic Engineers) — это профессиональная организация, деятельность которой включает в себя разработку коммуникационных и сетевых стандартов. Стандарты для LAN-сетей, разработанные Институтом IEEE, в настоящее время являются преобладающими при проектировании и эксплуатации сетей.

LLC (Logical Link Control — подуровень управления логическим каналом) — это верхний из двух подуровней канального уровня, определенных в стандарте IEEE. Подуровень LLC осуществляет контроль ошибок, управление потоками, созданием фреймов и адресацией на MAC-уровне. Основным протоколом LLC является спецификация IEEE 802.2, которая описывает как вариант сети с установкой соединения, так и без него.

MAC (Media Access Control — подуровень управления доступом к передающей среде) — это нижний из двух подуровней канального уровня, определенных спецификацией IEEE. MAC-подуровень управляет доступом к передающей среде, таким, как передача маркера или конкуренция за доступ. См. также *LLC*.

MAC-адрес (MAC address) — это стандартизированный адрес канального уровня, который требуется каждому устройству, подсоединенному к сети LAN. Другие устройства сети используют этот адрес для нахождения отдельного устройства в сети, создания и обновления таблиц коммутации и структур данных. MAC-адреса имеют длину 6 байтов и назначаются Институтом IEEE. Такие адреса также называют аппаратными, адресами MAC-уровня или физическими адресами.

OUI (Organizationally Unique Identifier — уникальный идентификатор организации) представляет собой три назначаемых Институтом IEEE октета в 48-битовом блоке MAC-адреса устройства.

Возврат (backoff) — задержка повторной передачи, вызванная произошедшей коллизией.

Дуплексная передача (full duplex) — это возможность одновременной передачи данных между отправляющей и принимающей станциями в двух направлениях.

Заголовок (header) — управляющая информация, размещаемая перед модулем передачи верхнего уровня при инкапсуляции данных для передачи по сети.

Задержка распространения пакета (propagation delay) — время, требуемое данным для прохождения по сети от станции-отправителя до станции-получателя.

Инкапсуляция (encapsulation) — упаковка данных в заголовок некоторого конкретного протокола. Например, данные протоколов высокого уровня перед передачей помещаются в заголовок Ethernet. Аналогичным образом при соединении посредством мостов разнородных сетей весь фрейм из одной сети может быть помещен после заголовка, используемого протоколом канального уровня другой сети.

Концевик (trailer) — это управляющая информация, добавляемая во фрейм при инкапсуляции после данных для последующей передачи фрейма по сети.

Максимальный модуль передачи данных (Maximum Transmission Unit — MTU) — это максимальный размер пакета в байтах, который может быть обработан конкретным интерфейсом.

Множественный доступ с обнаружением коллизий (Carrier Sense Multiple Access/ Collision Detect — CSMA/CD) представляет собой механизм доступа к среде передачи, при использовании которого устройства, готовые к передаче данных, предварительно прослушивают канал для выяснения, не занят ли он. Если в течение заданного промежутка времени канал не занят, начинается передача. Если два устройства начинают передачу одновременно, происходит коллизия, которая регистрируется всеми участвующими в коллизии устройствами. Такая коллизия вызывает у устройств задержку повторной передачи в течение некоторого случайным образом выбираемого промежутка времени. Метод доступа CSMA/CD используется в сетях спецификаций Ethernet и IEEE 802.3.

Ошибка выравнивания (alignment error) фрейма происходит, когда конец сообщения не совпадает с границей октета.

Ошибка выхода за границы фрейма (range error) возникает в том случае, когда фрейм содержит разрешенное значение в поле длины фрейма (Length field), однако это значение не совпадает с количеством октетов, находящихся в поле данных (Data field) полученного фрейма.

Полудуплексная передача (half duplex) представляет собой возможность передачи данных между передающей и принимающей станциями в каждый конкретный момент времени только в одном направлении.

Протокол SNMP (Simple Network Management Protocol — простой протокол управления сетью) — протокол управления сетью, используемый, как правило, только в сетях протокола TCP/IP. Протокол SNMP предоставляет средства мониторинга и управления сетевыми устройствами, а также управления конфигурациями, сбором статистических данных, управлением производительностью сети и безопасностью в сети.

Распределенный интерфейс данных оптоволоконного канала (FDDI — Fiber Distributed Data Interface) представляет собой стандарт 3T9.5 для LAN-сетей, установленный Американским национальным Институтом стандартизации (American National Standards Institute — ANSI), определяющий сеть с передачей маркера со скоростью передачи 100 Мбит/с по оптоволоконному кабелю на расстояние до 2 км. Для обеспечения резервирования в протоколе FDDI используется структура двойного кольца.

Сбойный пакет (jabber). В стандарте 802.3 сбойный пакет несколько раз определяется как передача длительностью от 20000 до 50000 битовых интервалов. Однако большинство средств диагностики регистрирует и сообщает о сбойных пакетах каждый раз, когда обнаруживается передача блока длительностью, превышающей максимально допустимый размер фрейма, который значительно меньше 20000–50000 битовых интервалов.

Сеть Ethernet со скоростью передачи 10 Гбит/с (10-Gb Ethernet). Созданная на базе технологий, используемых в большинстве современных LAN-сетей, технология

10 Гбит/с Ethernet описывается как новая технология, предлагающая боле эффективный и менее дорогой подход к передаче данных по магистральным соединениям между отдельными сетями, оставаясь при этом цельной технологией на протяжении всего маршрута перемещения данных. В настоящее время есть возможность поднять скорость в сетях Ethernet до 10 Гбит/с.

Сеть Token Ring — это локальная сеть, в которой для управления доступом используется передача маркера. Разработана и поддерживается корпорацией IBM. Сеть Token Ring работает со скоростями от 4 до 16 Мбит/с и использует кольцевую топологию.

Симплексный режим передачи (simplex) — это режим передачи, при котором возможна передача данных от передающей станции принимающей только в одном направлении. Примером симплексной технологии может служить обычное широковещательное телевидение.

Спецификация Ethernet — базовая LAN-спецификация, созданная корпорацией Xerox и впоследствии развивавшаяся корпорациями Xerox, Intel и Digital Equipment. Сети Ethernet используют метод доступа CSMA/CD и разнообразные типы кабелей со скоростями передачи 10, 100 и 1000 Мбит/с. Стандарты Ethernet и IEEE 802.3 аналогичны.

Спецификация Gigabit Ethernet — стандарт высокоскоростных Ethernet-сетей, одобренный комитетом стандартизации IEEE 802.3z в 1996 году.

Спецификация IEEE 802.2 — протокол IEEE для локальных сетей LAN, определяющий реализацию подуровня LLC канального уровня эталонной модели OSI. Стандарт IEEE 802.2 задает методы обработки ошибок и интерфейс службы сетевого (третьего) уровня.

Спецификация IEEE 802.3 — протокол Института IEEE для LAN-сетей, определяющий реализацию MAC-подуровня канального уровня (т.е. физическую часть последнего). В спецификации IEEE 802.3 используется метод доступа CSMA/CD для набора возможных скоростей передачи данных в разнообразных физических средах. Расширения стандарта IEEE 802.3 определяют различные реализации технологии Fast Ethernet. Физические модификации первоначальной спецификации IEEE 802.3 включают в себя версии 10BASE2, 10BASE5, 10BASE-F, 10BASE-T и 10BROAD36. Физическими модификациями технологии Fast Ethernet являются 100BASE-TX и 100BASE-FX.

Технология Fast Ethernet. Этот термин используется в отношении любой из ряда Ethernet-спецификаций, которые работают со скоростью передачи данных 100 Мбит/с. Технология Fast Ethernet обеспечивает скорость передачи, в 10 раз бо́льшую, чем спецификация Ethernet 10BASE-T, сохраняя при этом такие характеристики 10BASE-T, как формат фрейма, MAC-механизмы и размер блока MTU. Эта общность механизмов позволяет использовать существующие приложения и средства управления сетью технологии 10BASE-T в сетях Fast Ethernet. Технология Fast Ethernet является расширением спецификации IEEE 802.3.

Технология передачи данных без установки соединения (connectionless) представляет собой метод передачи данных без установки виртуального канала.

Удлиненный фрейм (long frame) — фрейм, длина которого превосходит максимально допустимую, с учетом возможного добавления тега.

Фрейм-призрак (ghost). Этот термин был предложен корпорацией Fluke Networks для обозначения энергии (шума), которая обнаруживается в кабеле и выглядит подобно фрейму, однако не имеет действительного поля SFD. Для того чтобы быть квалифицированным как фрейм-призрак, такой "псевдофрейм" должен иметь длину не менее 72 октетов, в противном случае он идентифицируется как удаленная коллизия.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. Что из перечисленного ниже *не* является стандартным подуровнем спецификации IEEE?

а) Управление доступом к среде передачи (Media Access Control).

б) Управление каналом передачи данных (Data Link Control).

в) Управление логическим каналом (Logical Link Control).

г) Ничто из вышеперечисленного.

2. К каким уровням эталонной модели OSI относятся стандартные IEEE-подуровни?

а) Ко второму и третьему.

б) К первому и второму.

в) К третьему и четвертому.

г) К первому и третьему.

3. В каком процессе в качестве подуровня участвует LLC?

а) Шифрование.

б) Инкапсуляция.

в) Создание фреймов.

г) Все вышеперечисленное.

4. Что представляют первые шесть шестнадцатеричных цифр MAC-адреса?

а) Серийный номер интерфейса.

б) Уникальный идентификатор организации.

в) Уникальный идентификатор интерфейса.

г) Ничто из вышеперечисленного.

5. MAC-адреса имеют длину _____ битов.

а) 12.

б) 24.

в) 48.

г) 64.

6. Как называется метод доступа, используемый в сетях Ethernet и описывающий работу таких сетей?

а) TCP/IP.

б) CSMA/CD.

в) CMDA/CS.

г) CSMA/CA.

7. Где записан MAC-адрес?

а) В трансивере (приемопередатчике).

б) В микросхеме BIOS компьютера.

в) В сетевом адаптере (NIC).

г) В микросхеме CMOS.

8. Какое из приведенных ниже утверждений наилучшим образом описывает обмен данными между двумя устройствами сети LAN?

а) Устройство-отправитель инкапсулирует данные во фрейм вместе с MAC-адресом получателя и пересылает его. Этот фрейм виден всем устройствам LAN-сети, однако устройства, адрес которых не совпадает с адресом получателя, игнорируют его.

б) Устройство-отправитель инкапсулирует данные и помещает MAC-адрес получателя во фрейм. После этого оно направляет фрейм в сеть, где только устройство с адресом, совпадающим с адресом получателя, может просмотреть адресное поле.

в) Устройство-получатель инкапсулирует данные во фрейм вместе с MAC-адресом устройства-отправителя и направляет этот фрейм в сеть. Устройство с совпадающим с адресом удаляет такой фрейм.

г) Все устройства в локальной сети получают фрейм и передают его на обработку центральному процессору, а программное обеспечение принимает решение, удалить фрейм или обработать.

9. Какие функции связаны с созданием фреймов?

а) Идентификация компьютеров, которые вступают в связь друг с другом.

б) Сообщение о том, когда начинается и заканчивается связь между двумя компьютерами.

в) Установка флагов в поврежденных фреймах.

г) Все вышеперечисленное.

10. К чему относится термин “управление доступом к среде передачи” (Media Access Control)?

а) К состоянию, в котором адаптер NIC захватил доступ к передающей среде сети и готов к передаче.

б) К правилам доступа к передающей среде и освобождения ее.

в) К протоколам, которые определяют, какому компьютеру в среде общего доступа разрешено передавать данные.

г) К формальной битовой последовательности, которая была передана.

11. Какое из приведенных ниже описаний наилучшим образом описывает сеть CSMA/CD?

а) Переданные одним узлом данные проходят по всей сети, их получают и анализируют все остальные узлы.

б) Сигналы посылаются непосредственно получателю, если станции-отправителю известны как MAC-, так и IP-адрес.

в) Отправленные одним узлом данные направляются ближайшему маршрутизатору, который пересылает их непосредственно получателю.

г) Сигналы всегда посылаются в широковещательном режиме.

12. Когда происходят коллизии в LAN-сетях Ethernet и IEEE 802.3?

а) Когда один из узлов направляет пакет в сеть, не уведомляя об этом другие узлы.

б) Когда две станции прослушивают сеть и, не обнаружив текущей передачи, начинают передачу одновременно.

в) Когда два сетевых узла посылают пакеты узлу, который больше не ведет широковещательную передачу.

г) Когда обнаруживается флуктуация фазы сигнала и во время нормальной передачи происходит ее нарушение.

13. Что является важной функцией второго (канального) уровня?

а) Управление логическим каналом.

б) Адресация.

в) Управление доступом к передающей среде.

г) Все вышеперечисленное.

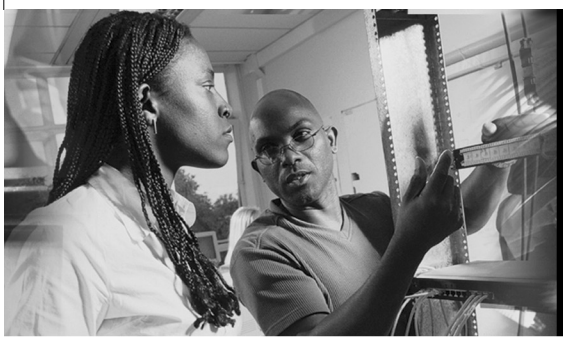
14. Какое из приведенных ниже утверждений истинно в отношении детерминистического MAC-протокола?

а) Он определяет коллизии и указывает способ их обработки.

б) Он позволяет концентратору определить количество активных в данный момент пользователей.

в) Он позволяет станциям отправлять данные "по очереди".

г) Он позволяет сетевым администраторам использовать "говорящую палочку" ("talking stick") для управления доступом к среде пользователей, которые квалифицируются как "нарушители порядка" ("troublemakers").



ГЛАВА 7

Технологии Ethernet

В этой главе...

- описаны различные Ethernet-технологии со скоростью передачи 10 Мбит/с;
- описана технология 10BASE-T;
- указан стандарт распайки разъемов 10BASE-T;
- рассмотрены принципы построения структур с использованием стандарта 10BASE-T;
- описаны разновидности Ethernet-технологии со скоростью передачи 100 Мбит/с;
- указаны три основные особенности технологии Fast Ethernet;
- рассказывается, что такое стандарт 100BASE-TX и какой UTP-кабель и почему позволил данному стандарту достичь значительного коммерческого успеха;
- описана Ethernet-технология со скоростью передачи 1000 Мбит/с;
- описаны различия между технологиями Ethernet, Fast Ethernet и Gigabit Ethernet;
- описана технология 10BASE5;
- описана технология 10BASE2;
- описана технология 10BASE2;
- описана технология 10BASE-FX;
- описана структура Fast Ethernet и указаны ограничения на длину кабеля;
- описаны технологии 1000BASE-SX и 1000BASE-LX;
- рассмотрена технология 100BASE-T и причины ее создания;
- описан принцип построения структур Gigabit Ethernet;
- высказаны предположения о дальнейшей эволюции стандартов Ethernet;
- описана технология Ethernet со скоростью передачи 10 Гбит/с и ее принципиальные отличия от других технологий;
- описан принцип построения структур Ethernet со скоростью передачи данных 10 Гбит/с.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

алгоритм без возврата к нулю, с. 359,
манчестерское кодирование, с. 360,
кодирование, с. 360,
толстый коаксиал, с. 361,

thicknet, с. 361,
тонкий коаксиал, с. 363,
thinnet, с. 363,
стандарт 100BASE-TX, с. 370,
стандарт 100BASE-FX, с. 370,
сигнал-шум, с. 370,
принцип четырехмерного пятиуровневого модулирования амплитуды импульса, с. 382,
кодирование с инверсией без возврата к нулю, с. 372,
стандарты 1000BASE-T, 1000BASE-SX, с. 381,
стандарт 1000BASE-LX, с. 381,
кодирование 8b1q4, с. 382,
мультиплексирование со спектральным уплотнением сигнала, с. 392.

Технология Ethernet и связанные с ней протоколы группы IEEE 802.3 являются одними из самых важных сетевых стандартов в мире. Благодаря большому успеху исходной технологии Ethernet, а также надежности ее реализации, она продолжает активно развиваться. Такое развитие происходит в результате возросших потребностей современных локальных вычислительных сетей. Вероятнее всего, развитие технологии на основе сетей Ethernet продолжится и в будущем, чтобы удовлетворить потребности сетей завтрашнего дня.

В предыдущей главе мы кратко рассказали об истории создания технологии Ethernet и соответствующих стандартах. Мы также упомянули, что под названием *Ethernet* обычно подразумевается целое семейство Ethernet-технологий. В этой главе мы исследуем группу технологий Ethernet более детально.

В этой главе дано введение в технологии коммутации и установления мостового соединения второго уровня, которые позволяют уменьшить перегрузки в локальных сетях посредством уменьшения трафика и увеличения пропускной способности.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Технологии Ethernet со скоростью передачи данных 10 и 100 Мбит/с

Этот раздел посвящен особенностям наиболее важных разновидностей технологии Ethernet. Изложенный ниже материал предназначен не для запоминания, а скорее для формирования у читателя понимания того, какие характеристики являются общими для всех разновидностей технологии Ethernet, а также преимуществ и недостатков, присущих основным коммерческим реализациям технологии Ethernet.

Популярность технологии Ethernet началась с использованием толстого коаксиального кабеля в стандарте 10BASE5. Однако инсталляция толстого коаксиального кабеля была достаточно сложной задачей. В стандарте 10BASE2 использовался *тонкий коаксиальный кабель*, он был проще в установке и терминировании; однако максимальная длина сегмента сети сократилась с 500 до 185 метров. Большим шагом вперед в уже наметившемся направлении сокращения затрат на монтаж и уменьшения общей стоимости стало появление стандарта 10BASE-T. Расстояние, которое мог преодолевать сигнал, сократилось до 100 метров, что привело к появлению таких устройств, как повторители (repeaters) и многопортовые концентраторы (hubs). Использование повторителей позволило увеличить диаметр сетей стандарта 10BASE-T вплоть до 500 метров. С увеличением размеров рабочих групп и сложности используемых приложений пропускная способность совместно используемого концентратора становилась узким местом в сети. Появление коммутаторов стандарта 10BASE-T позволило снять ограничения, связанные с пропускной способностью концентраторов и общей длиной сети, — соединения типа "станция-станция" преобразовались теперь в соединения "точка-точка".

Мощь, разносторонность и экономическая эффективность стандарта 10BASE-T привела к взрывному росту количества пользователей локальных сетей и пользователей сети Internet (что также увеличило трафик в локальных сетях) и усложнению используемых приложений. В ответ на потребность в сетях с высокой пропускной способностью была разработана технология Fast Ethernet. Версия Fast Ethernet для медного кабеля 100BASE-TX стала наиболее коммерчески популярной и успешной технологией локальных сетей. Вместе с ней появилось достаточно много блестящих разработок для обеспечения совместимости данной технологии со стандартом 10BASE-T (например, совмещение интерфейсов со скоростями 10 и 100 Мбит/с). В качестве конкурента для технологии магистральных каналов локальных сетей FDDI (Fiber Distributed Data Interface — распределенный интерфейс передачи данных по волоконно-оптическим каналам) была предложена технология Ethernet стандарта 100BASE-FX на основе оптического кабеля. Во всех указанных технологиях Ethernet используется концепция MAC-адресов, один и тот же формат фрейма и метод множественного доступа с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection — CSMA/CD).

10-мегабитовые технологии Ethernet

На рис. 7.1 показаны различные реализации интерфейсов физического уровня, которые поддерживаются в технологии Ethernet. Спецификации *10BASE5*, *10BASE2* и *10BASE-T* во всех последующих разделах будут рассматриваться как устаревшие.

Четыре характеристики являются общими для традиционных спецификаций Ethernet:

- параметры синхронизации;
- формат фрейма;
- процесс передачи;
- базовые принципы построения.

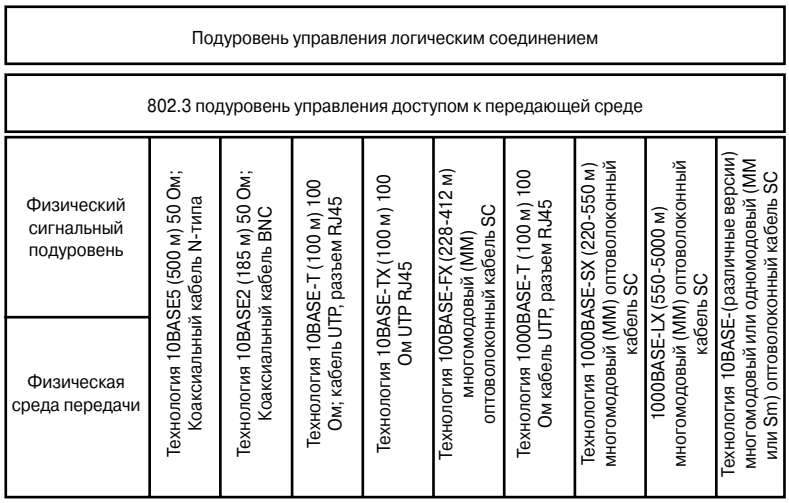


Рис. 7.1. Различные технологии на основе Ethernet

После изучения общих для всех трех исторически важных версий Ethernet характеристик мы подробно рассмотрим каждую из них.

Как показано в табл. 7.1, спецификации 10BASE2, 10BASE5 и 10BASE-T используют одни и те же временные параметры. Следует отметить, что время передачи одного бита (битовый интервал — bit-time) для скорости 10 Мбит/с равен 100 наносекундам (нс), или 0,1 миллисекундам (мс), или 1 десятимиллионной секунды.

Таблица 7.1. Параметры технологии Ethernet со скоростью передачи 10 Мбит/с

Параметр	Значение
Время передачи бита	100 нс
Канальный интервал	512 битовых интервалов
Интервал между фреймами	96 битов[1]
Количество коллизионных попыток	16
Предельный интервал ожидания в конфликтной ситуации	10
Размер коллизионного jam-пакета	32 бита
максимальный размер фрейма без метки	1518 октетов
Минимальная длина фрейма	512 битов (64 октета)

Спецификации 10BASE2, 10BASE5 и 10BASE-T используют единый формат фрейма. На рис. 7.2 показан Ethernet-фрейм, который используется на MAC-подуровне.

[1] *Официальное значение параметра, согласно стандарту. — Прим. ред.*

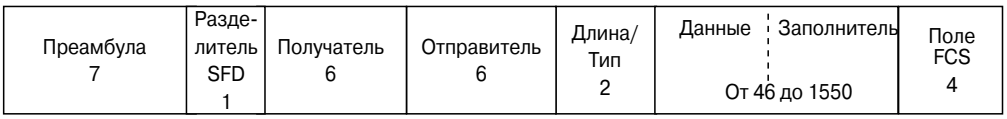


Рис. 7.2. Ethernet-фрейм

Процесс передачи данных для традиционных спецификаций Ethernet одинаков вплоть до нижней части физического уровня эталонной модели OSI. По мере продвижения фрейма от MAC-подуровня к физическому уровню выполняются дополнительные процессы, прежде чем биты окажутся в среде передачи физического уровня. Одним из наиболее важных процессов на этой стадии является проверка параметра нарушения качества сигнала (Signal Quality Error — SQE). Подход, подобный этому, используется во многих сетевых технологиях. На физическом уровне сети постоянно происходят взаимодействия, не связанные с передачей пользовательских данных, которые необходимы для проверки работоспособности сети. Механизм SQE всегда используется в полудуплексном режиме; допускается его работа в дуплексном режиме, но это не является обязательным. Механизм SQE используется в следующих ситуациях:

- через 4-8 микросекунд после обычной передачи для указания того, что исходящий фрейм успешно доставлен;
- при возникновении коллизий;
- при появлении *дефектного сигнала* в среде передачи; в качестве дефектных сигналов могут выступать обнаруженный сбойный фрейм или отражение сигнала, возникшее вследствие проблем с кабелем, например, из-за замыкания (для различных сред передачи требуется выполнение разных условий);
- в случае, если передача была прервана по причине сбоя, вызванного передачей сверх положенного времени.

ВНИМАНИЕ!

В кодировании по алгоритму NRZ (без возврата к нулю) поддерживается постоянный уровень сигналов без изменений (возврата к уровню 0 Вольт) внутри битового интервала.

Все варианты структур Ethernet со скоростью передачи данных 10 Мбит/с выполняют над октетами, полученными от MAC-подуровня, процедуру, называемую кодированием сигнала в линии (line-encoding). Кодирование в линии описывается алгоритмом преобразования битов в электрические сигналы, передающиеся по проводам. Простейшие варианты *кодирования*, такие, как *алгоритм без возврата к нулю* (*nonreturn to zero* — NRZ), в которых единичному биту соответствуют 5 Вольт, а нулевому — 0 Вольт, обычно имеют неудовлетворительные временные и электрические характеристики. По этой причине были разработаны алгоритмы кодирования, обладающие необходимыми параметрами и подходящие для любых сред передачи. В системах со скоростью передачи 10 Мбит/с применяется алгоритм под названием

манчестерское кодирование (manchester encoding). На рис. 7.3 проиллюстрирован принцип манчестерского кодирования: по оси Y измеряется напряжение в вольтах, по оси X — время.

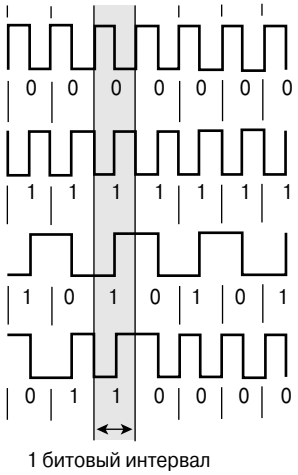


Рис. 7.3. Пример манчестерского кодирования

Манчестерское кодирование основано на методике определения двоичного числа по направлению изменения напряжения в середине битового интервала. В примере, проиллюстрированном рис. 7.3, временной интервал, необходимый для передачи одного бита, обозначен вертикальным выделением для всех четырех исследуемых волновых форм. Изменение положительного значения напряжения на отрицательное в середине битового интервала для верхней из показанных волновых форм интерпретируется как двоичное число 0.

Для второй волновой формы (второй график сверху), напротив, внутри битового интервала имеется переход от отрицательного значения к положительному, что соответствует двоичному числу 1.

В отличие от первых двух примеров, в которых волновая форма задает последовательности одинаковых двоичных чисел (0 — в первом случае и 1 — во втором), третий пример показывает волновую форму для последовательности из чередующихся двоичных чисел. В первых двух примерах сигнал обязан возвращаться в исходное значение в пределах каждого периода, чтобы внутри каждого битового интервала изменение сигнала было одинаковым. При кодировании разных, идущих друг за другом, двоичных значений нет необходимости возвращать уровень сигнала к его предыдущему значению, чтобы создать необходимое изменение уровня сигнала в середине битового интервала. Четвертая волновая форма иллюстрирует сигнал, кодирующий последовательность различных двоичных чисел.

Устаревшая технология Ethernet имеет ряд общих структурных особенностей. Все версии ее называют *разделяемой средой Ethernet (shared Ethernet)*, поскольку в них используется общий домен коллизий. В Ethernet-сетях допустимо и является обычной

практикой использование разных сред передачи (10BASE2, 10BASE5, 10BASE-T и т.д.). Вопросы совместимости и методов взаимодействия различных версий не входят в стандарт, поэтому при внедрении сетей со смешанными средами передачи следует особое внимание уделять общим структурным принципам построения конкретной реализации или версии технологии. По мере роста и усложнения сети возрастает вероятность превышения допустимых значений задержек в сети. Временны*е* ограничения зависят от следующих параметров:

- длины кабеля и запаздывания сигнала;
- задержек в повторителях;
- задержек в трансиверах (включая сетевые адаптеры, концентраторы и коммутаторы);
- уменьшения межфреймового интервала;
- задержек внутри сетевых станций.

Дополнительная информация: правило 5-4-3

Для технологии Ethernet со скоростью передачи данных 10 Мбит/с существуют временны*е* ограничения, которые не позволяют использовать более 5 сегментов в сети. Такие сегменты могут быть разделены не более, чем четырьмя повторителями. Это означает, что две удаленные станции могут быть соединены не более, чем четырьмя последовательными повторителями. В сетях, которые построены на коаксиальном кабеле, есть дополнительное ограничение, которое запрещает использование более трех непустых сегментов между любыми двумя удаленными станциями. Допустимо использование оставшихся двух сегментов для расширения диаметра домена коллизий; такие сегменты называются связующими (link segments). Основная особенность связующих сегментов заключается в том, что они используются для подключения с их помощью только двух устройств. Все соединения на основе витой пары, такие, как 10BASE-T, удовлетворяют определению связующего сегмента.

Технология 10BASE5

В первой реализации технологии Ethernet 10BASE5 (в 1980 году) данные передавались со скоростью 10 Мбит/с по единой шине из толстого коаксиального кабеля, за что технология и получила название *толстый коаксиал*, или *Thicknet*. Стандарт 10BASE5 важен по исторической причине: он описывал первую среду передачи данных, использовавшуюся в технологии Ethernet. На сегодняшний день такой кабель можно найти только в старых и давно существующих сетях. В современных телекоммуникационных структурах эта технология используется редко, поскольку ее главное преимущество — большая длина сегмента — может быть достигнута другими средствами. Хотя сеть 10BASE5 и недорогая, не требующая конфигурирования технология (нет необходимости в использовании концентраторов для увеличения длины системы), ее базовые компоненты, такие, как сетевые адаптеры, сегодня очень редко можно встретить в продаже; сама технология в целом очень чувствительна к отражениям сигнала внутри кабеля. Кроме всего прочего, сети на основе технологии 10BASE5 сильно зависят от состояния кабеля по всей длине коллизионного домена, и кабель является единой точкой отказа.

Временные характеристики, формат фрейма и процесс передачи данных, которые рассмотрены в главе 6, “Основы технологии Ethernet”, являются общими для всех устаревших реализаций технологии Ethernet со скоростью 10 Мбит/с.

В среде 10BASE5 используется манчестерское кодирование сигнала для толстого коаксиального кабеля. На рис. 7.4 показан сигнал в технологии 10BASE5, он изменяется в диапазоне примерно от 0 до -1 Вольт. Потенциально возможна ситуация, в которой среда 10BASE5 простаивает (состояние 0 Вольт) по нескольку дней, если ни одна из станций не инициирует передачу информации.

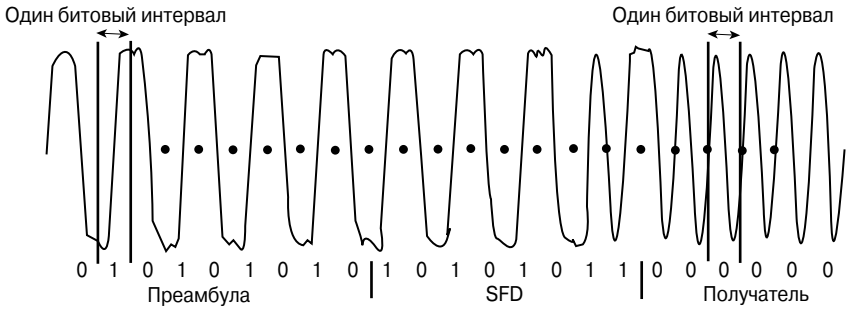


Рис. 7.4. Декодированный сигнал 10BASE5

На рис. 7.4 нанесены временные отметки, которые помогут определить временные интервалы, по которым происходит декодирование двоичных данных. Здесь по оси X измеряется напряжение, а по оси Y — время; напряжение измеряется между центральным проводом и оплеткой коаксиального кабеля.

На рис. 7.5 показано, что толстый коаксиальный кабель 10BASE5 имеет сплошной центральный провод с минимальной нормированной номинальной скоростью передачи данных (Nominal Velocity of Propagation — NVP) 0,77 и значением импеданса (полного внутреннего сопротивления) 50 Ом. Для подключения к кабелю используются N-образные соединители с резьбой. Каждый из пяти возможных сегментов толстого коаксиального кабеля может иметь длину до 500 метров[2]. Каждая станция подключается к трансиверу через AUI-кабель (Attachment Unit Interface — AUI, интерфейс подключаемых сетевых устройств), который может иметь длину до 50 метров. Кабель тяжелый, громоздкий и неудобен в монтаже, однако благодаря большим допустимым расстояниям он долгое время использовался для отдельных приложений.

ВНИМАНИЕ!

Номинальной скоростью передачи данных называется скорость распространения электрического сигнала в кабеле, нормированная на скорость распространения электромагнитных волн (или света) в вакууме. Она обычно записывается в виде процентов и лежит в диапазоне от 70% до 75%.

[2] *1640 футов. — Прим. ред.*

Рис. 7.5. Толстый коаксиальный кабель 10BASE5

Спецификации и ограничения кабеля 10BASE5 включают в себя следующие моменты:

- только одна станция может передавать данные в определенный момент времени (в противном случае возникнет коллизия);
- среда и устройства 10BASE5 могут работать только в полудуплексном режиме;
- в каждом сегменте 10BASE5 могут существовать не более 100 станций, включая повторители.

Практическое задание 7.1.2. Декодирование волновой формы
Целью этого задания является обобщение знаний о сетевых средах передачи данных, первом, втором и третьем уровнях модели OSI и технологии Ethernet посредством декодирования цифровой волновой формы Ethernet-фрейма.

Технология 10BASE2

В 1985 году был предложен стандарт 10BASE2 (изначально 802.3a-1985), в котором использовался более легкий, меньший по размеру кабель, что значительно упрощало его монтаж по сравнению со стандартом 10BASE5. Поскольку в этом стандарте используется тонкий коаксиальный кабель, его часто называют *Thinnet.* Технологию 10BASE2 все еще можно встретить в старых сетях. Несмотря на то что сегодня существует не так уж много аргументов в пользу использования сетей 10BASE2, низкая стоимость кабеля и отсутствие необходимости использовать концентраторы, несомненно, привлекательны. По существу сеть 10BASE2 не требует настройки, но приобрести сетевые адаптеры будет так же непросто, как и в предыдущем случае. Так же, как и с сетями 10BASE5, системы 10BASE2 зависят от состояния кабеля вдоль всей длины коллизионного домена и являются единой точкой отказа.

Временны*е* характеристики, формат фрейма и процесс передачи, которые были рассмотрены в главе 6, “Основы технологии Ethernet”, являются общими для всех устаревших реализаций технологий Ethernet со скоростью передачи данных 10 Мбит/с.

В технологии 10BASE2 используется манчестерское кодирование сигнала в тонком коаксиальном кабеле. Сигнал в стандарте 10BASE2 изменяется от 0 до -1 Вольт (ось Y используется для измерения напряжения, а ось X — для времени; разность потенциалов измеряется между центральным проводником и экранирующей оплеткой). Среда 10BASE2 может находиться в состоянии простоя (0 Вольт) в течение нескольких дней, если ни одна из станций не передает данные. В технологии 10BASE2 используется асинхронный режим передачи данных.

Компьютеры в локальной сети, которая построена на основе описываемой технологии, соединены в виде цепочки последовательными неразрывными отрезками коаксиального кабеля. Такие отрезки-сегменты соединены при помощи BNC-соединителей (British Naval Connector — BNC) и подключаются к Т-образным разъемам на сетевых адаптерах, как показано на рис. 7.6. Коаксиальный кабель используется как общая шина для всей сети. Существующие рабочие станции могут быть легко перемещены и подключены в новом месте, не менее легко могут быть подключены к локальной сети и новые станции. Во всем остальном технология 10BASE2 использует тот же полудуплексный протокол стандарта Ethernet.

На рис. 7.6 показано, что тонкий коаксиальный кабель имеет скрученный центральный провод (при покупке кабеля следует убедиться, что он имеет именно такой центральный провод, который скручен из нескольких проводников; установка кабеля с цельным центральным проводом может вызывать определенные трудности). Кабель имеет минимальное значение скорости прохождения порядка 0,65, импеданс (или полное внутреннее сопротивление 50 Ом) и рассчитан на использование Т-образных соединений BNC-типа. Каждый из разрешенных пяти сегментов на основе тонкого коаксиального кабеля может иметь длину до 185 м[3], и каждая рабочая станция подключается непосредственно к Т-образному BNC-соединителю, врезанному в кабель.

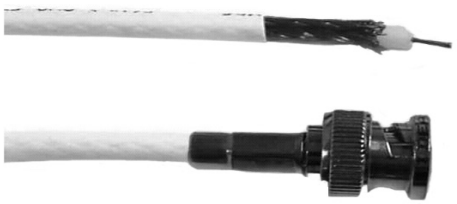


Рис. 7.6. Тонкий коаксиальный кабель и BNC-соединитель

Технология 10BASE-T

С появлением стандарта 10BASE-T (изначально 802.3i-1990) коаксиальный кабель был заменен более дешевым и простым в монтаже кабелем UTP (Unshielded Twisted Pair — неэкранированная витая пара). Этот кабель подключался к центральному устройству, концентратору или коммутатору, который является общей сетевой шиной. Тип кабеля, используемый в стандарте 10BASE-T, допустимые расстояния между концентратором и станциями, способ монтажа, коммутации и тестирования UTP-кабелей были стандартизированы в спецификациях на структурированные кабельные системы, благодаря чему были подробно описаны физические топологии, например, звездообразная. Изначально в стандарте 10BASE-T использовался полудуплексный метод передачи, однако впоследствии была добавлена дуплексная связь. Взрывоподобный рост популярности сетей Ethernet, когда данная

[3] *600 футов. — Прим. ред.*

технология стала доминирующей в локальных сетях, приходится на 1990 год и связан с использованием стандарта 10BASE-T и UTP-кабеля категории 5. Подробнее о сетевых топологиях и средах передачи данных рассказывается в главе 2, "Основы сетевых технологий", и главе 3, "Сетевая среда передачи данных".

Временны*е* характеристики, формат фрейма и процесс передачи, которые были описаны выше, применимы и в этой технологии.

В технологии 10BASE-T также используется манчестерское кодирование сигнала для кабеля UTP-типа категории 3 (в современных сетях — 5, 5e или выше).

Технология Ethernet со скоростью передачи данных 10 Мбит/с использует асинхронный режим передачи, и кабель также часто бывает не задействован в течение длительных промежутков времени, когда не происходит передача данных. В стандарте 10BASE-T каждые 125 миллисекунд (восемь раз в секунду) передаются *канальные импульсы (link pulse*), а в остальное время кабель может быть не задействован. Таким образом, сеть 10BASE-T заполнена импульсами соединения.

Каждый провод кабеля типа неэкранированная витая пара (UTP) стандарта 10BASE-T, максимальная длина которого не может превышать 90 метров, состоит из цельного проводника, диаметр которого должен находиться в пределах от 0,4 мм до 0,6 мм (от 26 до 22 AWG (American Wire Gauge — американская система оценки проводов)). В качестве соединительного кабеля, максимальная длина которого не должна превышать 10 м, используется перекрестный кабель с теми же характеристиками, но более гибкий, поскольку он часто подвергается нагрузкам и изгибается. Соответствующие кабели имеют значение NVP, равное 0,585, импеданс 100 Ом и снабжаются восьмиконтактными разъемами RJ-45, которые описаны в стандарте ISO/IEC 8877. Длина кабеля между станциями и концентратором обычно находится в диапазоне от 0 до 100 метров (от 0 до 328 футов), хотя точное значение для максимальной длины определяется величиной задержки сигнала в сегменте (любая длина кабеля, при которой задержка не превышает 1000 нс, считается допустимой и зависит от используемого оборудования). В большинстве случаев многопарный UTP-кабель с диаметром проводника 0,5 мм (24 AWG) соответствует требованиям к максимальному расстоянию до 100 м.

Несмотря на то что кабель категории 3 подходит для использования в сетях стандарта 10BASE-T, сегодня настоятельно рекомендуется при монтаже новых сетей использовать кабель категории 5e или выше. Также рекомендуется придерживаться стандартов T568A или T568B при разводке проводов и запрессовке разъемов. Такая практика монтажа позволит использовать одну и ту же среду передачи для работы разных протоколов канального доступа (включая 1000BASE-T) без замены кабельного хозяйства.

В табл. 7.2 показана схема расположения выводов соединения стандарта 10BASE-T. Обратите внимание, что для передачи и приема используются разные провода (в коаксиальном кабеле есть только один провод).

На рис. 7.7 показана принципиальная и физическая схема прямого соединения двух станций. Для такой схемы требуется так называемый перекрестный кабель (crossover cable), в котором Tx-сигнал станции А передается на Rx станции Б. Таким образом реализуются 2 соединения (TxA на RxБ и TxБ на RxA).

Таблица 7.2. Расположение контактов стандарта 10BASE-T

Номер контакта	Сигнал
1	TD+. Передача данных, положительный дифференциальный сигнал
2	TD-. Передача данных, отрицательный дифференциальный сигнал
3	RD+. Прием данных, положительный дифференциальный сигнал
4	Не используется
5	Не используется
6	RD-. Прием данных, отрицательный дифференциальный сигнал
7	Не используется
8	Не используется

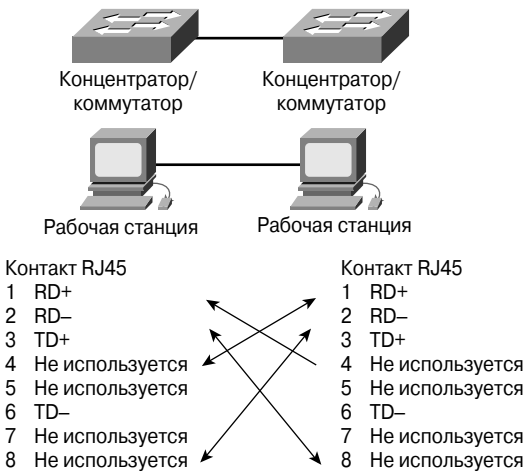


Рис. 7.7. Соединение двух станций напрямую в стандарте 10BASE-T

На рис. 7.8 показано соединение между станциями и повторителями, многопортовыми повторителями (концентраторами) или коммутаторами. Такое же соединение может быть использовано между маршрутизатором и концентратором или коммутатором. В этих случаях используется прямой кабель. Следует обратить внимание, что внутри концентраторов реализована та же шинная топология, являющаяся доменом коллизий. При подключении рабочей станции к коммутатору при помощи прямого кабеля каждое соединение является двухточечным. Внутреннее устройство коммутатора позволяет использовать полную пропускную способность одновременно для каждой пары проводов или портов коммутатора без коллизий.

Поскольку при соединении двух станций, коммутаторов или станции с коммутатором используются связи типа “точка-точка”, во всех этих случаях имеются два физически разделенных канала передачи по двум парам UTP-кабеля. В данном случае коллизии являются не физическим событием, а скорее логическим решением не

допускать одновременное использование сигналов Tx и Rx. Таким образом, для разработчика сети существует выбор между полудуплексной (с административными ограничениями, обусловленными природой алгоритма CSMA/CD) и дуплексной (без физических коллизий) конфигурациями. В большинстве случаев используется дуплексный режим, при котором не только отсутствуют коллизии, но и удваивается пропускная способность соединения. Когда соответствующий стандарт был впервые предложен IEEE, он носил название 802.3x-1997 Full-Duplex. Однако в случае соединения станции с концентратором, создающим домен коллизий, возможно использование только полудуплексного режима, где все соединения подчиняются правилам доступа к среде алгоритма CSMA/CD.

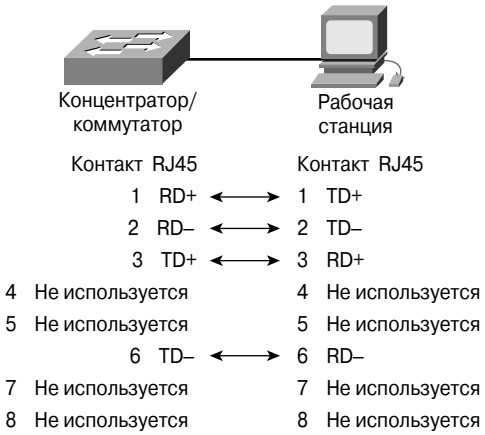


Рис. 7.8. Соединение с помощью прямого кабеля в стандарте 10BASE-T

Технология 10BASE-T поддерживает скорость передачи данных 10 Мбит/с в полудуплексном режиме, однако в дуплексном режиме скорость передачи трафика может достигать 20 Мбит/с (хотя часть пропускной способности используется на передачу служебных, а не пользовательских данных). Использование такой концепции стало необходимым для увеличения скорости передачи данных в Ethernet-сетях.

Принципы построения сетей 10BASE-T

Обычно линия связи 10BASE-T представляет собой соединение между рабочей станцией и концентратором или коммутатором. Концентраторы следует рассматривать как многопортовые повторители и учитывать существующие ограничения на количество повторителей между двумя удаленными станциями. Коммутаторы по своему принципу работы соответствуют многопортовым мостам, и при их использовании существует только ограничение по длине линии связи, которая не должна превышать 100 м. Ограничений на допустимое количество коммутаторов между удаленными станциями нет.

Несмотря на то что концентраторы могут объединяться в стек (этот процесс иногда называют каскадированием, или последовательным соединением), следует по возможности избегать этого, чтобы не выйти за пределы допустимых значений задержки сигнала между удаленными станциями. Физические размеры сетей 10BASE-T в вопросе о допустимом количестве повторителей подчиняются тем же правилам, что и сети стандартов 10BASE2 10BASE5. Если для подключения станций требуются несколько концентраторов, лучше организовать их в иерархическом порядке, сформировав древовидную структуру, нежели последовательной цепочкой. Чем меньше повторителей разделяют станции, тем выше производительность сети. С помощью объединяемых в стек концентраторов или концентраторов с высокопроизводительной внутренней шиной (backplane) можно подключить большое количество станций; при этом весь стек будет рассматриваться как единое устройство, один концентратор. Не существует ограничений на количество объединяемых в последовательные цепочки (daisy-chaining) концентраторов.

Теоретически между станциями допустимы любые расстояния, однако не следует забывать об одном важном структурном ограничении. Вне зависимости от структурных особенностей построения сети и задействованных сред передачи, одним из основных требований является сведение к минимуму задержек между удаленными станциями. Чем меньше максимальное значение задержки, тем выше общая производительность сети. Рассмотрим две распространенные схемы построения сетей.

На рис. 7.9 показаны пять сегментов и четыре повторителя между станцией 1 и любыми другими станциями. Для соединения типа 10BASE-T правило о недопустимости использования более трех заполненных станциями сегментов не применимо, поскольку нет станций, одновременно использующих один и тот же кабель. Все соединения можно рассматривать как связующие сегменты.

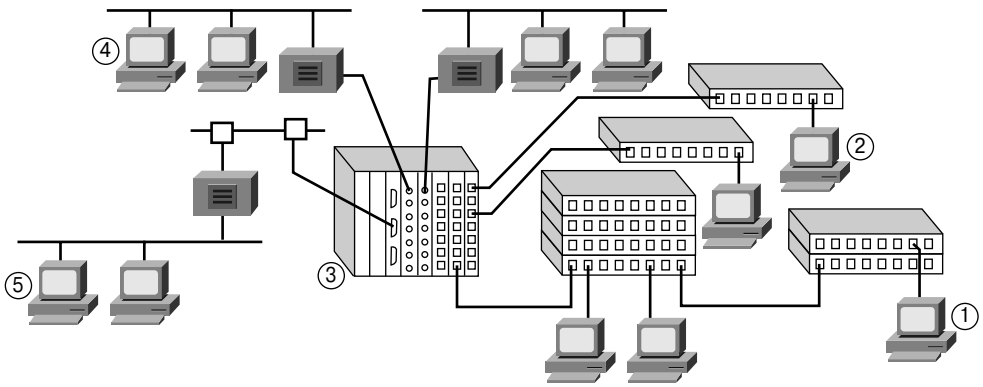


Рис. 7.9. Пример смешанной сетевой структуры со скоростью передачи данных 10 Мбит/с

В схеме на рис. 7.10 между любой из станций (за исключением станции 1) присутствует не более 3-х повторителей. Поскольку для разных маршрутов используются соединения 10BASE2 и 10BASE5, вступают в силу дополнительные ограничения (такие, как правило о трех заполненных сегментах).

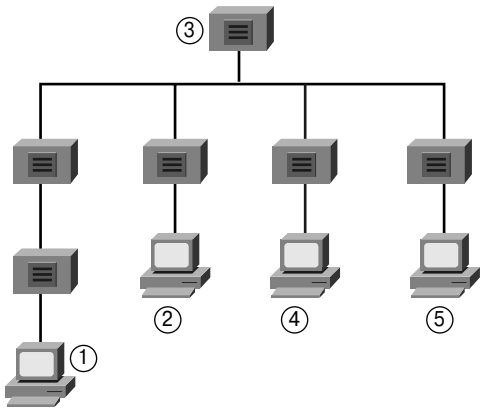


Рис. 7.10. Альтернативный пример смешанной сетевой структуры со скоростью передачи данных 10 Мбит/с

В соединениях стандарта 10BASE-T можно создавать сегменты длиной до 100 м без повторителей. На первый взгляд это расстояние может показаться большим, но на практике при монтаже сети в реальных зданиях его не всегда достаточно. Концентраторы могут помочь при решении этой проблемы, однако следует помнить об ограничении в четыре последовательных устройства, которое связано с временными параметрами. Широкое распространение коммутаторов сделало указанные ограничения менее принципиальными. Если рабочая станция подключена к коммутатору на расстоянии 100 метров, следующее соединение длиной 100 метров может быть использовано для подключения к следующему коммутатору, и т.д. Поскольку большинство современных сетей 10BASE-T являются коммутируемыми, то такое ограничение относится только к расстояниям между устройствами, но не к максимальной длине сегмента сети. В рассматриваемом стандарте допустимо использование топологий типа “кольцо”, “звезда” и “расширенная звезда”. Наиболее часто возникают проблемы, связанные с логической топологией и потоками данных, но не временными параметрами или ограничениями по расстоянию.

Таблица 7.3. Характеристики соединений стандарта 10BASE-T

Соединение	Максимальный размер сегмента
Станция-станция, станция-коммутатор, коммутатор-коммутатор	100 м без ограничений на количество последовательных соединений
Станция-концентратор	100 м, ограничения согласно правилу о 4-х концентраторах

Технология Ethernet со скоростью передачи 100 Мбит/с

Технология Ethernet со скоростью передачи 100 Мбит/с, также известная как Fast Ethernet (быстрая технология по сравнению с оригинальной технологией Ethernet со скоростью передачи данных 10 Мбит/с), включает в себя целую серию

технологий. Двумя наиболее успешными коммерческими реализациями идеи такой технологии стали стандарты *100BASE-TX* (на основе медного UTP-кабеля) и *100BASE-FX* (на основе многомодового оптического волокна). В текущем разделе рассмотрены сходства и различия обеих технологий.

Общими для технологий 100BASE-TX и 100BASE-FX являются:

- временны*е* параметры;
- формат фрейма;
- некоторые этапы процесса передачи данных.

В табл. 7.4 перечислены рабочие параметры технологии Ethernet, которая работает на скорости 100 Мбит/с.

Таблица 7.4. Параметры работы 100 Мбит/с технологии Ethernet

Параметр	Значение
Время передачи одного бита (битовый интервал)	10 нс
Канальный интервал	512
Интервал между фреймами	96 битов
Количество коллизионных попыток	16
Интервал ожидания при коллизии	10
Размер jam-пакета коллизии	32 бита
Максимальный размер фрейма	1518 октетов
Минимальный размер фрейма	512 битов (64 октета)

Технологии 100BASE-TX и 100BASE-FX используют одинаковые временные параметры. Следует отметить, что один битовый интервал в технологии Ethernet со скоростью 100 Мбит/с составляет 10 нс, что равно 0,01 мкс, или одной стомиллионной секунды. Формат фрейма для скорости передачи данных 100 Мбит/с полностью совпадает с форматом технологии 10 Мбит/с.

Благодаря появлению Fast Ethernet скорость передачи данных увеличилась в 10 раз. В результате появились новые требования. Время, необходимое для передачи одного бита, уменьшилось, при этом возросла частота передачи. Необходимо тщательно выдерживать временные параметры; требуются частоты, близкие к предельным значениям для используемых сред передачи. Это в итоге привело к большей чувствительности к помехам. Для решения возникших проблем, связанных с синхронизацией, пропускной способностью и соотношением *сигнал-шум (Signal-to-Noise Ratio — SNR*) в сетях со скоростью 100 Мбит/с, используются два раздельных этапа кодирования сигнала. Основная идея состоит в использовании систем кодирования, спроектированных для получения необходимых характеристик сигналов, их эффективной передачи по сети, включая вопросы синхронизации, эффективного использования полосы пропускания и улучшенного соотношения сигнал-шум. Первая часть процесса кодирования называется механизмом 4 бита/5 битов (4bit/5bit —

4B/5B), вторая часть — это фактическое кодирование сигнала со всеми его особенностями для передачи по медному проводу и оптическому волокну.

Оба рассматриваемых в этой главе стандарта Ethernet, которые работают со скоростью 100 Мбит/с, 100BASE-TX и 100BASE-FX, кодируют полубайты (четырехбитовые группы), полученные из MAC-подуровня. Четырехбитовые комбинации преобразовываются в пятибитовые символы; символы несут в себе контрольную информацию (такую, как начало фрейма или флаг состояния "среда не занята"). Полный фрейм, предназначенный для передачи, содержит контрольные символы и символы данных (групповой код данных). Такое дополнительное усложнение нужно для того, чтобы достичь десятикратного увеличения скорости передачи.

После применения 4B/5B-кодирования биты (в форме групповых кодов) необходимо передать через среду передачи (что предполагает применение линейного кодирования). Использование алгоритма кодирования 4-х битов в 5 означает, что за один и тот же интервал времени требуется передать 125 Мбит вместо ста. Эта особенность накладывает дополнительные строгие требования к качеству среды передачи, передатчиков и приемников. В периоды времени, когда нет данных для передачи, передаются группы битов "заполнения" для заполнения пустых периодов и поддержки синхронизации. В этом и состоит основное отличие способа обработки данных для разных сред передачи: медного провода в стандарте 100BASE-TX и оптического волокна стандарта 100BASE-FX.

Технология 100BASE-TX

Потребность в сетях с большей скоростью передачи данных привела в 1995 году к появлению технологии 100BASE-T Fast Ethernet и стандарта автоматического определения скорости (изначально 802.3u-1995). Благодаря технологии 100BASE-T скорость передачи в сетях Ethernet увеличилась до 100 Мбит/с. Стандарт 100BASE-TX, являющийся модификацией 100BASE-T для кабеля UTP-типа категории 5, имел и имеет несомненный коммерческий успех. Вскоре появились двухскоростные концентраторы и коммутаторы 10/100, позволяющие организовывать одновременную передачу данных в сетях Ethernet как на базовой скорости 10 Мбит/с, так и на скорости 100 Мбит/с.

Исходная технология Ethernet, в которой использовался коаксиальный кабель, может работать только в полудуплексном режиме. Следовательно, только одно устройство может передавать данные в определенный момент времени. В 1997 году технология Ethernet была доработана; появился дуплексный режим передачи (изначально стандарт 802.3x), позволяющий передавать данные более чем одной станции одновременно. Изобретение Ethernet-коммутаторов дало возможность использовать дуплексный режим передачи и за счет этого более эффективно организовать сетевой трафик, чем это делали концентраторы. Коммутаторы все более активно заменяют концентраторы в высокоскоростных сетях благодаря их способности работать в дуплексном режиме и более эффективно обрабатывать Ethernet-фреймы.

Временные характеристики, формат фрейма и способ передачи этой технологии были описаны в главе 6, "Основы технологии Ethernet", и являются общими для обеих версий технологии Fast Ethernet, рассматриваемых в этой главе.

В технологии 100BASE-TX данные кодируются по алгоритму 4B/5B, потом "перемешиваются" (scrambling — перестановка элементов) и преобразуются в многоуровневый сигнал для передачи MLT-3 (MultiLevel Transmit 3 — трехуровневый сигнал), являющийся кодовым сигналом в линии на основе UTP-кабеля категории 5. Алгоритм MLT-3 преобразует двоичный поток данных в электрическую волновую форму, используя постоянную сигнальную систему. *Кодирование с инверсией без возврата к нулю (NonReturn-to-Zero, Invert — NRZI*) отличается от алгоритма MLT-3 тем, что в последнем уровень сигнала изменяется от отрицательных до положительных значений, в отличие от двух уровней в коде NRZI.

ВНИМАНИЕ!

В NRZI-кодировании сигнал сохраняет постоянные значения напряжения без изменения сигнала (без возврата к уровню 0 Вольт), и наличие данных интерпретируется по изменению сигнала в начале битового интервала. Подобно этому отсутствие изменения интерпретируется как отсутствие данных.

На рис. 7.11 показаны несколько примеров кодирования MLT-3.

Основное правило для кода MLT-3 гласит, что двоичное число 1 соответствует циклическому переходу сигнала на более низкий уровень, после чего должен произойти возврат к исходному значению. Двоичное число 0 не вызывает изменений уровня сигнала.

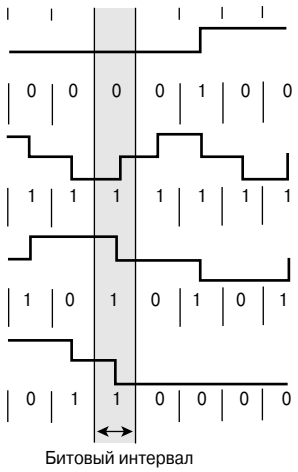


Рис. 7.11. Примеры кодирования с использованием алгоритма MLT-3

В примере, который показан на рис. 7.11, один битовый интервал затемнен для всех исследуемых волновых форм. Для верхней волновой формы внутри выделенного битового периода изменение сигнала не происходит. Такое поведение сигнала соответствует двоичному числу 0. Если бы волновая форма в данном примере задавала только последовательные двоичные нули, соответствующий сигнал оставался бы неизменным и имел бы либо высокий уровень, либо нулевой, либо низкий. За единственной единицей в верхнем примере следуют последовательные нули. На рисунке видно, что двоичное число 0 может появляться при разных уровнях сигнала. Уровень зависит от того, каким было предыдущее значение (высоким или низким), и изменяется в противоположном направлении. Следовательно, для первой волновой формы можно утверждать, что предшествующий сигнал, который не показан на рисунке, имел низкий уровень.

Во второй из приведенных на рис. 7.11 волновых форм имеется изменение уровня сигнала в середине битового интервала. Изменение соответствует двоичному числу 1. При этом не имеет значения, каким был характер изменения (уменьшение или увеличение), и неважно, каким стал итоговый уровень сигнала — высоким, низким или равным нулю. В третьем примере показан сигнал, соответствующий чередующимся значениям двоичных чисел. На этом примере снова проиллюстрировано основное правило: о том, что отсутствие изменений в сигнале соответствует двоичному числу 0, а их наличие — двоичному числу 1. Уменьшение или возрастание сигнала представляет единицу. Сигнал в виде продолжительной горизонтальной линии соответствует последовательности двоичных нулей.

На рис. 7.12 показан пример сигнала 100BASE-TX, записанный с помощью осциллографа. (По оси Y измеряется напряжение, а по оси X — время.)

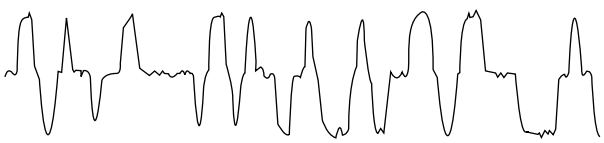


Рис. 7.12. Пример сигнала 100BASE-TX

В процессе начальной установки соединения принимающая сторона ожидает только 4B/5B-группы с кодом “среда свободна”.

Схема подключения кабеля для 100BASE-TX полностью совпадает с применяемой в стандарте 10BASE-T. Используются две отдельные пары для приема и передачи. Для соединения между станциями и повторителями или концентраторами применяется прямой кабель. Внутри концентратора для скорости 100 Мбит/с реализована общая шина, являющаяся общим доменом коллизий. Однако для широко распространенных сегодня концентраторов с автоматическим определением скорости 10/100 Мбит/с внутренняя структура устройств несколько сложнее. Следует также отметить, что несмотря на то что концентраторы для сетей Ethernet со скоростью передачи 100 Мбит/с значительно быстрее концентраторов, которые работают со скоростью 10 Мбит/с, коллизии по-прежнему являются общей проблемой, поскольку

устройства обоих типов основаны на принципах структуры с общей шиной. Только использование коммутаторов и дуплексного режима передачи данных может помочь избежать проблем с коллизиями.

Для соединения коммутатора с рабочей станицей служит прямой кабель. Схема внутреннего устройства коммутатора дает возможность использовать полностью полосу пропускания по каждому из его портов и избежать коллизий.

Все соединения типа "станция-станция", "коммутатор-коммутатор" и "станция-коммутатор" в технологии Fast Ethernet являются соединениями "точка-точка": они имеют два раздельных коммуникационных канала. В этой ситуации коллизии не являются физическим явлением, а результатом административного логического решения не разрешать одновременно использовать сигналы Tx и Rx (прием и передача). Таким образом, использование полудуплексного (административное ограничение алгоритма CSMA/CD) или дуплексного режима (когда физические коллизии отсутствуют) определяет качество работы системы и может быть задано в конфигурации устройства. В большинстве случаев используется дуплексный режим передачи.

При подключении рабочей станции к концентратору необходимо учитывать, что внутри концентратора реализована шинная топология, определяющая домен коллизий. Следовательно, в таких соединениях может использоваться *только* полудуплексный режим передачи, подчиняющийся правилам алгоритма CSMA/CD.

Возникает вполне логичный вопрос: "Доступны ли в Fast Ethernet скорости передачи 200 Мбит/с?" Технология 100BASE-TX передает трафик со скоростью 100 Мбит/с в полудуплексном режиме (хотя часть передаваемых данных является служебной информацией). Но в дуплексном режиме 100BASE-TX поддерживает передачу данных на скорости до 200 Мбит/с (хотя, опять-таки, часть передаваемых данных является служебной информацией). Концепция использования дуплексного режима передачи приобрела исключительное значение в связи с потребностью в увеличении скорости передачи данных в Ethernet-сетях. О принципах построения сетей 100BASE-TX рассказывается далее в этой главе.

Технология 100BASE-FX

Зачем понадобился стандарт 100BASE-FX (введенный как часть стандарта 802.3u-1995)? На тот момент, когда был предложен стандарт Fast Ethernet на основе медного провода, использование оптического кабеля было необходимо для магистральных приложений, межэтажных соединений в зданиях, где не всегда возможно использование медного провода, и в условиях сильных помех. Стандарт 100BASE-FX также рассматривался в качестве альтернативы популярной в то время технологии FDDI (технология двойного оптического кольца со скоростью передачи 100 Мбит/с). Однако на сегодняшний день подавляющее большинство инсталляций Fast Ethernet использует стандарт 100BASE-TX. Одной из причин, по которой стандарт 100BASE-FX не получил широкого распространения, было относительно быстрое появление технологии Gigabit Ethernet для медного кабеля и оптического волокна, которые сегодня являются доминирующими решениями для магистральных каналов, высокоскоростных соединений и большинства инфраструктурных потребностей. Временны*е* характеристики, формат фрейма и способ передачи, описанные

в главе 6, “Основы технологии Ethernet”, используются в технологии Fast Ethernet со скоростью передачи 100 Мбит/с, которая основана на оптической среде.

В стандарте 100BASE-FX используется 4B/5B-кодирование совместно с алгоритмом NRZI для кодирования сигнала в линии. Сигналами являются импульсы света от светодиодов в многомодовом оптическом волокне. Алгоритм NRZI-кодирования задает двоичное значение в зависимости от наличия или отсутствия изменений уровня сигнала в середине битового интервала. Стандарт 100BASE-FX использует синхронный режим передачи.

На рис. 7.13 показаны примеры NRZI-кодирования (по оси X измеряется оптическая мощность, по оси У — время).

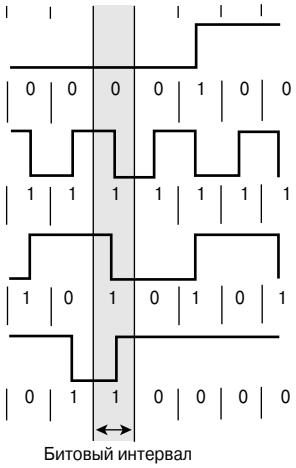


Рис. 7.13. Примеры NRZI-кодирования

В приведенных на рисунке примерах один битовый интервал затенен. Уровень сигнала для верхней волновой формы не меняется, следовательно, этот битовый интервал интерпретируется как двоичное число 0. Отсутствие изменений кодирует двоичное число 0. Волновая форма, соответствующая всем последовательным 0, имела бы вид постоянного сигнала с высоким или низким уровнем.

На второй волновой форме, в выделенном битовом интервале, сигнал изменяется. Изменению сигнала соответствует двоичное число 1, при этом не имеет значения, увеличивался или уменьшался сигнал. Третья волновая форма показывает сигнал для чередующихся значений двоичных чисел. На этом примере еще более наглядно видно, что отсутствие изменений сигнала соответствует двоичному числу 0, а наличие изменений — числу 1.

Последовательный битовый поток, кодированный по алгоритму NRZI, передается с помощью световых импульсов. Из-за циклических временных задержек, возникающих при полном включении/выключении передатчика, используются световые импульсы низкой и высокой мощности. Логическому нулю соответствует низкий уровень мощности, а логической единице — высокий.

В табл. 7.5 показана схема использования контактов в стандарте 100BASE-FX. Чаще всего для оптической пары используются соединители одного из двух типов: ST или SC.

Таблица 7.5. Контакты 100BASE-FX

Оптическая пара	Сигнал
1	Tx (лазерный и LED-передатчики)
2	Rx (детектор — высокоскоростной фотодиод)

На рис. 7.14 показано соединение двух оптических интерфейсов. Два отдельных волокна многомодового оптического кабеля обычно объединены, и на каждом конце находятся сдвоенные соединители.

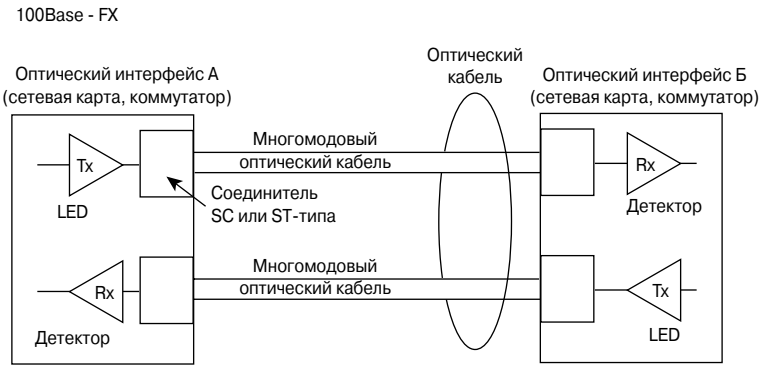


Рис. 7.14. Оптическое соединение двух интерфейсов

MAC-подуровень работает с соединениями типа “точка-точка», в то время как оптоволоконные каналы по своей сути являются дуплексными, поскольку существуют отдельные оптические волокна для Rx- и Tx-сигналов. Соединение 100BASE-FX может работать в полудуплексном режиме, но с определенными ограничениями по длине и количеству допустимых сегментов. Следует четко представлять себе, что в оптической среде физических коллизий быть не может, поскольку есть только последовательные оптические импульсы. Однако существует возможность принудительно, посредством соответствующей настройки, использовать режим CSMA/CD, запретив одновременную передачу Tx- и Rx-сигналов.

Можно ли передавать данные со скоростью 200 Мбит/с, используя оптические технологии? Подобно тому, как при использовании UTP-кабеля существуют отдельные каналы для передачи и приема данных, в технологии 100BASE-FX также есть два отдельных канала для приема и передачи и, следовательно, скорость в 200 Мбит/с достижима.

Принципы построения сетей Fast Ethernet

В технологии Fast Etehernet связи состоят в основном из соединений между станциями и концентратором или коммутатором. Концентраторы фактически являются многопортовыми повторителями, и между удаленными станциями допустимо использование ограниченного количества таких устройств. Коммутаторы в самом простейшем случае можно рассматривать как многопортовые мосты. При использовании таких устройств действует ограничение на длину UTP-кабеля в 100 м, но ограничений на их количество в цепочке нет.

Повторители должны быть маркированы при помощи слова *Class (класс повторителя*) с указанием римской цифры I или II в кружочке, для обозначения устройств класса I или класса II (Class I или Class II). Концентраторы первого класса вносят задержку до 140 битовых интервалов. Любой повторитель, не принадлежащий к одному из двух типов (100BASE-TX или 100BASE-FX), является повторителем класса I. Следует отметить, что немаркированные повторители также являются устройствами класса I. На рис. 7.15 показан максимальный диаметр коллизионного домена при использовании одного повторителя класса I стандарта 100BASE-TX. Использование коммутаторов снимает эти ограничения, а предельные значения определяются максимальной длиной соединения между интерфейсами, зависящей от типа передающей среды.

Рис. 7.15. Максимальный диаметр коллизионного домена при использовании концентратора первого класса

Повторитель класса II вносит задержку не более 92-х битовых интервалов. Благодаря меньшей величине задержки допустимо использование двух последовательных устройств этого класса, но только с очень коротким кабелем между ними. На рис. 7.16 показан максимальный диаметр коллизионного домена для концентраторов второго класса стандарта 100BASE-TX. Использование коммутаторов снимает эти ограничения, и единственным ограничивающим фактором является максимальная длина кабеля между интерфейсами, величина которой зависит от конкретной среды передачи.

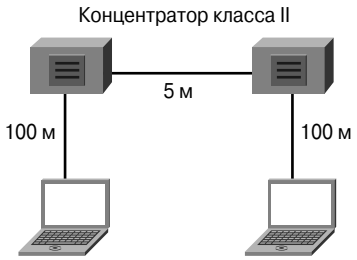


Рис. 7.16. Диаметр коллизионного домена для концентраторов второго класса

Как и для версий технологий Ethernet со скоростью передачи 10 Мбит/с, допустимы некоторые изменения в принципах построения сети для версий со скоростью 100 Мбит/с. Однако эти изменения не должны вносить дополнительные задержки. Если в сети используется новое высокопроизводительное оборудование, возможно, некоторые ограничения удастся преодолеть. Например, если используется кабель, который больше допустимой длины между повторителями, потребуется более короткий кабель для подключения станций. Однако нарушение принципов построения сети для стандарта 100BASE-TX настоятельно не рекомендуется. Вносимые структурные изменения не должны противоречить временным параметрам, описанным в статье 29 действующего стандарта 802.3, и должны быть предусмотрены в используемом оборудовании. Любое устройство, поддерживающее преобразование между несколькими скоростями передачи, например, 10 и 100 Мбит/с, является мостом второго уровня модели OSI. Устройство, способное выполнять преобразование сигнала между средами с разными скоростями передачи данных, не может быть повторителем. Однако одно и то же устройство может повторять сигнал между портами, передающими на одинаковой скорости.

UTP-кабель стандарта 100BASE-TX практически не отличается от кабеля для 10BASE-T, за исключением того, что производительность связи должна удовлетворять более высокому стандарту категории 5 или ISO Class D. Длина кабеля 100BASE-TX между двумя повторителями класса II не может превышать 5 м.

Длина соединений при работе в дуплексном режиме может быть выше значений, указанных в табл. 7.6, поскольку в этом случае существенной является только способность среды передачи доставлять пригодный для декодирования сигнал, а не двукратная задержка (round-trip — задержка на передачу сигнала в прямом и обратном направлении). Не так уж редко можно встретить сети Fast Ethernet, работающие в полудуплексном режиме. Однако использование полудуплексной передачи нежелательно, поскольку сигнальная схема изначально рассчитана на дуплексный режим работы, и поэтому принудительное использование полудуплексного взаимодействия является неразумным использованием ресурсов.

Рекомендуется все соединения между станциями и концентратором или коммутатором настраивать на автоматическое определение режима работы, давая таким образом возможность использовать максимальную производительность. Отключать

автоопределение нужно только в том случае, если какие-то соединения не могут быть установлены с использованием функции автоопределения. В большинстве случаев соединения должны устанавливаться без проблем автоматически.

В табл. 7.6 перечислены правила построения сетей Fast Ethernet.

Таблица 7.6. Длина соединений для различных структур

Структура	100BASE-TX (м)	100BASE-FX (м)	100BASE-TX и 100BASE-FX (м)
Станция-станция, станция-коммутатор, коммутатор-коммутатор (полу- или дуплексный)	100	412	-
Один повторитель, класс I (полудуплексный)	200	272	100 TX 160,8 FX
Один повторитель, класс II (полудуплексный)	200	320	100 TX 208 FX
Два повторителя, класс II (полудуплексный)	205	228	105 TX 211,2 FX

Соединения 100BASE-TX не требуют повторителей для расстояний до 100 метров. На первый взгляд такое расстояние кажется достаточно большим, но в реальных зданиях его часто бывает недостаточно. Концентраторы помогают преодолеть ограничения на длину соединений, но при этом остаются в силе правила, перечисленные в табл. 7.6 и связанные с временными параметрами ограничения. Широкое распространение коммутаторов сделало ограничения на длину соединений менее существенными. Рабочая станция может быть расположена на расстоянии до 100 м от коммутатора, который в свою очередь может быть подключен другим стометровым соединением к следующему коммутатору, и т.д. Именно максимально возможная длина сегмента является практическим ограничением между устройствами для сетей Fast Ethernet, большинство из которых являются коммутируемыми. С этой технологией можно использовать любые топологии: “кольцо”, “звезда” и “расширенная звезда”. В этом случае возникает вопрос выбора логической топологии и маршрутов потоков данных, а не ограничений по времени или расстоянию.

Практическое задание 7.1.9a. Знакомство с сетевым анализатором Network Inspector компании Fluke Networks

Целью этого задания является демонстрация возможностей и методов использования анализатора Network Inspector (NI) для обнаружения и анализа сетевых устройств внутри широковещательного домена. В описании к заданию показаны основные приемы и возможности, которые могут быть использованы в последующих лабораторных работах для поиска неисправностей в сетях.

Практическое задание 7.1.9b. Знакомство с анализатором протоколов Protocol Inspector компании Fluke Networks

Целью этого задания является демонстрация возможностей и методов использования анализатора протоколов Protocol Inspector для анализа сетевого трафика и захвата фреймов. В описании к заданию показаны основные приемы и возможности, которые могут быть использованы в последующих лабораторных работах для поиска неисправностей в сетях.

Интерактивная презентация: структура технологии Fast Ethernet

Цель презентации — закрепить знания о технологии Fast Ethernet.

Гигабитовые и 10-гигабитовые технологии Ethernet

Метод Fast Ethernet (100 Мбит/с) продемонстрировал значительное развитие технологий по сравнению с традиционной сетью Ethernet (10 Мбит/с). Еще более значительный прогресс, достигнутый в гигабитовой технологии (Gigabit Ethernet) относительно Fast Ethernet, свидетельствует о мощи стандартов IEEE, успехе разработок и задает направление развития рынка. Технология Gigabit Ethernet, работающая со скоростью передачи данных 1000 Мбит/с, в 100 раз увеличивает скорость передачи информации в сети по сравнению с популярными и повсеместно используемыми сетями 10BASE-T. Хотя принципы MAC-адресации, доступа CSMA/CD и, что еще более важно, формат фрейма сохранились такими же, как и в предыдущих версиях Ethernet, многие другие аспекты работы MAC-уровня, физического уровня и среды передачи претерпели значительные изменения.

Сегодня допустимо использование одного медного провода для скоростей передачи данных 10/100/1000 Мбит/с. Гигабитовые коммутаторы и маршрутизаторы с гигабитовыми портами доступа к сети в наши дни становятся привычными устройствами в монтажных шкафах. Все больше устанавливается соединений с использованием одно- и многомодовых оптических кабелей. Одной из отличительных особенностей технологии Gigabit Ethernet является применение оптических носителей сигнала. Однако потребность в использовании существующего кабельного хозяйства на основе медных проводов привела к появлению очень продуманной технологии, позволяющей использовать столь популярный в 10 Мбит/с- и 100 Мбит/с-версиях среды Ethernet UTP-кабель категории 5. Все технологии Gigabit Ethernet по своей природе являются дуплексными. Свидетельством уверенного развития технологии служит разработка в настоящий момент стандартов передачи данных со скоростями 40, 100 и 160 Гбит/с. Наиболее впечатляющим является переход Ethernet из технологии, используемой только внутри локальных сетей, в разряд решений для объединения удаленных локальных, региональных и распределенных вычислительных сетей.

Технологии Ethernet со скоростью передачи 1000 Мбит/с

В 1998 году комиссией 802.3z Института инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers — IEEE) был принят стандарт 1000BASE-X. Этот стандарт поднял скорость передачи данных по оптоволоконным

каналам связи в дуплексном режиме до 1 Гбит/с, таким образом увеличив скорость в 100 раз по сравнению со стандартом 10BASE-T. Стандарт 1000BASE-T, описывающий технологию со скоростью 1 Гбит/с и использующий медный UTP-кабель категории 5, был принят в 1999 году.

В табл. 7.7 перечислены рабочие параметры технологии Ethernet, которая работает со скоростью 1000 Мбит/с

Таблица 7.7. Рабочие параметры среды Gigabit Ethernet

Параметр	Значение
Время передачи одного бита	1 нс
Канальный интервал	4096 битовых интервалов
Интервал между фреймами	96 битов[4]
Количество коллизионных попыток	16
Интервал ожидания при коллизии	10
Размер коллизионного jam-пакета	32 бита
Максимальный размер фрейма без метки	1518 октетов
Минимальный размер фрейма	512 битов (64 октета)
Максимальный всплеск	65536 битов

Стандарты 1000BASE-T, *1000BASE-SX* и *1000BASE-LX* используют одинаковые временные параметры. Необходимо отметить, что 1 битовый интервал (время передачи одного бита) на скорости 1000 Мбит/с равен 1 нс, т.е. 0,001 микросекунды, или 1 миллионной секунды. Также необходимо помнить, что некоторые отличия во временных параметрах по сравнению с традиционной технологией Ethernet и Fast Ethernet связаны со специфическими проблемами, возникающими при столь малых значениях битовых и канальных интервалов.

Технология Ethernet со скоростью передачи 1000 Мбит/с (Gigabit) использует тот же формат фрейма, что и технологии со скоростями 10 и 100 Мбит/с. Для разных реализаций технологии Gigabit Ethernet, в зависимости от используемой среды передачи, реализованы различные алгоритмы преобразования фреймов в биты.

Метод Gigabit Ethernet увеличил скорость передачи данных в 10 раз по сравнению с Fast Ethernet. Так же, как это было в случае с Fast Ethernet, увеличение скорости наложило дополнительные требования: передающиеся по соединению биты занимают меньший промежуток времени (1 нс), возросла частота передачи, что потребовало более тщательной синхронизации. Для передачи необходимы частоты, близкие к предельным значениям для среды передачи, что вызвало повышенную чувствительность к помехам. Для решения возникших проблем с синхронизацией, пропускной способностью и соотношением сигнал/шум в технологии Gigabit Ethernet для кодирования информации используются два отдельных этапа. Основная идея состоит в использовании кодов, которые обеспечивают необходимые характеристики

[4] *Официальное значение параметра, согласно стандарту. — Прим. ред.*

пользовательских данных, включая синхронизацию, эффективное использование пропускной способности и улучшенные соотношения сигнал/шум.

Повторяющиеся битовые группы MAC-подуровня преобразовываются в символы, которые могут контролировать такую информацию, как начало фрейма, конец фрейма, и указывать состояние простоя среды передачи. Полный фрейм разбивается на контрольные символы и символы данных (группы кодов данных). Дополнительная сложность реализации необходима для достижения десятикратного увеличения скорости сети по сравнению с Fast Ethernet. В стандарте 1000BASE-T для кодирования первой части используется алгоритм, называемый *8bit-1Quinary quarter (кодирование 8B1Q4*). Вторая часть кодирования отвечает за фактическое кодирование сигнала для конкретной среды передачи и использует принцип *четырехмерного пятиуровневого модулирования амплитуды импульса* (*4-dimensional 5 level pulse amplitude modulation — 4D-PAM5)*. Использование последовательно алгоритмов кодирования сигнала 8B1Q4 и 4D-PAM5 обеспечивает синхронизацию, требуемую пропускную способность и необходимые характеристики для соотношения сигнал/шум, позволяющие передавать данные в дуплексном режиме по каждой из четырех используемых пар проводов одновременно. Для стандарта 1000BASE-X используется кодирование 8-bit/10-bit (8B/10B) (основанное на принципах, аналогичных алгоритму 4B/5B) и простое NRZ-кодирование в линии для оптического сигнала.

Технология 1000BASE-T

При разработке стандарта 1000BASE-T (802.3ab-1999 Gigabit Ethernet over twisted pair) ставились следующие задачи:

- необходимо было включить возможность использовать существующие кабельные сети на основе витой пары категории 5;
- необходимо было гарантировать работоспособность кабеля, прошедшего тест категории 5e, который проходит практически любой кабель при условии правильно установленных и запрессованных разъемов на его концах;
- требовалось обеспечить совместимость с технологиями 10BASE-T и 100BASE-TX;
- необходимо было предусмотреть возможность использования такого стандарта для построения магистралей внутри зданий, связей между коммутаторами, кабельных узлов, серверных блоков и подключения высокоскоростных рабочих станций;
- необходимо было обеспечить десятикратное увеличение пропускной способности по сравнению с технологией Fast Ethernet, ставшей широко распространенной средой, используемой потребителями.

Для достижения требуемой скорости при использовании медного провода категории 5e задействуются все четыре пары провода. Кабель категории 5e может надежно передавать трафик до 125 Мбит/с. Использование сложной электрической схемы, дуплексной передачи для одной пары позволяет передавать до 250 Мбит/с по каждой из пар, поэтому полная пропускная способность для четырех пар составляет

1000 Мбит/с (1 Гбит/с). При рассмотрении принципа работы технологии удобно рассматривать эти четыре пары проводов в качестве "линий", по которым одновременно передаются данные (сборка данных производится в точке назначения получателем).

Временны*е* характеристики, формат фрейма и способ передачи были рассмотрены в главе 6, "Основы технологии Ethernet", и являются общими для всех рассматриваемых версий технологии Ethernet, которые работают со скоростью передачи данных 1000 Мбит/с.

В соединениях 1000BASE-T используется 8B1Q4-кодирование и алгоритм линейного кодирования 4D-PAM5 для кабелей категории не ниже 5e. Для достижения скорости в 1 Гбит/с требуется одновременное использование всех четырех пар в дуплексном режиме. Такой механизм работы приводит к возникновению непрерывных коллизий в каждой из пар проводов, природа которых отличается от коллизий, возникавших в первых Ethernet-сетях на основе коаксиального кабеля. Термин *постоянные коллизии* означает, что передача и прием данных происходят одновременно по одному и тому же проводу, что приводит к очень сложному виду фронтов импульса (voltage patterns). Однако, поскольку в рассматриваемой технологии используются сложные встроенные электрические цепи, которые наряду с прочими технологиями используют еще и технику под названием *подавление эха (echo cancellation*), они обеспечивают надежную работу линии связи.

Несмотря на постоянные коллизии сигнала, система все же работает благодаря тщательному выбору уровней сигнала напряжения и использованию механизма прямого исправления ошибок уровня 1 (Layer 1 Forward Error Correction — FEC).

На рис. 7.17 показан *передаваемый* сигнал (Tx) 1000BASE-T (где по оси Y указано напряжение, а по оси X — время, измеренное с помощью осциллографа). Напряжение измеряется как разностный сигнал между двумя проводами внутри одной из четырех пар, присутствующих в кабеле UTP-типа.

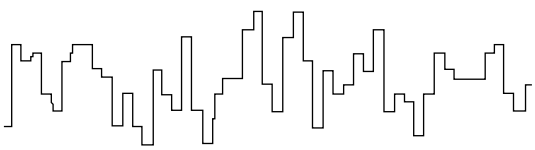


Рис. 7.17. Передаваемый сигнал (Tx) в линии 1000BASE-T

На рис. 7.18 показан *реальный* сигнал, снятый с помощью цифрового осциллографа в нескольких метрах от передатчика вдоль кабеля. По оси Y измеряется напряжение, а по оси X — время. Напряжение измеряется как разностный сигнал между двумя проводами внутри одной из четырех пар, присутствующих в кабеле UTP-типа.

Рис. 7.18. Реальный сигнал 1000BASE-T

Замечательным является тот факт, что сигнал может быть полностью декодирован, и это при том, что в периоды простоя в кабеле присутствуют 9 уровней сигнала, а во время передачи — 17 уровней. Процесс передачи начинается со сложного кодирования данных для передачи в линию. Далее, на рис. 7.18 показано, как выглядит реальный сигнал, который искажен постоянными коллизиями, эффектами затухания и воздействия шума: сигнал выглядит как аналоговый. Ключевым моментом технологии является то, что при помощи хорошо продуманной электрической схемы декодируется даже такой сигнал. Однако при нарушении стандартов на терминирование и защиту от помех технология подвержена проблемам, которые связаны с кабелем. Соединение Gigabit Ethernet работает очень хорошо, если выполнены необходимые требования к передающему кабелю, разъемам и по защите от помех.

В табл. 7.8 собрана полная информация об использовании всех четырех пар UTP-кабеля. Как A, B, C и D обозначены линии передачи данных в одном кабеле. Данные от передающей станции аккуратно делятся на четыре потока, кодируются, передаются и распознаются параллельно, после чего собираются в один поток.

Таблица 7.8. Схема распайки контакта для соединения 1000BASE-T

Номер контакта	Сигнал
1	BI_DA+ (двунаправленные данные, положительное направление)
2	BI_DA- (двунаправленные данные, отрицательное направление)
3	BI_DB+ (двунаправленные данные, положительное направление)
4	BI_DB- (двунаправленные данные, отрицательное направление)
5	BI_DC+ (двунаправленные данные, положительное направление)
6	BI_DC- (двунаправленные данные, отрицательное направление)
7	BI_DD+ (двунаправленные данные, положительное направление)
8	BI_DD- (двунаправленные данные, отрицательное направление)

На рис. 7.19 схематически показана одновременная дуплексная передача по четырем парам. Кабельные соединения типа “станция-станция”, “коммутатор-коммутатор” и “станция-коммутатор” организуются так же, как и для технологии Fast Ethernet.

Исключительно важным является то, что стандарты для Gigabit, Fast и 10BASE-T Ethernet совместимы между собой. На первый взгляд это может показаться малореальным, но выясняется, что если установленные кабельные системы протестированы на соответствие категории 5e, и все восемь проводов в разъеме RJ-45 подключены,

такие системы могут использоваться совместно для технологий Gigabit, Fast и 10BASE-T Ethernet. Аналогично, как после появления стандартов Fast Ethernet появились 10/100 интерфейсы, были разработаны интерфейсы 10/100/1000. Благодаря использованию одинакового формата фрейма, совместимого кабельного хозяйства и разработки разумного интерфейса все технологии отлично работают вместе.

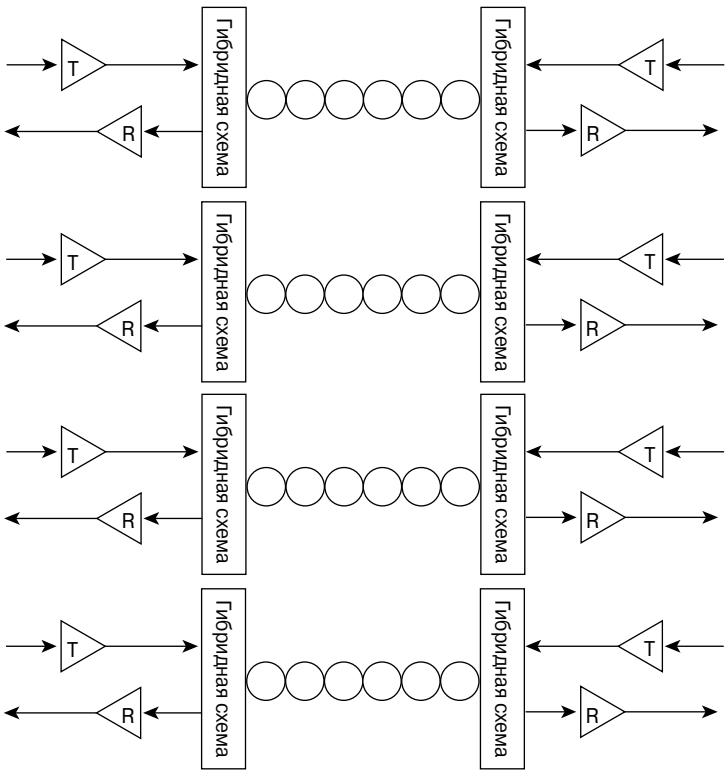


Рис. 7.19. Передача сигнала 1000BASE-T

По историческим причинам в технологии 1000BASE-T сохранены режим доступа CSMA/CD и полудуплексный режим передачи. Однако в подавляющем большинстве случаев среда 1000BASE-T используется в дуплексном режиме, который достигается посредством сложных гибридных электрических цепей, которые могут одновременно использоваться как для передачи (Tx), так и приема данных (Rx).

Перед началом взаимодействия участники передачи определяют, кто из них будет действовать в качестве основного источника меток времени и кто, используя проток данных, — в качестве вторичного источника. Источники меток времени (т.е. синхронизации) служат для создания временных маркеров, использующихся при передаче сигнала. Обычно процесс происходит во время отработки функции автоопределения, хотя может быть настроен вручную. Набор остальных параметров задается

аналогичным образом, включая тип режима передачи (полудуплексный или дуплексный). В процессе автоопределения многопортовые устройства (коммутатор или концентратор) обычно выбираются в качестве основного источника меток времени. Подведем итоги всему сказанному: когда время передачи одного бита равно 1 нс, при скорости передачи данных 1 млн. бит/с и при использовании всех четырех пар для одновременной передачи и приема данных синхронизация исключительно важна.

После рассмотрения технологий 1000BASE-X (1000BASE-SX 1000BASE-LX) мы сравним их с 1000BASE-T.

Технологии 1000BASE-SX и 1000BASE-LX

Технология Gigabit Ethernet на основе оптоволоконного кабеля является одной из наиболее предпочтительных при создании магистральных соединений. Она имеет ряд существенных преимуществ:

- скорость передачи данных составляет 1000 Мбит/с, что позволяет объединять группы широко используемых устройств Fast Ethernet;
- устойчива к помехам;
- отсутствуют потенциальные проблемы с заземлением между кабелем и полом, стенами или зданиями;
- существует множество устройств стандарта 1000BASE-X;
- максимально допустимая длина сегмента достаточно велика.

Стандарт для Gigabit Ethernet-сетей был представлен как дополнение к стандарту IEEE 802.3 под названием “802.3z-1998 1000BASE-X Gigabit Ethernet”. Единственной областью, в которой применение стандартов 1000BASE-SX и 1000BASE-LX происходит медленнее других, является подключение настольных рабочих станций. В этих случаях стандарт 1000BASE-T считается наиболее проверенным и надежным для повседневного использования, кроме того, 10/100/1000 Мбит/с-интерфейсы под медный провод одинаковы.

В стандарте 1000BASE-X используется 8B/10B-кодирование, преобразованное в NRZ-кодирование сигнала в линии. Для этого в качестве источника используется либо недорогой коротковолновой лазер с длиной волны 850 нм (или в некоторых случаях светоизлучающий диод) и многомодовый оптический кабель (1000BASE-SX, где литера S означает коротковолновой либо короткий) или длинноволновой лазер 1310 нм и одномодовый оптический кабель (1000BASE-LX, где литера L означает длинноволновой либо длинный).

Метод NRZ-кодирования основан на определении уровня сигнала в пределах единичного временного интервала и вычисления на его основе битового значения для данного периода. В отличие от большинства описанных ранее схем кодирования, эта схема использует уровень сигнала, а не характер его изменения.

В примере, который показан на рис. 7.20, один из временных периодов затенен. На верхней волновой форме уровень сигнала остается низким во всех периодах, кроме последнего. Низкий уровень соответствует двоичному числу 0. Единственная

двоичная единица появляется в самом последнем периоде и соответствует высокому уровню сигнала.

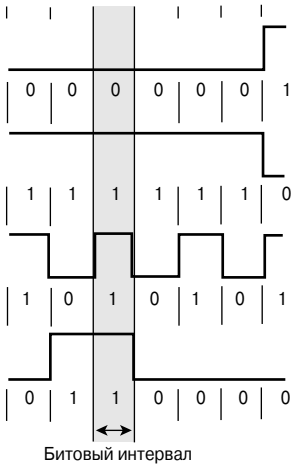


Рис. 7.20. Пример NRZ-кодирования

На второй волновой форме высокий уровень сигнала сохраняется для всех периодов времени, кроме последнего. Высокий уровень соответствует двоичному числу 1. Как и в первом примере, единственный период, в котором появляется двоичное число 0, демонстрирует отличный от предыдущего уровень сигнала. Третья волновая форма соответствует чередующимся двоичным числам, а не последовательности одинаковых значений. На этом примере наглядно показано, что низкий уровень сигнала соответствует двоичному числу 0, а высокий — 1.

В четвертом примере показаны случайно чередующиеся значения. В трех из предложенных выше примеров видно, почему данная схема кодирования может вызывать искажения для постоянного тока в медном проводе. В третьем примере, где уровень сигнала изменяется для каждого последующего периода, смещение напряжения для постоянного тока менее вероятно. Для примеров, в которых сигнал представляет последовательность одинаковых двоичных чисел, вероятность возникновения смещения напряжения за счет постоянного тока для медного кабеля велика, что может привести к потере синхронизации. Для оптического кабеля такая проблема не существует.

Последовательный сигнал, кодированный при помощи NRZ-алгоритма, передается при помощи импульсов света в соответствии со стандартами 1000BASE-SX или 1000BASE-LX. Из-за периодических циклических задержек, возникающих каждый раз при полном включении-выключении передатчика, используются импульсы света высокой и низкой мощности. Логический нуль соответствует низкому значению, логическая единица — высокой мощности.

В табл. 7.9 показан исключительно простой интерфейс взаимного подключения Gigabit Ethernet для оптического кабеля. В большинстве случаев используются оптические соединители SC-типа.

Таблица 7.9. Интерфейс взаимного подключения для Gigabit Ethernet

Оптическое волокно	Сигнал
1	Tx (лазерный передатчик)
2	Rx (высокоскоростной фотодиодный детектор)

На рис. 7.21 показана схема подключения для стандарта 1000BASE-SX. С многомодовым оптическим кабелем обычно используется коротковолновой лазер (или иногда светоизлучающий диод).

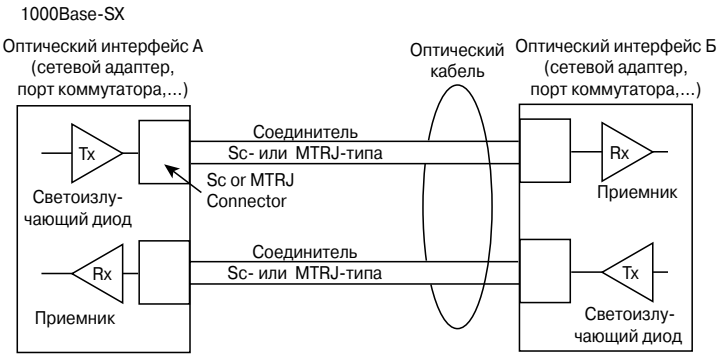


Рис. 7.21. Оптическое соединение 1000BASE-SX

На рис. 7.22 показана схема подключения для стандарта 1000BASE-LX. С одномодовым оптическим кабелем обычно используется лазерный источник, что позволяет передавать сигнал на расстояния до 5000 м.

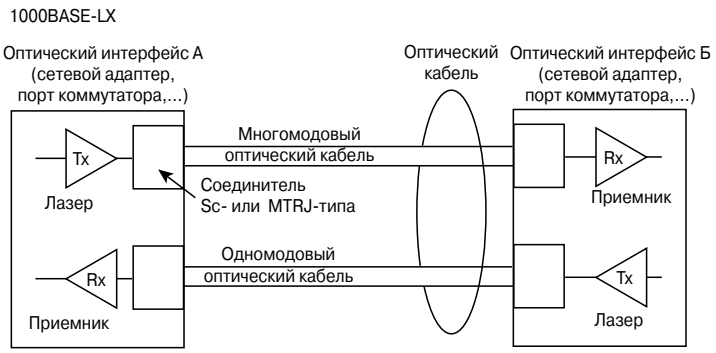


Рис. 7.22. Оптическое соединение 1000BASE-LX

В применяемом для оптических соединений MAC-методе используются соединения типа “точка-точка”. Таким образом, оптические соединения благодаря использованию отдельных кабелей для передачи и приема по своей сути являются дуплексными. В технологии Gigabit Ethernet разрешено использование единственного повторителя между двумя станциями.

Принципы построения сетей Gigabit Ethernet

Любое Ethernet-устройство, способное работать на разных скоростях передачи, например, 100 Мбит/с и 1000 Мбит/с, является мостом второго уровня модели OSI. Устройство не может работать с разными скоростями и при этом оставаться повторителем.

Дуплексные соединения могут быть значительно длиннее, чем это показано в табл. 6.9 и 6.10, поскольку их длина ограничена только свойствами передающей среды, а не задержками передачи и подтверждения. В основе принципа построения среды Gigabit Ethernet используются дуплексные соединения типа “станция-станция”, “станция-коммутатор”, “коммутатор-коммутатор” и “коммутатор-маршрутизатор”. Стандарт 1000BASE-SX предназначен для использования с многомодовым оптическим кабелем. Стандарт 1000BASE-LX использует как многомодовые, так и одномодовые оптические кабели.

В табл. 7.10 и 7.11 перечислены максимальные расстояния при использовании стандартов 1000BASE-SX и 1000BASE-LX. Практический предел расстояния между устройствами определяется коммутируемым характером сетей Gigabit Ethernet. Допустимы топологические схемы построения сети в виде последовательной цепочки, звезды и расширенной звезды. В этом случае вопрос только в выборе логической топологии и маршрута потока данных, а не ограничения по времени или расстоянию.

Таблица 7.10. Максимально допустимая длина кабелей для стандарта 1000BASE-SX

Среда (многомодовый оптический кабель, мкм)	Модальная пропускная способность	Максимальное расстояние (м)
62,5	160	220
62,5	200	275
50	400	500
50	500	550

Таблица. 7.11. Максимально допустимая длина кабелей для стандарта 1000BASE-LX

Среда (мкм)	Модальная пропускная способность	Максимальное расстояние (м)
62,5, многомодовый кабель	500	550
50, многомодовый кабель	400	550
50, многомодовый кабель	500	550
10, одномодовый кабель	-	5000

UTP-кабель для стандарта 1000BSE-T практически не отличается от используемого в стандартах 10BASE-T и 100BASE-TX, за исключением того, что производительность соединения должна соответствовать высшей категории 5e или ISO класса D (2000).

Так же, как в случае с 10- и 100-Мбит/с-версиями сети Ethernet, допустимы незначительные изменения правил построения сети. Однако для случая полудуплексного режима передачи дополнительные задержки недопустимы. Изменение правил построения сети стандарта 1000BASE-T весьма нежелательно. На расстоянии 100 м оборудование стандарта 1000BASE-T работает на пределе физических возможностей по распознаванию сигнала. При наличии проблем с кабелем или внешних помех использование приемлемого в нормальных условиях кабеля становится невозможным даже на допустимых для технологии расстояниях. Любые изменения в правилах построения сети необходимо делать в соответствии со спецификациями на временные характеристики, описанные в стандарте 802.3, и технической информацией о производительности используемого оборудования.

Дуплексные соединения могут быть длиннее, чем это указано в табл. 7.12, поскольку их длина ограничена только способностью среды пропускания доставить сигнал, который может быть декодирован. Они не имеют ограничений, связанных с временем доставки и подтверждения. Очень сложно встретить соединения Gigabit Ethernet, которые работают в полудуплексном режиме. Принудительная работа в полудуплексном режиме для сети, использующей дуплексную сигнальную схему, неразумна с точки зрения использования ресурсов. Работа в полудуплексном режиме накладывает дополнительные ограничения на эффективную длину кабеля, кроме того, существенно возрастают накладные расходы, связанные с расширением несущего сигнала. Повторители в среде Gigabit Ethernet используются, как правило, редко. Это означает, что в большинстве случаев соединения осуществляются между станцией и мостом второго уровня OSI или между двумя мостами, ограничивая таким образом коллизионный домен.

Рекомендуется, чтобы все соединения между станциями и коммутатором были настроены на автоопределение, что позволит достичь максимально высокой общей производительности без риска неправильной конфигурации и поможет избежать случайных ошибок при конфигурировании прочих необходимых для правильной работы среды Gigabit Ethernet параметров.

В табл. 7.12 перечислены параметры полудуплексного режима передачи. Поскольку большинство сетей Gigabit Ethernet являются коммутируемыми, для них действуют параметры, приведенные в табл. 7.10 и 7.11.

Таблица 7.12. Длина кабелей для разных конфигураций в полудуплексном режиме передачи

Схема подключения	1000BASE-T (м)	1000BASE-SX/LX (м)	1000BASE-SX/LX и 1000BASE-T (м)
Станция-станция	100	316	-
Один повторитель	200	220	100, 1000BASE-T 110, 1000BASE-SX/LX

Технология Ethernet со скоростью передачи 10 Гбит/с

В 2002 году был основан комитет IEEE 802.3ae. Разрабатываемый им стандарт определяет спецификации для дуплексной передачи данных по оптическому кабелю со скоростью 10 Гбит/с. Стандарты 802.3ae и 802.3 (оригинальная версия Ethernet), а также все остальные версии Ethernet имеют много общего. Недавно появившаяся технология Ethernet со скоростью передачи 10 Гбит/с (10GbE) показала перспективы дальнейшего развития Ethernet-систем. Использование 10GbE для локальных сетей, сетей хранилищ данных, региональных и распределенных сетей открыла новые возможности для развития сетей. Что же такое 10GbE и где его следует использовать?

Оригинальные технологии Ethernet — Fast Ethernet и Gigabit Ethernet — сегодня доминируют на рынке. Следующим этапом на пути эволюции Ethernet является технология 10 Гбит/с Ethernet (10GbE, позволяющая передавать данные на скорости 10 000 000 000 бит/с). Удовлетворить растущие потребности в пропускной способности при сохранении прежнего формата фрейма и прочих характеристик канального уровня возможно благодаря использованию недорогого, легкого в применении и хорошо совместимого стандарта 10GbE. Эта технология может использовать только оптический кабель в качестве среды передачи, и благодаря ей становится возможным создание сквозных крупномасштабных Ethernet-сетей.

Значительный рост Internet-трафика и объемов потоков данных внутренних сетей требует все больших пропускных способностей для межсетевых соединений и обеспечивает быстрый рост популярности Gigabit Ethernet. Поставщики услуг сетей Internet и частных сетей могут использовать среду 10GbE для создания недорогих высокоскоростных и совместимых соединений между удаленными несущими коммутаторами и маршрутизаторами. Уже сегодня рассматриваются возможности использования 10GbE для таких приложений, как точки присутствия (POP — Point Of Presence), блоки серверов, цифровые видеостудии, сети хранилищ данных и магистральные соединения.

Появление технологии 10GbE привело к существенным концептуальным изменениям. Традиционно Ethernet рассматривается как технология для локальных сетей. Однако стандарт физического уровня для 10GbE позволяет увеличить расстояния (до 40 км при использовании одномодового оптического волокна) и обеспечивает совместимость с синхронными оптическими (SONET) и синхронными цифровыми сетями (SDH). Возможность работать на расстояниях до 40 км делает технологию 10GbE пригодной для использования в сетях регионального масштаба. Совместимость с сетями SONET/SDH, работающими на скоростях до 9,584640 Гбит/с (канал OC-192), делает возможным использование технологии 10GbE в распределенных сетях. Для некоторых приложений стандарт 10GbE может составить конкуренцию технологии ATM.

Ниже приводятся сравнительные характеристики технологии 10GbE с другими разновидностями Ethernet.

- В технологии 10GbE используется тот же формат фрейма, что обеспечивает совместимость всех технологий: устаревших версий, Fast Ethernet, Gigabit и 10 Гбит/с Ethernet без преобразования протоколов и фреймов.

- Время передачи бита равно 0,1 нс. Остальные временные характеристики вычисляются соответственно.
- Нет необходимости в использовании алгоритма доступа CSMA/CD, поскольку все соединения оптического кабеля дуплексные.
- Подуровни уровней 1 и 2 модели OSI практически полностью совпадают с аналогичными спецификациями для стандарта 802.3 с небольшими дополнениями для обеспечения передачи данных на расстояния до 40 км по оптическим каналам и совместимости с сетями SONET/SDH.
- Технология предоставляет возможности для создания гибких, эффективных, надежных и относительно недорогих соединений между локальными сетями.
- Эта среда обеспечивает возможность передавать данные в локальных, региональных и распределенных сетях, используя единый транспортный метод второго уровня.

Базовым стандартом, описывающим метод доступа CSMA/CD, является IEEE 802.3. Дополнение к этому стандарту под названием 802.3ae описывает семейство технологий 10GBASE. Как это всегда бывает с новыми технологиями, рассматриваются несколько разных спецификаций, включая следующие:

- **10GBASE-SR** предназначен для коротких расстояний и использует существующие многомодовые оптические кабели. Рассчитан на расстояния от 26 до 82 метров;
- **10GBASE-LX4** использует *мультиплексирование со спектральным уплотнением сигнала (Wavelength-Division Multiplexing — WDM)*. Рассчитан на расстояния от 240 до 300 метров при использовании существующего многомодового оптического кабеля, и до 10 км при использовании одномодового оптического кабеля;
- **10GBASE-LR** и **10GBASE-ER** рассчитаны на расстояния от 10 до 40 километров при использовании одномодового оптоволокна;
- **10GBASE-SW**, **10GBASE-LW** и **10GBASE-EW** разработаны для использования с оборудованием OC-192/STM SONET/SDH для распределенных сетей.

Комитет IEEE 802.3ae совместно с Альянсом 10 Gb Ethernet (10 GEA) работают над стандартизацией перечисленных выше технологий.

Спецификация 10 Gb Ethernet (IEEE 802.3ae) была стандартизована в июне 2002 года. Она представляет собой дуплексный протокол, использующий оптический кабель в качестве среды передачи. Максимальное расстояние передачи зависит от типа используемого кабеля. При использовании одномодового кабеля максимальное расстояние передачи может достигать 40 км (около 25 миль). Среди членов комитета ведутся дискуссии о возможности создания стандартов для технологии Ethernet со скоростью передачи информации 40, 80 и даже 100 Гбит/с. Принимая во внимание постоянное развитие технологии Ethernet, нет оснований считать, что подобные планы не будут реализованы. Более высокая скорость передачи и бо́льшие расстояния — качества, которые сделали Ethernet не только технологией для локальных, но

и региональных сетей — не единственные новшества, которые будут рассмотрены далее. Поскольку в качестве передающей среды используется оптический кабель, вероятность возникновения ошибок при передаче данных по сети стала намного меньше по сравнению с оригинальными версиями технологии Ethernet. В сети с меньшей вероятностью возникновения ошибок вполне логичным будет передавать данные, используя пакеты большей длины.

Верхний предел количества данных, которые могут передаваться в Ethernet-пакете (фрейме), равняется 1500 байтам. Попытка передать фрейм большей длины приведет к ошибке, и такой фрейм будет отброшен. Таким был стандарт до появления новых технологий Ethernet. При низкой вероятности возникновения ошибок передачи большие файлы могут быть использованы в сети более эффективно, если в каждом фрейме передается больший объем данных. Причина этого состоит в том, что компьютеры расходуют свои ресурсы на генерацию обязательных составляющих каждого Ethernet-фрейма — заголовков и концевиков. Например, если в каждом фрейме будет передаваться в шесть раз больше данных, потребуется меньше (в шесть раз) фреймов для передачи исходного файла. Это означает, что передатчику потребуется сгенерировать (а приемнику обработать) меньше заголовков и концевиков модулей передачи данных, в результате потребуется меньше времени для передачи большого файла между двумя компьютерами. Распределенные сети, которые построены на оптических кабелях, постоянно передают большие пакеты данных.

По этой причине, в особенности в случае подключения многогигабитовой локальной сети к распределенной сети, вероятнее всего, в будущем будут использоваться большие Ethernet-фреймы (так называемые Jumbo-фреймы). Jumbo-фреймом называется любой Ethernet-фрейм, содержащий более 1500 байтов данных. Рекомендуемый максимальный размер для Jumbo-фрейма составляет около 9000 байтов. В настоящий момент Jumbo-фреймы не являются частью нового стандарта IEEE 802.3ae. Однако вполне вероятно, что отдельные производители Ethernet-оборудования встроят возможность использования Jumbo-фреймов при построении Ethernet-сетей на основе их оборудования. Такое действие может подтолкнуть комитет IEEE 802.3 к ратификации использования фреймов большего размера в будущих многогигабитовых стандартах.

В табл. 7.13 перечислены рабочие параметры сетей 10-гигабитовой технологии Ethernet.

Таблица 7.13. Рабочие параметры Ethernet-сетей со скоростью передачи данных 10 Гбит/с

Параметр	Значение
Время передачи одного бита	0,1 нс
Канальный интервал[5]	-
Интервал между фреймами	96[6] битов

[5] *В десятигигабитовой технологии Ethernet не предусмотрен полудуплексный режим работы, поэтому параметры, которые связаны с канальным интервалом и коллизиями, не определены. — Прим. ред.*

[6] *Указанное значение является стандартным, но всегда одинаково у всех производителей. — Прим. ред.*

Окончание табл. 7.13

Параметр	Значение
Максимальное число коллизионных попыток	-
Интервал ожидания при коллизии	-
Размер jam-пакета коллизии	-
Максимальный размер фрейма без метки	1518 октетов
Максимальный размер фрейма	512 битов (64 октета)
Максимальный всплеск	-
Расширенный интервал между фреймами[7]	104 бита

Удивительно, но 10-гигабитовая технология использует тот же формат фрейма, что и среды Ethernet со скоростью передачи данных 10, 100 и 1000 Мбит/с.

Среда передачи, соединения и принципы построения сетей 10GbE

Технология 10-Gb Ethernet в 10 раз увеличила скорость передачи данных по сравнению с Gigabit Ethernet. Так же, как и в случае с Gigabit Ethernet, увеличение скорости вызвало дополнительные требования — время передачи бита стало короче (0,1 нс), что потребовало более тщательной синхронизации. Кроме того, передача происходит на частотах, близких к предельным значениям пропускной способности для используемых физических сред, и данные становятся более подвержены помехам. Для решения проблем с синхронизацией, пропускной способностью и соотношением сигнал/шум в среде 10 Гбит/с Ethernet используются два отдельных этапа кодирования. Основная идея состоит в использовании кодеков, разработанных таким образом, чтобы при представлении данных получить желаемые характеристики сигнала, включая синхронизацию, использование полосы пропускания и параметры соотношения сигнал/шум.

Битовые последовательности преобразуются в символы, которые могут контролировать разнообразную информацию (начало фрейма, конец фрейма, состояние простоя среды). Полный фрейм разбивается на контрольные символы и символы данных (группы кодировки данных). Дополнительные усложнения технологии необходимы для достижения десятикратного увеличения скорости по сравнению с Gigabit Ethernet. В стандарте используется 8B/10B-кодирование (принципиально похожее на 4B/5B), а затем один из нескольких типов линейного кодирования для оптического кабеля.

На рис. 7.23 показано, как происходит 8B/10B-кодирование. В среде 10-Gb-Ethernet используются несколько вариантов комплексного кодирования, предшествующего кодированию сигнала в линии, такие, как 8B/10B и 64B/66B. Биты кодов затем преобразуются в сигналы линии: низкий уровень мощности света соответствует двоичному

[7] *Расширение межфреймового интервала предусмотрено только для технологии 10GBASE-W. — Прим. ред.*

числу 0, высокая мощность света задает двоичное число 1. Комплексные последовательные битовые потоки используются для всех версий 10GbE, за исключением 10GBASE-LX4, где применяется расширенное мультиплексирование со спектральным уплотнением сигнала (Wide Wavelength Division Multiplexing — WWDM) для одновременного мультиплексирования четырехбитовых потоков в виде четырех световых потоков разной длины волны, передаваемых одновременно.

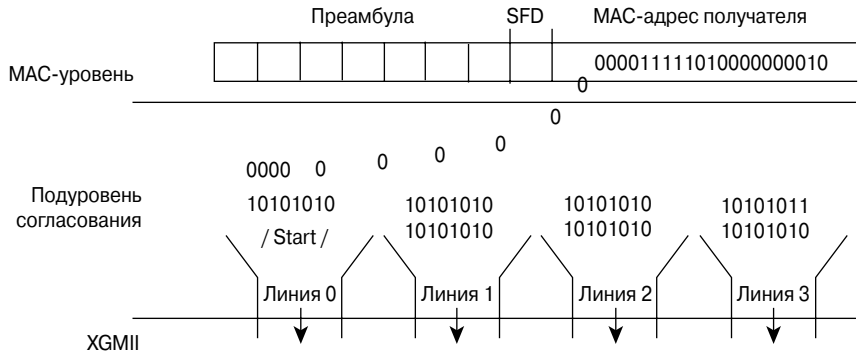


Рис. 7.23. Преобразование MAC-фреймов в 4 потока данных в 10-гигабитовой среде Ethernet

На рис. 7.23 показано, каким образом MAC-фреймы преобразуются в четыре битовые линии для параллельной передачи по четырем парам UTP-кабеля или для последовательной передачи лазером в качестве битового потока в одномодовом оптическом кабеле.

На рис. 7.24 показан случай использования четырех лазерных источников с немного отличающейся длиной волны света[8]. В процессе обработки пришедшего по кабелю оптического сигнала приемник демультиплексирует его в четыре отдельных потока оптических сигналов. Затем эти потоки преобразуются обратно в четыре набора электрических сигналов с использованием процедуры, обратной той, что используется при преобразовании сигнала на разных подуровнях по пути к MAC-уровню.

На сегодня большинство 10GbE-продуктов реализованы в виде дополнительных модулей расширения для высокопроизводительных маршрутизаторов и коммутаторов. В будущем следует ожидать появления большого разнообразия сигнальных компонентов по мере развития технологии 10GbE. Дальнейшее развитие оптических технологий приведет к использованию более совершенных передатчиков и приемников в устройствах соответствующего класса, которые будут разрабатываться на основе модульного подхода. Все разновидности технологии 10GbE используют оптический кабель. Для соединений используются два типа оптических кабелей: 10 мкм — одномодовый кабель, и 50 или 62,5 мкм — многомодовый

[8] *На рисунке PMD — Physical Medium Dependent, подуровень физического уровня, зависящий от среды передачи, который непосредственно взаимодействует с физической средой и выполняет основные функции битовой передачи данных по сети. — Прим. ред.*

кабель. В технологии поддерживается определенный диапазон для величин затухания и дисперсии, но при этом существуют ограничения на максимально допустимые расстояния.

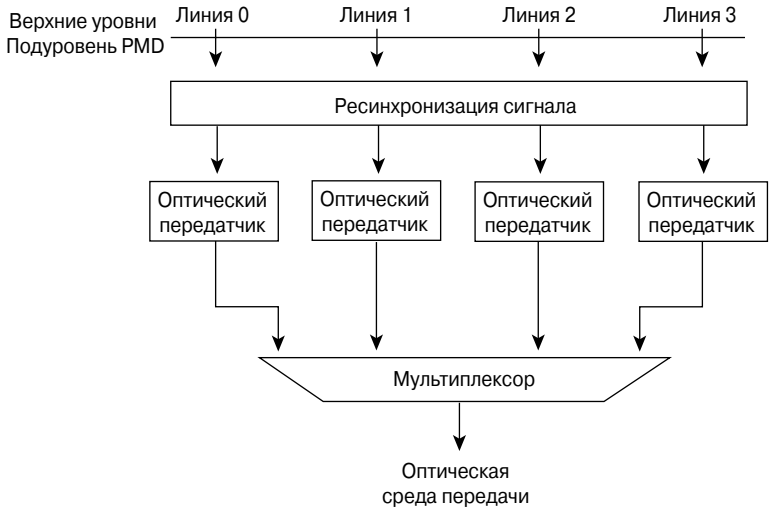


Рис. 7.24. Мультиплексирование сигнала для 10GBASE-LX4

Наиболее широко распространены оптические соединители SC-типа. Поскольку средой передачи для 10GbE является оптический кабель, обычно при подключении оптической пары Tx-контакт устройства 1 подключается к Rx-контакту устройства 2, и наоборот. Основными устройствами, которые подключаются непосредственно через 10GbE, являются высокопроизводительные модульные коммутаторы и маршрутизаторы. В табл. 7.14 показана распайка разъемов для 10GbE.

Таблица 7.14. Распайка разъемов для 10GbE

Оптический кабель	Сигнал
1	Tx (лазерный передатчик)
2	Rx (высокоскоростные фотодиодные детекторы)

Высокоскоростная технология Ethernet работает только в дуплексном режиме передачи, и в ней используются только оптические кабели. В связи с этим коллизий не бывает, и ограничения, связанные с методом доступа CSMA/CD, здесь не играют роли.

С развитием стандартов и продуктов 10GbE появляется большой выбор соответствующих рекомендаций и структурных решений. Наиболее важным является то, что стандарт 10GbE с его возможностями работать в локальных, региональных, сетях хранилищ данных и распределенных сетях открывает перед инженерами возможности построения очень сложных сквозных Ethernet-сетей. Уже сегодня локальные,

региональные, распределенные сети и сети хранилищ данных строятся на основе технологии Gigabit Ethernet.

В технологии 10GbE используется только оптический кабель в качестве среды передачи. Оборудование позволяет работать с 62,5 мкм и 50 мкм-многомодовым, а также 10 мкм-одномодовым оптическим кабелем. Несмотря на то что в стандарте поддерживается только оптический кабель, некоторые предельные расстояния на удивление невелики. В 10-гигабитовой технологии Ethernet не предполагается использование повторителей, поскольку полудуплексный режим передачи данных не поддерживается.

Так же, как и для версий со скоростями передачи в 10, 100 и 1000 Мбит/с, допустимы незначительные изменения принципов построения сети. Допустимые изменения ограничены эффектами потери сигнала и его искажения при прохождении по кабелю. Из-за дисперсии света и прочих эффектов на определенных расстояниях от источника световой импульс становится невозможно декодировать. Прежде чем применять какие-либо модификации, необходимо проверить возможность их использования на соответствие техническим спецификациям текущего стандарта 802.3, а также технической документации используемого оборудования.

В табл. 7.15 перечислены различные реализации 10-гигабитовой технологии Ethernet. Спецификации R и W описываются соответствующими записями (например, 10GBASE-E описывается как 10GBASE-ER, так и 10GBASE-EW).

Таблица 7.15. Реализации 10-гигабитовой технологии Ethernet

Стандарт	Длина волны (нм)	Тип кабеля (диаметр сердцевины)	Минимальная модальная пропускная способность (МГц/км)	Рабочая длина (м)
10GBASE-LX4	1310	62,5, многомодовый	500	от 2 до 300
10GBASE-LX4	1310	50, многомодовый	400	от 2 до 240
10GBASE-LX4	1310	50, многомодовый	500	от 2 до 300
10GBASE-LX4	1310	10, одномодовый	-	от 2000 до 10 000
10GBASE-S	850	62,5, многомодовый	160	от 2 до 26
10GBASE-S	850	62,5, многомодовый	200	от 2 до 33
10GBASE-S	850	50, многомодовый	400	от 2 до 66
10GBASE-S	850	50, многомодовый	500	от 2 до 82
10GBASE-S	850	50, многомодовый	2000	от 2 до 300
10GBASE-L	1310	10, одномодовый	-	от 2000 до 10 000
10GBASE-E	1550	10, одномодовый	-	от 2000 до 30 000i[9]

[9] *Стандарт допускает расстояния до 40 км при условии, что затухание достаточно мало. — Прим. ред.*

Следует отметить многообразие технологии 10GbE. Широкий набор оптических кабелей и лазерных источников сигнала может быть использован на расстояниях, которые необходимы не только для локальных, но и для региональных и распределенных сетей.

Будущее технологии Ethernet

В предыдущих разделах было рассказано о развитии технологии Ethernet, начиная с классических методов, к Fast, Gigabit и многогигабитовым технологиям. Несмотря на то что другие сетевые технологии по-прежнему используются (те, что были установлены ранее), Ethernet является доминирующей технологией для подавляющего большинства новых сетей. На сегодня технология Ethernet является стандартом для вертикальной, горизонтальной структурированной кабельной сети и соединений внутри зданий. Фактически недавно разработанные версии Ethernet стирают границы между локальными, региональными и распределенными сетями с точки зрения географических расстояний, покрываемых единым участком сети.

На рис. 7.25 проиллюстрировано, как увеличился ареал использования технологии Ethernet.

Рис. 7.25. Рост количества сетей и расширение сферы влияния технологии Ethernet

Несмотря на широкое распространение продуктов для гигабитовой и 10-гигабитовой технологий Ethernet, Институт IEEE и Альянс 10-GB-Ethernet к настоящему моменту уже предложили стандарты для скоростей передачи 40, 100 и даже 160 Гбит/с. Какая из технологий будет в итоге принята, зависит от нескольких факторов, включая уровень зрелости технологии и стандартов, степень поддержки рынком и цену.

Исследователи разработали механизмы разрешения конфликтов в среде Ethernet, которые отличны от схемы CSMA/CD. Однако проблема коллизий, фундаментальный недостаток концентраторов и топологии с общей шиной 10BASE5, 10BASE2, 10BASE-T и 100BASE-TX уходит в прошлое. Благодаря использованию

UTP-кабелей и оптического волокна, в которых имеются отдельные пути для передаваемых и принимаемых данных, а также снижению цен на коммутируемые соединения полудуплексные соединения и топология с общей шиной перестали играть важную роль.

В перспективе будут использоваться три разновидности сетевых сред передачи:

- медный провод (со скоростью передачи данных до 1000 Мбит/с, возможно, больше);
- беспроводные технологии (со скоростью передачи данных до 1000 Мбит/с, возможно, больше);
- оптическое волокно (в настоящий момент скорость передачи данных составляет до 10 000 Мбит/с, в ближайшем будущем — больше).

В отличие от медного провода и беспроводной связи, где используемые для передачи сигналов частоты приближаются к практическому пределу, исключительно большая пропускная способность оптического кабеля в обозримой перспективе не будет ограничивающим фактором. В оптических системах ограничения скорости связаны только с технологией производства электронных компонентов — передатчиков и приемников. По этой причине будущие разработки в технологии Ethernet будут связаны, вероятно, с усовершенствованием лазерных источников света и одномодовых оптических кабелей.

Когда Ethernet была относительно "медленной" технологией, полудуплексный режим передачи не предполагал наличия функций качества обслуживания (Quality of Service — QoS), необходимых для передачи трафика определенного типа. В данном случае речь идет о таких технологиях, как IP-телефония и широковещательное видео.

Однако высокоскоростные технологии Ethernet, использующие дуплексный режим передачи и доминирующие на современном рынке, доказали, что они могут использоваться даже с очень требовательными к качеству услуг приложениями, что делает потенциальный круг приложений, используемых совместно с технологией Ethernet, еще шире. По иронии судьбы, возможность гарантировать сквозное качество услуг, способствовавшее в середине 1990-х годов продвижению технологии ATM на рынок настольных рабочих станций и распределенных сетей, сегодня является основной целью, к которой стремится технология Ethernet, сменив ATM.

Технологии Ethernet, которым уже около 30 лет, продолжают свое развитие и имеют прекрасные перспективы.

Резюме

В этой главе были рассмотрены следующие ключевые темы:

- существуют несколько разновидностей технологии Ethernet: "просто" Ethernet, технология Fast Ethernet, Gigabit Ethernet и технология 10-Gigabit Ethernet. Каждому варианту технологии присуща разная скорость работы;

  - технология Ethernet со скоростью передачи 10 Мбит/с (обычная технология Ethernet) ограничена временными параметрами, и поэтому в сети может быть не более пяти сегментов и не более четырех повторителей;
  - сети технологии 10BASE-T основаны на дешевом и легко устанавливаемом кабеле медной витой пары третьей или пятой категории UTP;
  - соединения 10BASE-T могут быть использованы для подключения рабочих станций к коммутатору или концентратору, но их не рекомендуется использовать в магистралях;
- в перспективе будут использоваться три разновидности сетевых сред передачи:
  - медный провод (со скоростью передачи данных до 1000 Мбит/с, возможно, больше);
  - беспроводные технологии (со скоростью передачи данных до 1000 Мбит/с, возможно, больше);
  - оптическое волокно (в настоящий момент скорость передачи данных составляет 10 000 Мбит/с, в ближайшем будущем — больше).

Для закрепления материала воспользуйтесь относящимися к этой главе интерактивными материалами, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Ключевые термины

1000BASE-LX — спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи данных 1000 Мбит/с, в которой используются длинноволновой лазер и одномодовый оптический кабель. Максимальная длина сегмента составляет 10 000 м (32808,4 фута).

1000BASE-SX — спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи 1000 Мбит/с, в которой используется коротковолновой лазер и многомодовый оптический кабель. Максимальная длина сегмента составляет 550 м (1804,5 фута).

1000BASE-T — спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи 1000 Мбит/с, в которой используются четыре пары UTP-кабеля категории 5 и максимальная длина сегмента составляет 100 м (328 футов).

100BASE-FX — спецификация узкополосной[10] технологии Fast Ethernet со скоростью передачи данных 100 Мбит/с, в которой используются два волокна многомодового оптического кабеля для соединений. Для нормальной синхронизации сигнала в

[10] *Способ передачи данных по кабелю, при котором каждый бит данных кодируется отдельным электрическим или световым импульсом; при этом весь кабель используется в качестве одного канала связи. — Прим. ред.*

100BASE-FX соединение не должно превышать 400 м (1312 футов). Описывается стандартом IEEE 802.3.

100BASE-TX — спецификация узкополосной технологии Fast Ethernet со скоростью передачи данных 100 Мбит/с, в которой используется две пары кабеля UTP или STP. Первая пара используется для приема данных, вторая — для передачи. Для нормальной синхронизации сигнала в 100BASE-OX соединение не должно превышать 100 м (328 футов). Описывается стандартом IEEE 802.3.

10BASE2 — спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используется тонкий коаксиальный кабель с сопротивлением 50 Ом. Она является частью стандарта IEEE 802.3; ограничение на длину сегмента составляет 185 м (606 футов).

10BASE5 — спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используется толстый коаксиальный кабель с сопротивлением 50 Ом. Она является частью стандарта IEEE 802.3; ограничение на длину сегмента составляет 500 м (1640 футов).

10BASE-T — спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используются две пары кабеля типа витая пара (категории 3, 4, 5): одна пара — для передачи данных, другая — для приема. Она является частью стандарта IEEE 802.3; максимальная длина сегмента равна 100 м (328 футов).

4D-PAM5 представляет собой метод символьного кодирования, используемый в технологии 1000BASE-T. Четырехмерные пятеричные (4D) символы, полученные при 8B1Q4-кодировании, передаются с использованием пяти уровней напряжения (PAM5). Четыре символа передаются параллельно в каждый период времени.

8B1Q4 — кодирование, которое описано в стандарте IEEE 802.3, представляет собой метод обработки данных, используемый в технологии 1000BASE-T при конвертировании GMII-данных в четыре пятеричных символа (Q4), передающиеся за один период (1Q4).

Thinnet — термин, обозначающий более тонкий и менее дорогой коаксиальный кабель для стандарта 10BASE2.

Алгоритм кодирования "без возврата к нулю с инверсией" (NRZI —nonreturn to zero inverted) — метод, который обеспечивает постоянный уровень напряжения при отсутствии данных (сигнал не возвращается к уровню 0 Вольт) для заданного битового интервала. В этом алгоритме наличие данных определяется по наличию изменения уровня сигнала в начале битового интервала, и об отсутствии данных свидетельствует отсутствие изменений в сигнале.

Алгоритм кодирования "без возврата к нулю" (NRZ — nonreturn to zero) — метод, который обеспечивает постоянный уровень напряжения при отсутствии данных (сигнал не возвращается к уровню 0 Вольт) для заданного битового интервала.

Кодирование — процесс представления битов при помощи различных уровней напряжения.

Манчестерское кодирование (Manchester encoding) — это цифровая схема кодирования, используемая в стандарте IEEE 802.3 в сетях Ethernet, в которой междубитовые переходы используются для синхронизации; бинарному числу 1 соответствует высокий уровень сигнала в первый полупериод битового интервала.

Спектральное уплотнение сигнала (WDM — Wavelength-Division Multiplexing) — метод, позволяющийт одновременно передавать несколько световых импульсов с разной длиной волны в оптическом кабеле. Спектр каждого канала должен быть адекватным образом отделен от остальных.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. Как называется основной используемый в технологии Ethernet метод доступа к разделяемой среде передачи данных?

а) TCP/IP.

б) CSMA/CD.

в) CMDA/CS.

г) CSMA/CA.

2. Какова максимально допустимая длина толстого коаксиального кабеля в технологии Ethernet без использования повторителя?

а) 185 м.

б) 250 м.

в) 500 м.

г) 800 м.

3. Технология Ethernet со скоростью передачи 10 Мбит/с имеет временны*е* ограничения и позволяет использовать не более ____ сегментов, разделенных не более чем ____ повторителями.

а) Три, два.

б) Четыре, три.

в) Пять, четыре.

г) Шесть, пять.

4. Какая максимальная скорость передачи данных поддерживается технологией Fast Ethernet?

а) 5 Мбит/с.

б) 10 Мбит/с.

в) 100 Мбит/с.

г) 1000 Мбит/с.

5. Выберите из списка две кабельные спецификации для Gigabit Ethernet.

а) 1000BASE-TX.

б) 1000BASE-FX.

в) 1000BASE-SX.

г) 1000BASE-LX.

д) 1000BASE-X.

6. С помощью чего передаются данные в стандарте 1000BASE-SX?

а) Длинноволновой лазер в одно- и многомодовом оптическом кабеле.

б) Медный UTP-кабель категории 5.

в) Экранированный двухпарный медный STP-кабель с сопротивлением 150 Ом.

а) Коротковолновой лазер и одномодовый оптический кабель.

7. В каком из перечисленных ниже стандартов Gigabit Ethernet используется 4D-PAM5-кодирование?

а) 1000BASE-LX.

б) 1000BASE-SX.

в) 1000BASE-T.

г) 1000BASE-CX.

8. Какой из IEEE-стандартов описывает технологию 10-Gb Ethernet?

а) 802.3z.

б) 802.3u.

в) 802.3ae.

г) 803.3.

9. Какое из перечисленных ниже свойств присуще дуплексному режиму передачи по одному и тому же проводнику в технологии 1000BASE-T?

а) В линии постоянно происходят коллизии.

б) Повышается качество декодирования сигнала.

в) К каждому сеансу передачи данных добавляются два дополнительных транзитных узла.

г) Соотношение сигнал/шум заметно возрастает.

10. Какова максимальная длина канала, который работает на основе технологии 10 Гбит/с Ethernet?

а) 82 м.

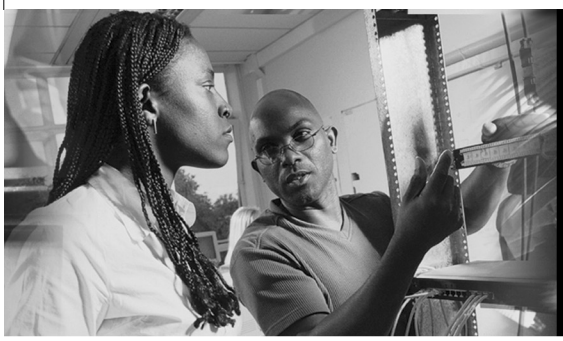
б) 240 км.

в) 10 км.

г) 40 км.

д) 82 км.

е) никаких ограничений нет.



ГЛАВА 8

Ethernet-коммутация

В этой главе...

- рассмотрен принцип работы мостов второго уровня;
- описан принцип работы коммутаторов локальных сетей;
- подробно рассмотрены основные методы коммутации фреймов: сквозная, бесфрагментная и коммутация с промежуточным сохранением фрейма, а также описаны их сходства и различия;
- описаны функции и особенности работы протокола распределенного связующего дерева (STP);
- рассмотрен принцип работы протокола STP;
- указаны различия между доменом коллизий и широковещательным доменом;
- описано, какие именно устройства первого, второго и третьего уровней эталонной модели OSI создают широковещательные домены, а какие — домены коллизий;
- описан процесс микросегментации;
- дано определение широковещательных рассылок;
- описан процесс перемещения потоков данных через компьютерную сеть;
- описано, что представляет собой сегментация, и перечислены устройства, которые создают сегменты.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

коллизии, с. 406,

широковещательные рассылки, с. 406,

протокол распределенного связующего дерева, с. 406,

режим коммутации с промежуточным хранением, с. 413,

режим сквозной коммутации, с. 413,

бесфрагментный режим коммутации, с. 413,

домен коллизий, с. 420,

широковещательный домен, с. 428,

сегмент, с. 430.

Разделяемая среда технологии Ethernet работает без нареканий только в идеальных условиях. Если устройств, которые пытаются получить доступ к среде сети, не много, то количество коллизий не превышает приемлемых значений. Однако когда число пользователей в сети растет, рост количества коллизий может привести к значительной деградации производительности сети. Технологии прозрачного объединения сетей с помощью мостов были разработаны для того, чтобы решить проблему уменьшения производительности при росте количества коллизий. Методы и алгоритмы коммутации потоков данных берут свое начало от технологий мостов, и на сегодняшний день они стали ключевыми технологиями в современных локальных сетях Ethernet.

Коллизии и *широковещательные рассылки* являются вполне обычными и нормальными явлениями в современных сетях. Фактически они были "встроены" в базовую технологию Ethernet и высокоуровневые технологии еще на этапе разработки. Тем не менее, когда количество коллизий и широковещательных рассылок превышает оптимальный предел, заметно страдает как производительность сети, так и сетевое оборудование. Концепция доменов коллизий и широковещательных доменов связана с методами проектирования сетей и используется для уменьшения негативного влияния коллизий и широковещания на полезный сетевой трафик. В этой главе основное внимание уделено объяснению того, как с помощью мостов и коммутаторов можно разбить сеть на сегменты, чтобы увеличить общую производительность информационной инфраструктуры.

По мере увеличения количества узлов в физическом сегменте конкуренция за среду пропускания возрастает. Добавление новых узлов увеличивает потребность в доступной полосе пропускания и вносит дополнительную нагрузку на среду передачи. Дополнительный трафик увеличивает вероятность коллизий, вызывая большое количество повторных передач. Для решения этой проблемы большой сегмент разбивается на части при помощи коммутаторов серии Catalyst. Вновь созданные части становятся изолированными доменами коллизий. За счет такого подхода к построению структуры сети снижается количество коллизий и повышается надежность инфраструктуры.

Технологии коммутации и мостовые соединения уменьшают конкуренцию в локальных сетях за счет уменьшения трафика и увеличения пропускной способности. Мосты и коммутаторы локальных сетей, работающие на первом и втором уровнях модели OSI, пересылают фреймы на основе MAC-адресов, реализуя таким образом функции коммутации. Если MAC-адрес второго уровня не известен, устройство отсылает фрейм во все сегменты в надежде доставить его получателю. Мосты и коммутаторы локальных сетей также передают все широковещательные фреймы. Как следствие последней особенности, может произойти широковещательный шторм или трафик, передающийся по сети, будет бесконечно курсировать в замкнутой петле[1]. *Протокол распределенного связующего дерева (Spanning Tree Protocol — STP)* предотвращает образование подобных кольцевых маршрутов — это технология,

[1] *Такое возможно в сугубо коммутируемой среде (без маршрутизаторов) за счет того, что во фреймах второго уровня нет такого поля, как TTL, и поэтому фрейм может существовать вечно. — Прим. ред.*

позволяющая коммутаторам взаимодействовать друг с другом и обнаруживать физические петли в сети.

Ethernet-коммутация

В следующем разделе представлена обзорная информация о методах и особенностях коммутации в среде Ethernet. Основное внимание уделено следующим вопросам:

- мосты второго уровня эталонной модели OSI;
- коммутация второго уровня;
- принцип работы коммутатора;
- задержка передачи данных;
- режимы коммутации;
- протокол распределенного связующего дерева.

Использование мостов второго уровня

Мостом называется устройство, работающее на втором уровне эталонной модели OSI, которое предназначено для создания двух или более сегментов локальной сети, каждый из которых является отдельным доменом коллизий. С определенной точки зрения мосты необходимы для создания оптимальной пропускной способности. Мост предназначен для фильтрации трафика в локальной сети и его локализации и, кроме того, обеспечения соединения с другими частями (сегментами) локальной сети для передачи предназначенного им трафика. Для фильтрации и избирательной передачи сетевого трафика в мостах строятся таблицы всех MAC-адресов узлов, расположенных в сетевом сегменте и других сетях, и устанавливается соответствие таких адресов с портами самого устройства. Происходит это следующим образом:

- для передаваемых по сети данных мост сравнивает MAC-адрес получателя с MAC-адресом, хранящимся в таблице устройства;
- если MAC-адрес отправителя отсутствует в таблице адресов устройства, мост создает новую запись в таблице, которая связана с соответствующим портом-отправителем фрейма; такая привязка позволяет устройству быстро определить, по какому маршруту (т.е. в какой порт) нужно передавать все последующие фреймы, предназначенные для заданного сетевого устройства;
- если мост определяет, что MAC-адрес получателя фрейма находится в том же сегменте, что и адрес его отправителя, такие данные не передаются в другой сегмент. Этот процесс определения называется *фильтрацией*. Благодаря ему мосты могут существенно уменьшить объем трафика между сетевыми сегментами посредством ограничения ненужного трафика;
- если мост определяет, что MAC-адрес получателя фрейма не находится в том же сегменте, что и адрес его отправителя, данные передаются в соответствующий сегмент;

- если MAC-адрес получателя не известен мосту, производится широковещательная рассылка данных всем сетевым устройствам, за исключением отправителя. Такой процесс называется *лавинной передачей (flooding)*.

Презентация: объединение сегментов с помощью мостов
В этой видеопрезентации показано, как мост перенаправляет фреймы и заполняет свою таблицу адресов.

Коммутация второго уровня

Обычно у моста есть только два порта, и он делит домен коллизий на две части. Все решения принимаются мостом на основе информации о MAC-адресах второго уровня и никак не влияют на схему логической адресации третьего уровня. Таким образом, мост делит на менее крупные части коллизионный, но не логический или широковещательный домен. Вне зависимости от того, какое количество мостов используется в сети, и при условии, что в сети нет устройства, подобного маршрутизатору, работающему на третьем уровне, вся сеть использует единое логическое (широковещательное) адресное пространство. Мост будет создавать новые (и более мелкие) домены коллизий, но не будет увеличивать количество широковещательных доменов. Поскольку любое сетевое устройство обязано обрабатывать широковещательную информацию, мосты всегда передают ее. Следовательно, все сегменты в сетевой среде, использующей мосты, рассматриваются в качестве единого широковещательного домена.

Коммутаторы для локальных сетей по существу являются многопортовыми мостами, использующими *микросегментацию* для уменьшения количества коллизий в сети и увеличения пропускной способности. Коммутаторы для локальных сетей также поддерживают такие свойства, как дуплексное взаимодействие и множественные параллельные диалоги. На рис. 8.1 показана локальная сеть с тремя рабочими станциями, коммутатором и адресная таблица коммутатора. В коммутаторе есть четыре интерфейса (или сетевых соединения): станции А и В подключены к интерфейсу третьего коммутатора, а станция Б — к интерфейсу четвертого. Станция А намеревается передать данные станции Б (рис. 8.2).

Коммутатор, работающий на втором уровне, может анализировать адреса MAC-уровня. Когда коммутатор получает фреймы, переданные станцией А, он определяет MAC-адрес отправителя и записывает его в адресную таблицу (рис. 8.3).

Для проходящего через коммутатор трафика создается запись в адресной таблице, в которой указана станция-отправитель и интерфейс коммутатора, к которому она подключена. Теперь коммутатор знает, к какому порту подключена станция А. После того как этот фрейм данных обрабатывается в коммутаторе, он передается во все интерфейсы (посредством лавинной рассылки), поскольку станция-получатель не известна (рис. 8.4).

Однако после того как запись об адресе помещена в таблицу, приходит ответ от станции Б станции А. Теперь коммутатор знает, что станция Б подключена к его интерфейсу 4 (рис. 8.5).

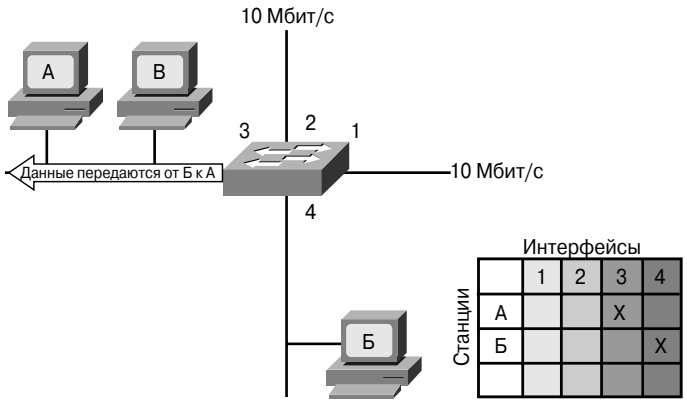


Рис. 8.1. Принцип работы коммутатора в локальной сети

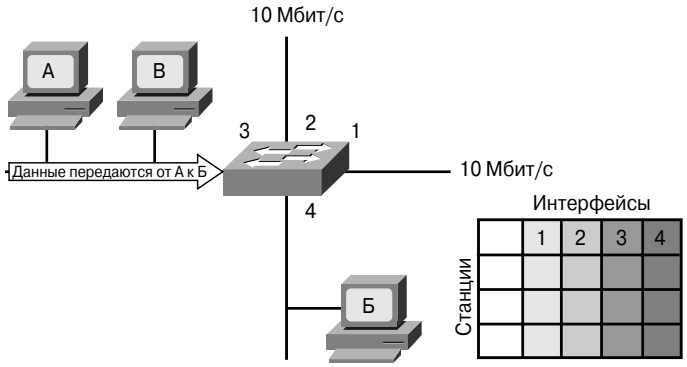


Рис. 8.2. Построение адресной таблицы

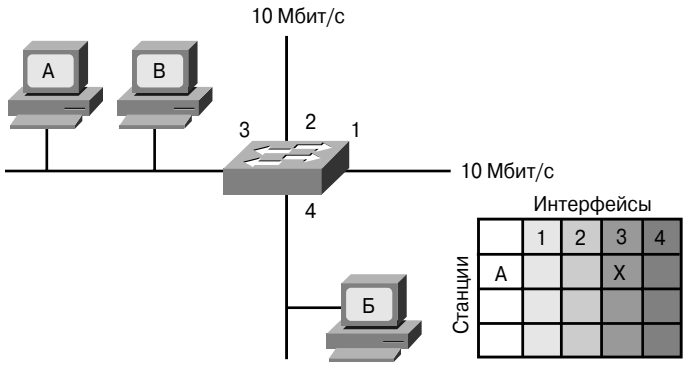


Рис. 8.3. Пересылка данных во все интерфейсы коммутатора

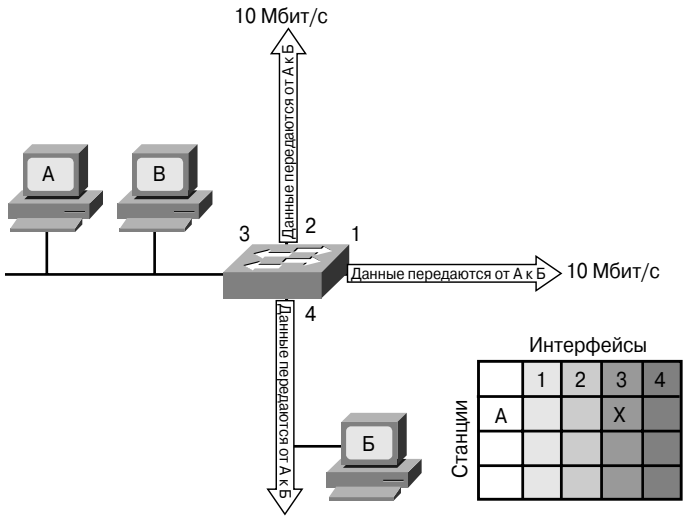


Рис. 8.4. Ответ на широковещательную рассылку

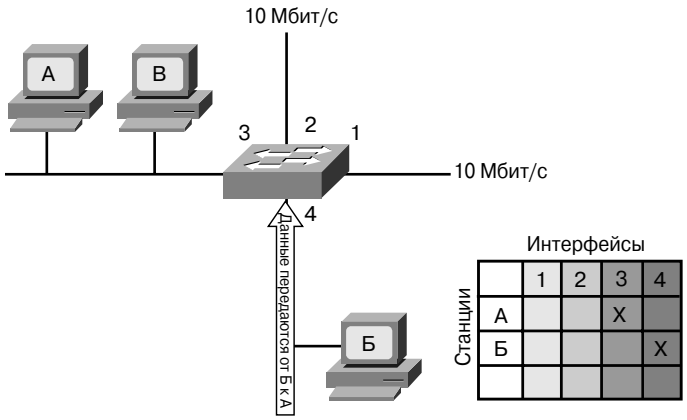


Рис. 8.5. Передача данных от известной станции

Данные передаются коммутатору, но на этот раз широковещательная рассылка не происходит. Коммутатор пересылает данные через интерфейс 3, поскольку знает, куда именно подключена станция А (рис. 8.1).

Во время исходной передачи было определено, на каком именно порту находится соответствующий MAC-адрес, что позволило коммутатору доставить данные более эффективно.

Принцип работы коммутатора

С развитием технологий стало возможным построение мостов с более развитыми возможностями. Конечной целью является построение такой топологии сети, где на каждый порт моста приходится по одному узлу. Такой подход настолько уменьшил бы домен коллизий, что коллизии практически перестали бы существовать. Коммутатор выполняет именно такую задачу и фактически является мостом со множеством портов. Получающиеся в результате маленькие физические сегменты называются *микросегментами*.

Помимо быстрых микропроцессоров и памяти, два других технологических новшества способствовали созданию коммутаторов. Ассоциативная память (Content Addressable Memory — CAM), по существу, использует обратный принцип по сравнению с традиционной памятью. Данные помещаются в память, и процессору возвращается связанный с ними адрес. Использование CAM-памяти позволяет коммутатору напрямую находить порт, соответствующий MAC-адресу, без использования специализированных алгоритмов поиска. Специализированные интегральные микросхемы (Application Specific Integrated Circuit — ASIC) — это устройства, состоящие из невыделенных логических элементов, которые могут быть запрограммированы для выполнения функций с очень высокими скоростями. Благодаря микросхемам ASIC операции, которые ранее должны были выполняться программным обеспечением, теперь могут выполняться аппаратно. Использование указанных двух технологий существенно сократило задержки за счет программного обеспечения и позволило коммутатору поддерживать темп работы, необходимый для обеспечения взаимодействия многих микросегментов и высоких скоростей передачи.

Дуплексный режим передачи

Еще одним механизмом, который позволил удвоить пропускную способность между узлами, является режим дуплексной передачи. Дуплексная передача между станциями возможна при использовании Ethernet-соединения типа “точка-точка”. Эта функция может быть полезна, например, при подключении узлов, интенсивно использующих полосу пропускания, как в случае соединения между сервером и коммутатором. Дуплексный режим передачи обеспечивает передачу данных без коллизий. Поскольку прием и передача могут осуществляться одновременно, нет необходимости в анализе доступной полосы пропускания.

Для соединения со скоростью 10 Мбит/с при дуплексной передаче предоставляется полоса пропускания в 10 Мбит/с для передачи данных и 10 Мбит/с — для приема, что в сумме дает эффективную полосу в 20 Мбит/с для одного соединения. Аналогично для соединения со скоростью передачи 100 Мбит/с дуплексный режим обеспечивает полосу пропускания 200 Мбит/с (рис. 8.6). Дуплексный режим передачи также поддерживает два коммуникационных пути для скорости 1 Гбит/с.

Рис. 8.6. Технология коммутации: дуплексный режим передачи данных

Микросегментация

Микросегментация способствует созданию выделенных сегментов и обеспечивает выделенную полосу пропускания для каждого сетевого узла. Каждый пользователь получает непосредственный доступ к полной полосе пропускания и не конкурирует с остальными пользователями за пропускную способность структуры. Это означает, что пара устройств, подключенных к одному коммутатору, может взаимодействовать параллельно с минимальным количеством коллизий. Микросегментация ограничивает коллизии в сети и эффективно увеличивает емкость сети для каждой из подключенных станций.

Задержка

Задержка, иногда называемая *задержкой распространения информации (propagation delay*), — это время, которое необходимо фрейму или пакету для прохождения всего пути от узла отправителя к получателю по сети. Задержки в сети определяются множеством факторов. Перечислим основные из них:

- задержки среды передачи, вызванные конечной скоростью распространения сигналов по кабелю;
- задержки электрических цепей, вызванные электрическими компонентами, обрабатывающими сигнал на его пути по сети;
- программные задержки, вызванные программным обеспечением при реализации алгоритмов коммутации и протоколов передачи;
- задержки, связанные с содержимым фрейма, проявляющиеся тогда, когда принимается решение о коммутации фрейма (например, устройство не может маршрутизировать фрейм к получателю до тех пор, пока не будет прочитан соответствующий MAC-адрес получателя).

Время ожидания рассчитывается как время между моментом, когда фрейм только начал свой путь от отправителя, и моментом, когда его первая часть достигла пункта назначения.

Режимы коммутации

Способ, которым содержимое фрейма коммутируется в порт назначения, обычно является компромиссом между временем ожидания и надежностью передачи. Три различных режима коммутации — с промежуточным хранением (store-and-forward), сквозной (cut-through) и бесфрагментный (fragment-free) — дают различные соотношения производительности и задержки передачи данных в сети.

Режим коммутации с промежуточным хранением

При использовании режима коммутации с промежуточным хранением информации коммутатор читает всю информацию во фрейме, проверяет его на отсутствие ошибок, принимает решение о коммутации в соответствующий порт и после этого пересылает фрейм в нужном направлении. На рис. 8.7 показана работа коммутатора в таком режиме. Очевидно, что коммутатору приходится тратить больше времени на чтение всего фрейма. Если фрейм содержит ошибки, он не передается и будет отброшен. Несмотря на то что сквозной режим коммутации быстрее, он не предоставляет механизм обнаружения ошибок. Задержки, вносимые при работе устройства в режиме с промежуточным хранением, обычно не представляют проблемы, тем не менее, данному режиму присуща максимальная величина задержки.

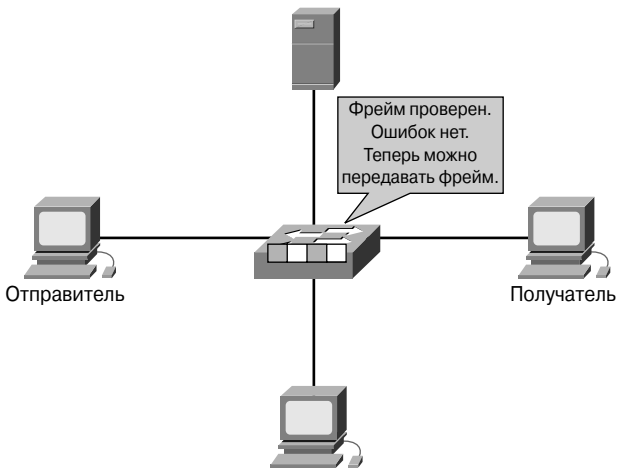


Рис. 8.7. Режим коммутации с промежуточным хранением

Режим сквозной коммутации

В этом режиме коммутатор при прохождении через него трафика считывает начало фрейма до адреса получателя и "перебрасывает" его получателю, не читая остаток фрейма (рис. 8.8).

Этот режим коммутации уменьшает задержки при передаче, однако в нем нет механизмов обнаружения ошибок.

Бесфрагментный режим коммутации

Этот режим является модифицированной формой сквозного режима. В нем передача осуществляется после фильтрации фрагментов коллизий, к которым относится подавляющее число ошибочных пакетов. Коммутатор в этом режиме ждет окончания проверки, не является ли полученный пакет коллизионным фрагментом, и только после этого передает его.

Рис. 8.8. Режим сквозной коммутации

Когда использовать различные режимы коммутации

При использовании режимов сквозной и бесфрагментной коммутации порт отправителя и порт получателя должны работать на одной скорости, чтобы не происходило преобразование фрейма. Такой режим работы называется *синхронной, или симметричной, коммутацией (synchronous switching*). Если скорости портов разные, фрейм должен быть полностью сохранен для технологии одной скорости, прежде чем он будет передан на другой. Такая схема называется *асинхронной коммутацией (asynchronous switching*). Для асинхронной коммутации должен использоваться режим с промежуточным хранением данных. Асинхронная (часто называемая также асимметричной) коммутация обеспечивает коммутируемые соединения между портами разной пропускной способности, например, 100 и 1000 Мбит/с. Асимметричная коммутация оптимизирована для клиент-серверного трафика, при котором множество клиентов одновременно общается с сервером, что требует выделения большей полосы пропускания для серверного порта с целью устранения узкого места в сети.

Основы протокола распределенного связующего дерева

При использовании множества соединенных между собой коммутаторов могут возникать кольцевые маршруты и отсутствовать четкий путь от отправителя к получателю. На рис. 8.9 показано, что при использовании простого иерархического дерева такие замкнутые маршруты появиться не могут.

На рис. 8.10 показано, что при появлении дополнительных коммутаторов или мостов для обеспечения резервирования соединений и повышения надежности сети и защиты от сбоев могут возникнуть кольцевые маршруты, следствием которых будет возникновение так называемой широковещательной лавины — чрезмерного количества широковещательных фреймов в сети.

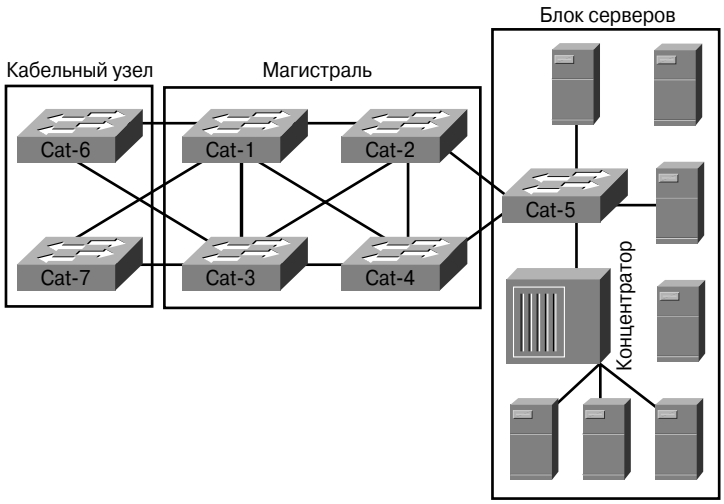


Рис. 8.9. Протокол STP предотвращает возникновение кольцевых маршрутов

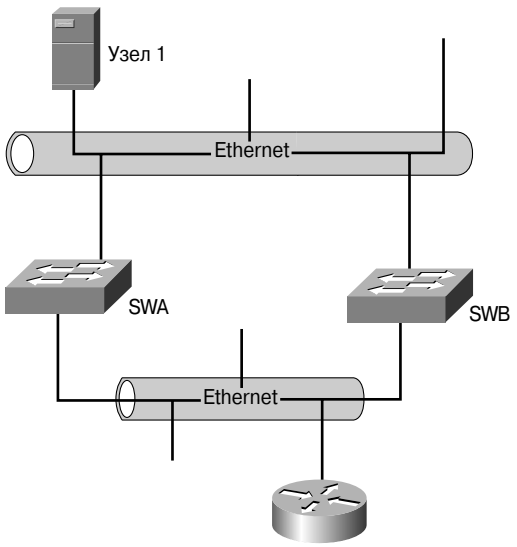


Рис. 8.10. Широковещательная лавина

В показанной на рис. 8.10 схеме сети возникает описанная ниже ситуация.

1. Узел 1 передает широковещательное сообщение.
2. Коммутатор SWA и коммутатор SWB получают фрейм.
3. Коммутатор SWA пересылает фрейм коммутатору SWB.
4. Коммутатор SWB пересылает фрейм коммутатору SWA.

5. Теперь каждый коммутатор видит множество фреймов от одной и той же широковещательной рассылки, которые приходят через разные порты устройств, и возникает кольцевой маршрут.

Чтобы избежать подобной ситуации, коммутаторы используют специальный протокол для взаимодействия друг с другом. Как показано на рис. 8.11 и 8.12, коммутатор посылает через все свои порты специальное сообщение, которое называется *модулем данных мостового протокола (Bridge Protocol Data Units — BPDU*), чтобы проинформировать остальные коммутаторы в сети о своем существовании. Коммутаторы используют алгоритм распределенного связующего дерева (Spanning Tree Algorithm — STA) для поиска и отключения резервных маршрутов. Процесс выключения порта называется *блокированием (blocking*). В результате обнаружения и исключения кольцевых маршрутов образуется иерархическое дерево без петель, однако альтернативные пути по-прежнему существуют на случай, если они понадобятся. Использующийся для обнаружения и предотвращения кольцевых маршрутов протокол известен как *протокол распределенного связующего дерева (Spanning Tree Protocol — STP*); он использует в своей работе модули BPDU. В результате использования этого протокола создается режим работы коммутаторов и маршрутизаторов, который называется *режимом с предотвращением кольцевых маршрутов.*

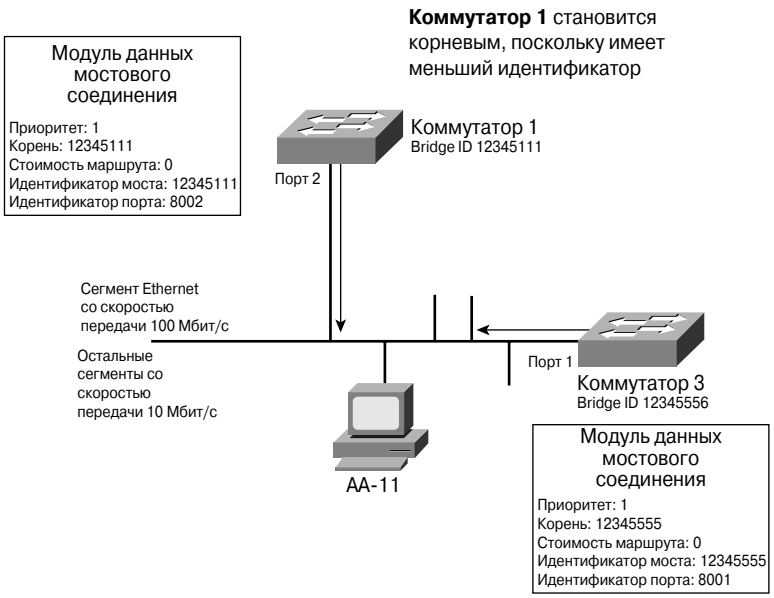


Рис. 8.11. Взаимодействие устройств посредством сообщений BPDU

Порты коммутаторов могут находиться в одном из следующих пяти режимах работы:

- **блокировка (Blocking)**. Порт в этом состоянии отправляет и прослушивает BPDU-сообщения, но не пересылает фреймы. В момент включения устройства все порты стандартно находятся в режиме блокировки;
- **прослушивание (Listening)**. Порт прослушивает BPDU-сообщения, чтобы убедиться в отсутствии кольцевых маршрутов в сети. Фреймы в этом состоянии не передаются;
- **самообучение (Learning)**. В этом состоянии коммутатор изучает MAC-адреса устройств и строит адресную таблицу. Фреймы не передаются;
- **передача (Forwarding)**. В этом состоянии порт передает и принимает пользовательские фреймы. BPDU-сообщения прослушиваются и передаются;
- **отключен (Disabled)**. Порт в этом состоянии не участвует в работе протокола STP. Такое состояние означает, что фреймы не передаются и BPDU-сообщения не прослушиваются.

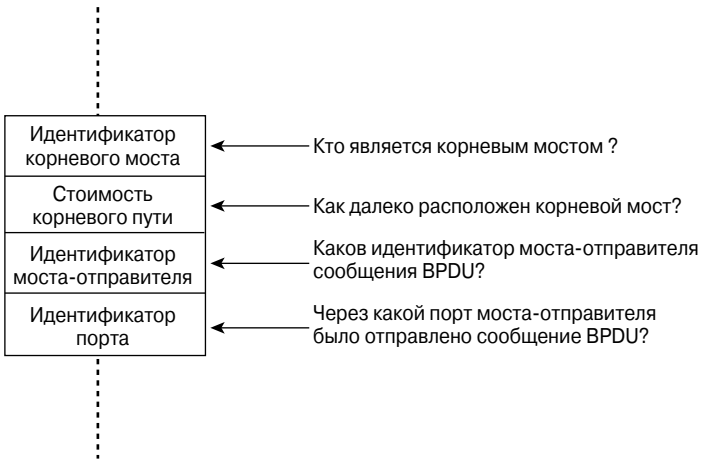


Рис. 8.12. Структура сообщений BPDU

На рис. 8.13 показаны некоторые из состояний портов и режимов работы в коммутируемой сетевой среде с использованием протокола STP (подробнее протокол STP рассматривается во втором томе книги).

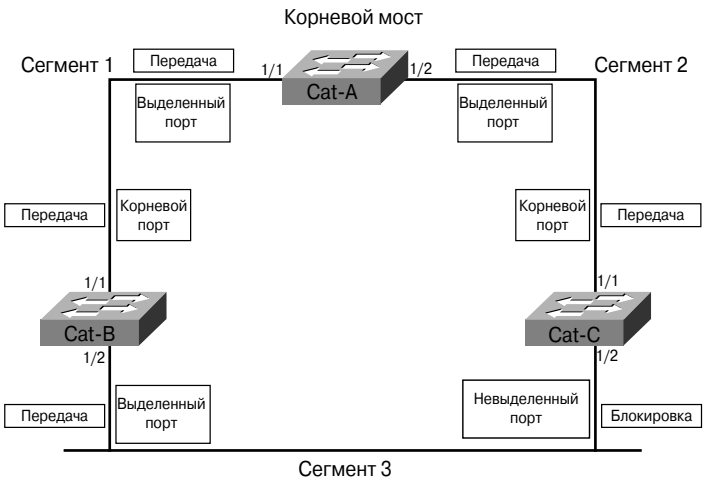


Рис. 8.13. Состояния портов в алгоритме распределенного связующего дерева

Широковещательные домены и домены коллизий

В этом разделе рассмотрены вопросы, относящиеся к коллизионным и широковещательным доменам. Избыточное широковещание и коллизии могут отрицательно повлиять на эффективность работы сети. Здесь обсуждаются способы уменьшения такого неблагоприятного воздействия широковещания коллизий. В разделе дается определения *сегмента* и рассматриваются различные типы сегментации.

Разделяемые сетевые среды

Для того чтобы понять, что представляет собой домен коллизий, необходимо сначала рассмотреть вопрос о том, что такое коллизии и чем они вызываются. Для объяснения понятия коллизии целесообразно рассмотреть передающую среду на первом (физическом) уровне и различные топологии сетей.

Как видно на рис. 8.14, имеются несколько различных типов непосредственного соединения сетей, когда они образуют общую разделяемую среду.

- **Совместно используемая среда передачи**. Такой способ соединения сетей возникает, когда все устройства имеют доступ к одной и той же среде передачи. Например, если несколько персональных компьютеров подсоединены к одному и тому же проводу, оптоволоконному кабелю или совместно используют одно и то же воздушное пространство, то они совместно используют общую для них среду передачи. В этом случае говорят, что они находятся в одном и том же домене коллизий. Другим примером общей передающей среды могут служить Ethernet-сети с общей шиной на основе коаксиального кабеля и Ethernet-сети на основе концентраторов (т.е. использующие кабель UTP).

- **Расширенная среда общего доступа.** Так называют специальный тип среды общего использования, в которой сетевые устройства могут расширить среду, передающую таким образом, что она сможет обеспечивать множественный доступ или предоставлять более длинные кабельные соединения. Расширенная среда общего доступа может быть создана с помощью повторителей или концентраторов. Посредством этой среды создается расширенный домен коллизий.
- **Сетевая среда с двухточечными соединениями**. Такая среда часто используется в удаленных сетевых соединениях и лучше всего знакома домашнему пользователю. Она представляет собой совместно используемую сетевую среду, в которой каждое устройство соединено только с одним другим устройством, например, при соединении компьютера с провайдером служб Internet с помощью модема и телефонной линии. Поскольку соединение "точка-точка" является выделенным и не используется другими устройствами, коллизии в такой среде исключены.

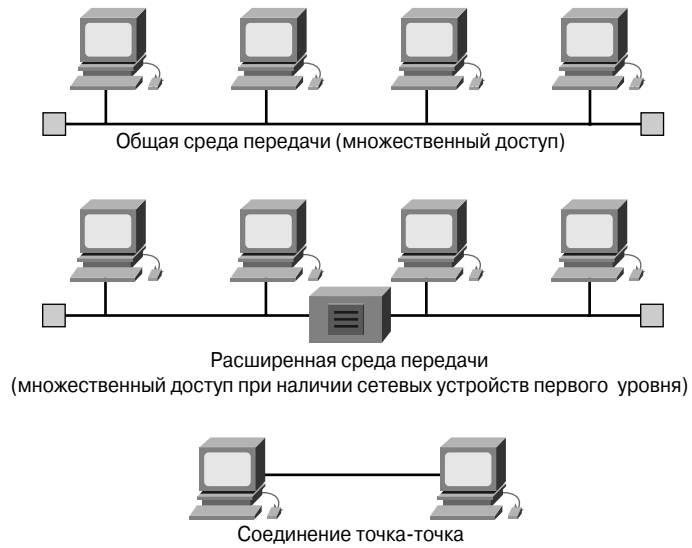


Рис. 8.14. Разделяемая сетевая среда

Дополнительная информация: сети, которые не подключены друг к другу напрямую

Некоторые сети не подсоединены непосредственно друг к другу; это означает, что между двумя осуществляющими связь узлами находятся сетевые устройства более высоких уровней или такие узлы разделены большими расстояниями. На рис. 8.15 также показаны два типа сетей, которые не соединены друг с другом непосредственно. Ниже приводится описание таких сетей.

- **Сети с коммутацией каналов (Circuit-switched**) — сеть без непосредственного соединения, в которой реальные электрические соединения поддерживаются только во время сеанса связи. При использовании технологии коммутации каналов создается сквозное физическое соединение между конечными точками (станциями). При этом вся полоса пропускания

предоставлена этому двухточечному соединению. Нынешняя телефонная система по-прежнему частично использует коммутацию каналов, хотя во многих странах телефонные системы уже в меньшей степени опираются на технологии с коммутацией каналов. Поскольку в таких системах отсутствует совместно используемая среда передачи, коллизии в них невозможны.

- **Сети с коммутацией пакетов**. В таких сетях вместо резервирования целого канала как выделенного соединения между двумя осуществляющими связь узлами отправитель пересылает сообщения в виде отдельных пакетов. Каждый пакет содержит в себе достаточно информации для того, чтобы его можно было доставить получателю. Сети с коммутацией пакетов часто используют общую физическую среду, но, поскольку создаваемые соединения "точка-точка" являются логическими, коллизии в таких сетях также отсутствуют.

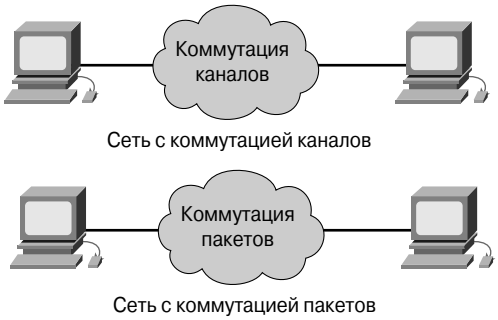


Рис. 8.15. Сети, которые не подключены друг к другу напрямую

Домены коллизий

Следует представлять себе принцип работы среды совместного использования, поскольку совместное использование создает возможность коллизий в сети. Аналогичная ситуация может возникнуть у автомобиля на автотрассе. Если на дороге имеется только один автомобиль, то возможность столкновения, очевидно, исключена. Однако если на той же полосе движения присутствуют другие автомобили, как показано на рис. 8.16, то происходит коллизия. Такая же ситуация возникает в сети.

Под *коллизией* (*collision*) понимается ситуация, в которой два бита одновременно проходят по одной и той же сети. В небольшой и сравнительно медленной сети можно создать систему, в которой отправка сообщений будет разрешена только двум компьютерам поочередно. Проблема возникает в том случае, когда в крупной сети имеется множество компьютеров, каждому из которых требуется регулярно передавать миллионы битов.

Домен коллизий представляет собой совокупность физических сегментов сети, в которой могут произойти столкновения (т.е. одновременная передача) пакетов. Частые коллизии делают работу сети неэффективной. Каждый раз, когда происходит коллизия, передача данных по сети на некоторое время прекращается. Такое время бывает различным и для каждого сетевого устройства определяется специальным алгоритмом; оно необходимо для того, чтобы можно было возобновить передачу информации по разделяемой среде.

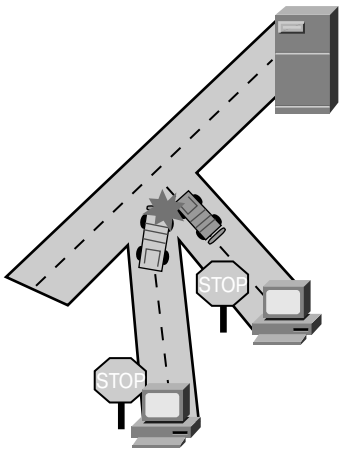


Рис. 8.16. Коллизия

Кроме случая отдельной изолированной LAN-сети технологии Ethernet, границы коллизионных доменов определяются устройствами, которые соединяют между собой сегменты сетевой среды передачи. Такие устройства могут быть классифицированы как устройства первого, второго и третьего уровней эталонной модели OSI. Устройства первогого уровня не могут изолировать друг от друга домены коллизий, в то время как устройства второго и третьего уровней способны это сделать (рис. 8.17). Разбиение коллизионных доменов на несколько более мелких с помощью устройств второго и третьего уровней называется *сегментацией (segmentation*).

Уровень приложений	
Уровень представления	
Сеансовый уровень	
Транспортный уровень	
Сетевой уровень	Делит домен коллизий
Канальный уровень	Делит домен коллизий
Физический уровень	Делит домен коллизий

Рис. 8.17. Сегментация коллизионных доменов

Устройства первого уровня, такие, как повторители и концентраторы, выполняют первичную функцию расширения кабельных сегментов сети Ethernet. При расширении сети возможно добавление новых станций. Однако при добавлении каждой новой станции возрастает потенциально объем передаваемых по сети данных. Поскольку устройства первого (физического) уровня передают далее все, что пересылается по сетевой среде, то чем больше объем данных, передаваемых в коллизионном домене,

тем больше вероятность возникновения коллизии. Конечным результатом расширения сети становится понижение производительности сети, что проявляется особенно остро в том случае, когда всем компьютерам сети требуется широкая полоса пропускания. Проще говоря, устройства первого уровня расширяют домены коллизий, как показано на рис. 8.18, однако длина соединений сети LAN при этом может оказаться слишком большой, что приведет к новым проблемам, связанным с коллизиями.

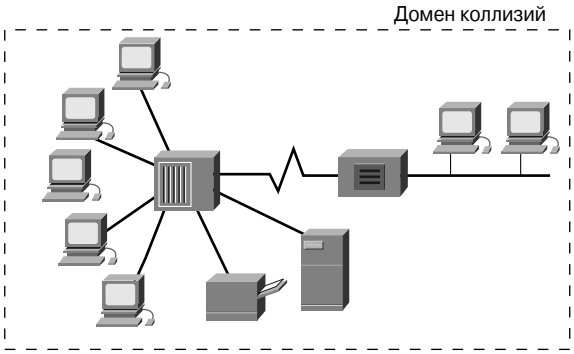


Рис. 8.18. Повторитель расширяет домен коллизий

Так называемое правило четырех повторителей в сетях Ethernet утверждает, что между любыми двумя компьютерами в сети не должно быть более четырех повторителей или концентраторов с функциями повторителя, как показано на рис. 8.19. Для того чтобы сеть технологии 10BASET, в которой используются повторители, эффективно функционировала, суммарная задержка распространения сигнала в прямом и обратном направлениях не должна превышать определенных пределов, в противном случае не все рабочие станции смогут прослушивать коллизии, происходящие в сети.

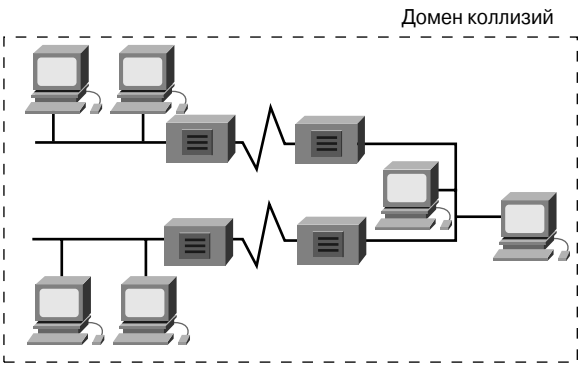


Рис. 8.19. Правило четырех повторителей в сетях Ethernet

Правило четырех повторителей основано на учете всех видов задержки: задержки повторителя, задержки распространения и задержки в сетевом адаптере NIC. Нарушение этого правила может привести к тому, что будет превышен максимально допустимый предел задержки. При его превышении резко возрастает количество запоздалых коллизий (late collisions). Коллизия называется запоздалой, если она происходит уже после передачи первых 64-х байтов фрейма. При возникновении запоздалых коллизий наборы микросхем в адаптере NIC не выполняют автоматически повторную передачу. Такие фреймы коллизии увеличивают задержку, называемую задержкой потребления (consumption delay). По мере возрастания задержки потребления и задержки распространения производительность работы сети падает. Эмпирическое правило работы сети Ethernet известно как правило 5-4-3-2-1. Оно подразумевает, что должны быть выполнены следующие условия:

- сеть, которая содержит повторители, максимум может содержать
  - 5 сегментов сетевой среды передачи;
  - 4 повторителя или концентратора;
  - 3 сегмента сети, в которой могут быть рабочие станции;
- 2 сегмента сети являются соединительными (и не содержат рабочих станций);
- один крупный домен коллизий.

Презентация: коллизии
В этой презентации проиллюстрированы коллизии в сетях со множественным доступом с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access with Collision Detection — CSMA/CS).

Сегментация

Профессионал в сетевой сфере должен уметь выделять в сети отдельные домены коллизий. При подсоединении нескольких компьютеров к сетевой среде, в которой отсутствуют другие сетевые устройства, образуется домен коллизий. Такое подсоединение может быть выполнено для ограниченного количества компьютеров, которые совместно используют общую среду передачи, также называемую сегментом. Как показано на рис. 8.20, устройства первого уровня расширяют домен коллизий, но не управляют им.

Устройства второго уровня делят домен коллизий на несколько доменов меньшего размера; такой механизм также называется сегментацией. Эта функция управления распространением фреймов в сети выполняется на основе MAC-адресов, присущих каждому устройству Ethernet-сети. Устройства второго уровня, такие, как мосты и коммутаторы, регистрируют MAC-адреса устройств и сегменты, в которых они находятся. На основе этой информации они могут управлять передачей данных на втором уровне. Эта функция устройств канального уровня делает работу сетей более эффективной за счет того, что становится возможной одновременная передача данных в разных сегментах LAN-сети без возникновения коллизий. Использование

мостов и коммутаторов позволяет разбить домен коллизий на несколько частей меньшего размера, каждый из которых сам является отдельным доменом коллизий.

В таких доменах меньшего размера будет находиться меньше станций и благодаря этому увеличится полоса пропускания, доступная каждой станции. Чем меньше объем передаваемых в сегменте потоков данных, тем больше вероятность того, что при необходимости для станции передать данные сетевая среда окажется свободной. Это преимущество будет проявляться до тех пор, пока объем межсегментной передачи данных остается небольшим. В противном случае устройство второго уровня может замедлить работу сети и само стать ее "узким местом".

Устройства третьего уровня, как и второго, не пересылают коллизии, которые поступают на один порт, на другой. По этой причине использование в сети устройств третьего уровня также разбивает домен коллизий на домены меньшего размера. Однако устройства третьего, или сетевого, уровня, кроме деления домена коллизий на меньшие, выполняют и иные функции. Эти устройства и выполняемые ими функции рассматриваются более подробно в разделе "Широковещательные домены" этой книги. На рис. 8.21 показаны устройства второго и третьего уровней, которые делят один домен коллизий на домены меньшего размера.

Широковещание на втором уровне

Для обмена данными со всеми доменами коллизий протоколы используют широковещательные и многоадресатные фреймы канального уровня эталонной модели OSI. Если какому-либо узлу требуется обратиться ко всем узлам сети, то он посылает фрейм с адресом получателя, равным 0xFFFFFFFFFFFF (широковещательный адрес). Этот адрес распознается сетевыми адаптерами (NIC) всех устройств сети.

Устройства второго уровня должны передавать все широковещательные и многоадаресатные фреймы методом лавинной рассылки, т.е. передавать их всем устройствам, которые к ним подсоединены. Накопление широковещательных и многоадресатных потоков данных от всех устройств сети иногда называют широковещательной радиацией. На рис. 8.22 показан мост, пересылающий широковещательные фреймы всем устройствам сети.

Поскольку адаптер NIC прерывает работу центрального процессора (CPU) для обработки данных каждого широковещательного домена или группы многоадресатной рассылки, широковещательная радиация отрицательно влияет на производительность устройств сети. Чаще всего оказывается, что для узла обработка широковещательных данных бесполезна, поскольку он не является пунктом назначения. Как правило, этому узлу не требуется объявляемая служба или о ней уже известно. Как показано на рис. 8.23, широковещательная радиация может значительно понизить производительность работы устройств сети. В IP-сетях тремя источниками широковещания и многоадресатных рассылок являются рабочие станции, маршрутизаторы и приложения многоадресатной рассылки.

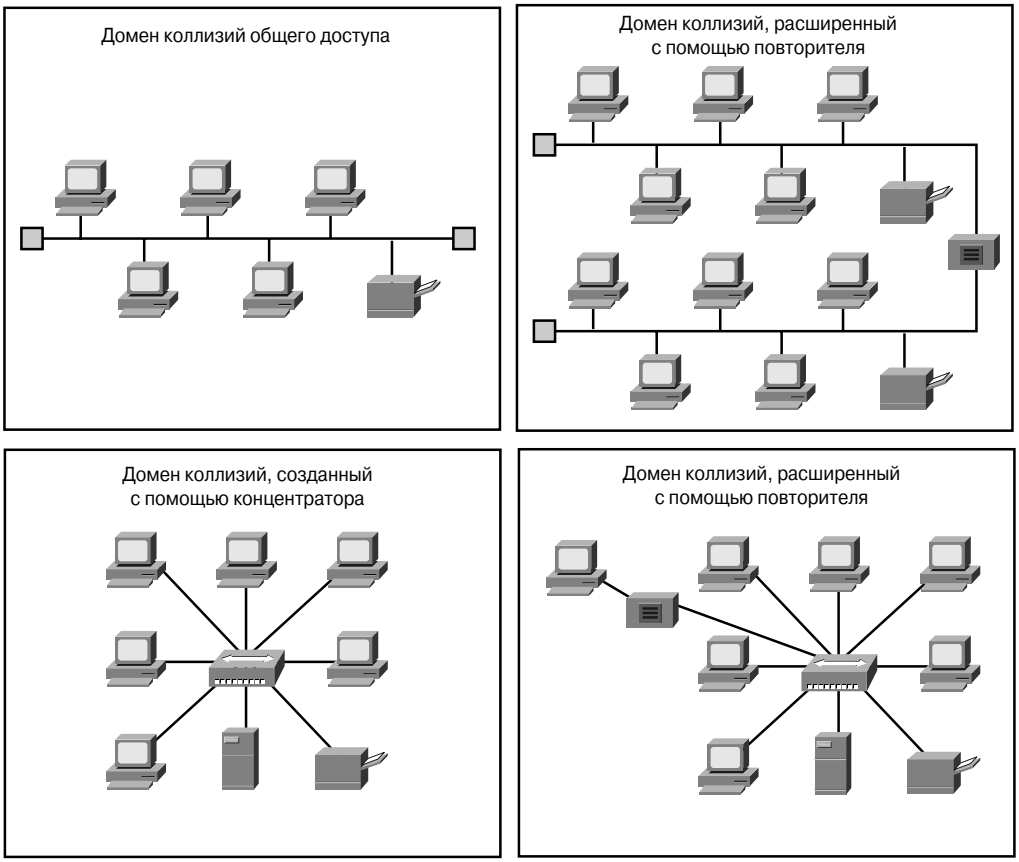


Рис. 8.20. Устройства первого уровня расширяют домены коллизий

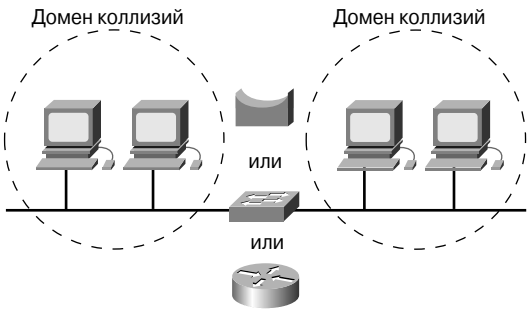


Рис. 8.21. Ограничение размера домена коллизий

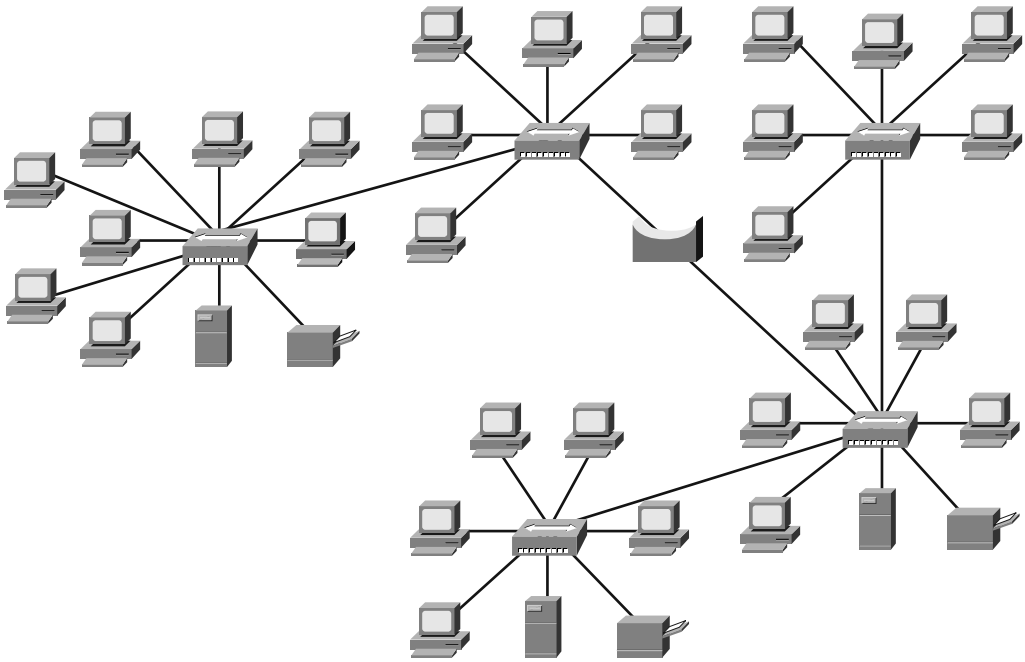


Рис. 8.22. Широковещание на втором уровне

Рис. 8.23. Влияние широковещания на станции IP-сети

Рабочие станции посредством широковещания рассылают запросы протокола преобразования адресов (Address Resolution Protocol — ARP) каждый раз, когда им необходимо найти MAC-адрес, который отсутствует в их ARP-таблицах. Например, команда **`telnet mumble.com`** преобразует MAC-адрес в IP-адрес с помощью системы доменных имен (Domain Name System — DNS), а затем широковещательно рассылает ARP-запрос для нахождения соответствующей станции. По общей оценке рабочая станция протокола IP кэширует от 10 до 100 адресов за каждые 2 часа работы.

Для типичной рабочей станции количество ARP-запросов составляет около 50 адресов за каждые 2 часа работы, т.е. 0,007 ARP-запроса в секунду.

Таким образом, 2000 конечных станций протокола IP создают около 14 ARP-запросов в секунду.

В табл. 8.1 приведены данные о среднем количестве широковещательных и многоадресатных фреймов в IP-сетях.

Таблица 8.1. Среднее количество широковещательных и многоадресатных сообщений в IP-сетях

Количество узлов	Средний процент потерь времени центрального процессора на одном узле
100	0,14
1000	0,96
10000	9,15

Хотя значения, приведенные в табл. 8.1, могут показаться относительно небольшими, однако они представляют значения лишь средней, рационально спроектированной IP-сети, в которой не используется протокол маршрутной информации (Routing Information Protocol — RIP). В тех случаях, когда объемы широковещательной передачи и многоадресатной рассылки достигают пиковых значений, потери времени работы процессора (CPU) могут превышать приведенные в таблице средние значения в десятки раз. Широковещательные штормы могут быть вызваны устройством, запрашивающим информацию у сети, которая стала слишком большой. При этом на первоначальный запрос может поступить так много ответов, что посылавшее его устройство не сможет их обработать; возможна также ситуация, когда первый запрос вызывает аналогичные запросы от других устройств, которые фактически блокируют нормальное перемещение потоков данных по сети.

IP-маршрутизатором является маршрутизатор или рабочая станция, на которой работает какой-либо дистанционно-векторный протокол. Некоторые сетевые администраторы конфигурируют на всех станциях протокол RIP (протокол маршрутизации) в качестве надежного средства, обеспечивающего резервирование и достижимость всех станций. Протокол RIP каждые 30 секунд рассылает широковещательные сообщения, содержащие всю таблицу его маршрутизации, всем остальным RIP-маршрутизаторам. Если в сети протокол RIP сконфигурирован на большом количестве маршрутизаторов и в среднем требуется 50 пакетов для передачи таблицы маршрутизации, то такие маршрутизаторы будут генерировать 3333 широковещательных пакета каждую секунду. Большинство сетевых администраторов конфигурирует протокол RIP лишь на небольшом количестве устройств — обычно от 5 до 10. В этом случае при среднем размере таблицы маршрутизации в 50 пакетов десять RIP-маршрутизаторов будут генерировать 16 широковещательных пакетов в секунду (протоколы маршрутизации и таблицы маршрутизации обсуждаются в главе 10, “Основы маршрутизации и принципы построения подсетей”).

Хотя многоадресатная рассылка является эффективным способом передачи потоковых мультимедийных данных большому количеству пользователей с помощью концентратора в совместно используемой среде, она оказывает неблагоприятное

воздействие на работу каждого пользователя в линейной коммутируемой сети. Под линейной коммутируемой сетью понимается сеть, состоящая из соединенных между собой коммутаторов, которая не использует маршрутизацию третьего уровня или аналогичные механизмы пересылки данных. Отдельное пакетное видеоприложение может генерировать поток данных многоадресатной рассылки объемом до 7 Мбайт, который в коммутируемой сети будет разослан во все сегменты, что неминуемо приведет к сильной перегрузке.

Широковещательные домены

Под *широковещательным доменом (broadcast domain*) понимается группа доменов коллизий, которые соединены между собой с помощью устройств второго (канального) уровня. Разбиение сети LAN на несколько доменов коллизий повышает эффективность работы сети за счет того, что становится возможной одновременная передача данных в отдельных доменах коллизий. Однако широковещательные потоки данных проходят через устройства второго уровня и, если их объем велик, могут уменьшить эффективность работы всей LAN-сети. Управление широковещанием должно происходить на третьем уровне, поскольку устройства двух нижних уровней такой возможности не имеют. Общий размер широковещательного домена может быть определен путем объединения всех доменов коллизий, которые обрабатывают поступивший в один из таких доменов широковещательный фрейм. Иными словами, широковещательный домен включает в себя все узлы сетевого сегмента, ограниченного устройствами третьего (сетевого) уровня. Широковещательные домены управляются на сетевом уровне, поскольку маршрутизаторы не пересылают широковещательные фреймы. Так, например, изображенный на рис. 8.24 маршрутизатор не будет пересылать широковещательные фреймы от рабочей станции, которая выделена цветом, в левой части рисунка, станциям, расположенным справа.

В действительности маршрутизаторы работают на первом, втором и третьем уровнях эталонной модели OSI. Как и все устройства первого уровня, они подсоединены к физической передающей среде и пересылают через нее данные. Функции третьего уровня позволяют маршрутизатору сегментировать широковещательные домены.

Для того чтобы пакет был переслан через маршрутизатор, он должен быть сначала обработан на втором (канальном) уровне и из него должна быть удалена информация уровня фрейма (заголовок и концевик второго уровня). Пересылка на третьем уровне основана не на MAC-адресе, а на IP-адресе получателя. Для того чтобы маршрутизатор переслал пакет, необходимо, чтобы последний содержал IP-адрес, лежащий вне диапазона адресов, назначенных данному сегменту сети LAN, а в таблице маршрутизации маршрутизатора имелся адрес получателя, которому предназначен этот пакет.

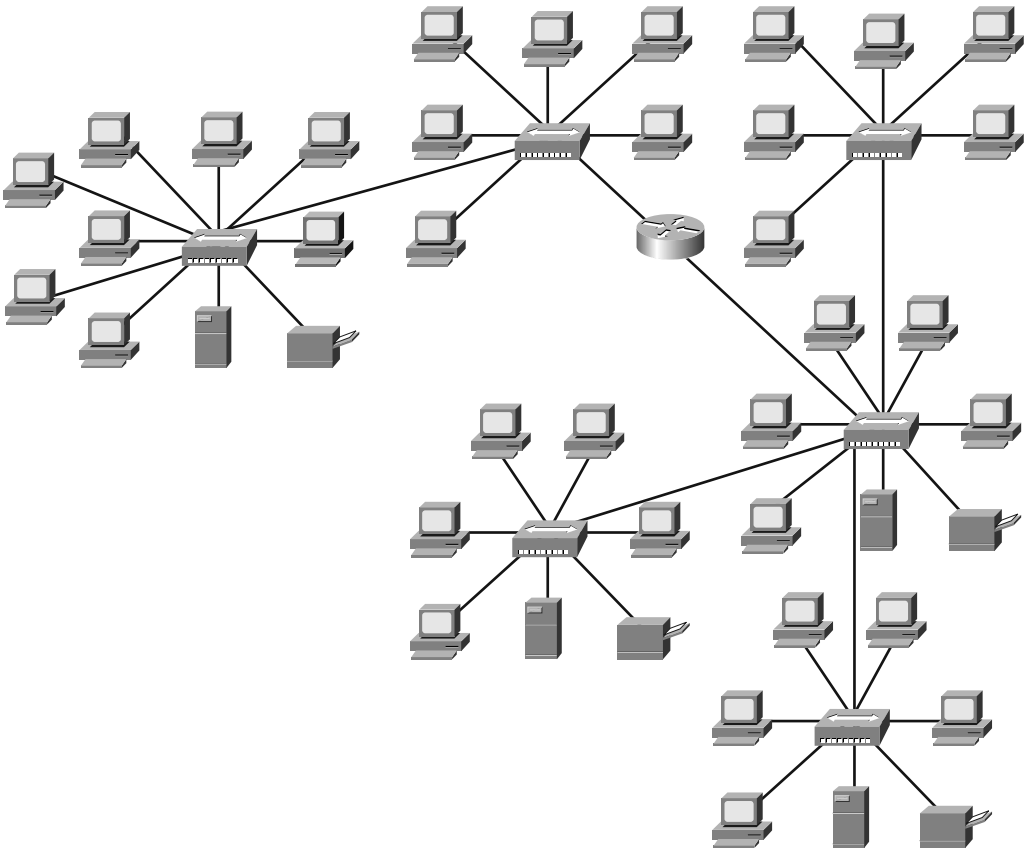


Рис. 8.24. Сегментация широковещательного домена

Потоки данных

Понятие потока данных в контексте коллизионных и широковещательных доменов относится к распространению данных по сети. Оно связано с прохождением данных через устройства первого, второго и третьего уровней, а также к способу инкапсуляции данных, который должен обеспечить их пересылку по сети получателю. Следует помнить о том, что на сетевом уровне данные инкапсулируются в заголовок, который содержит IP-адреса отправителя и получателя, а на канальном уровне — MAC-адреса отправителя и получателя. В целом работу сетевых устройств можно описать следующим образом: устройства первого уровня всегда пересылают фрейм, устройства второго уровня пытаются сделать это (т.е. пересылают, если нет причин, препятствующих этому), а устройства третьего уровня пересылают информацию при наличии достаточных причин. Это правило позволяет понять, как именно потоки данных перемещаются по сети.

Устройства первого уровня (повторители и концентраторы) не выполняют фильтрацию, поэтому все полученные данные передаются в следующий сегмент. Эти устройства лишь регенерируют и повторно синхронизируют фрейм и таким образом возвращают ему первоначальное качество для последующей передачи. Все сегменты, подсоединенные к устройству первого уровня, являются частями одного и того же широковещательного домена и домена коллизий.

Устройства второго уровня (мосты и коммутаторы) фильтруют данные на основе их MAC-адресов. Фрейм пересылается, если его пункт назначения расположен вне данного домена коллизий. Фреймы также пересылаются, если они являются широковещательными, многоадресатными или однодресатными, но направляемыми вовне данного домена коллизий. Единственный случай, когда фрейм не пересылается в соседние домены, — когда и станция-отправитель, и станция-получатель находятся в одном и том же домене коллизий. Устройство мостового типа (которое работает на втором уровне) создает несколько доменов коллизий, однако поддерживает только один широковещательный домен.

Устройства третьего уровня (маршрутизаторы и некоторые другие, появившиеся в последнее время) фильтруют пакеты данных на основе IP-адресов получателей. Единственный случай, когда пакет пересылается, — когда IP-адрес пакета лежит вне данного широковещательного домена и маршрутизатору известно расположение пункта назначения, в который требуется переслать пакет. Устройства третьего уровня создают несколько широковещательных доменов и доменов коллизий.

Поток данных, проходящий по IP-сети, содержит данные, которые перемещаются через устройства управления передачей на первом, втором и третьем уровнях эталонной модели OSI. Первый уровень отвечает за передачу данных по физической среде, второй уровень отвечает за управление передачей с учетом коллизионных доменов, а третий уровень управляет пересылкой данных через множество широковещательных доменов. На рис. 8.25 показано перемещение потока данных от рабочей станции X через маршрутизаторы А, Б и В к рабочей станции Y.

Сетевые сегменты

Как и многие другие сетевые термины и аббревиатуры, термин *сегмент (segment)* имеет несколько значений. В толковом словаре дается следующее его определение:

- отдельная часть чего-либо;
- одна из частей, на которые подразделяется/размечается некоторый объект или величина естественными либо подразумеваемыми границами.

В контексте передачи данных используются следующие определения термина *сегмент*:

- область сети, ограниченная мостами, маршрутизаторами или коммутаторами;
- в LAN-сетях, использующих шинную топологию, под сегментом подразумевается непрерывная электрическая цепь, которая часто подсоединена к другим таким же сегментам с помощью повторителей;

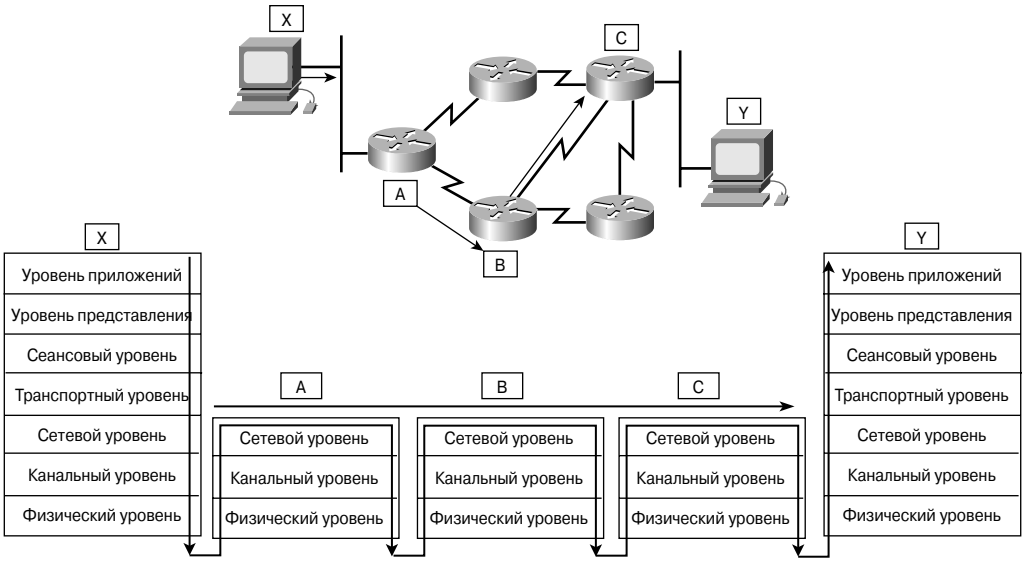


Рис. 8.25. Прохождение потока данных по сети

- в спецификации протокола TCP термин *сегмент* используется для описания отдельного информационного модуля транспортного уровня;
- для описания логических информационных модулей на различных уровнях эталонной модели OSI и на разных стадиях процесса передачи данных также используются такие понятия, как *дейтаграмма*, *фрейм*, *сообщение* и *пакет*.

На рис. 8.26 проиллюстрированы три определения термина *сегмент* в контексте передачи данных.

Чтобы дать правильное определение термина, необходимо учитывать контекст, в котором он употреблен. При использовании этого термина в контексте протокола TCP он означает отдельную порцию данных. Если же он используется в контексте физической сетевой среды, в которой есть маршрутизаторы, то подразумевается часть или область всей сети.

Интерактивная презентация: различные типы сегментов
В этой презентации разъяснены различные значения термина *сегмент*.

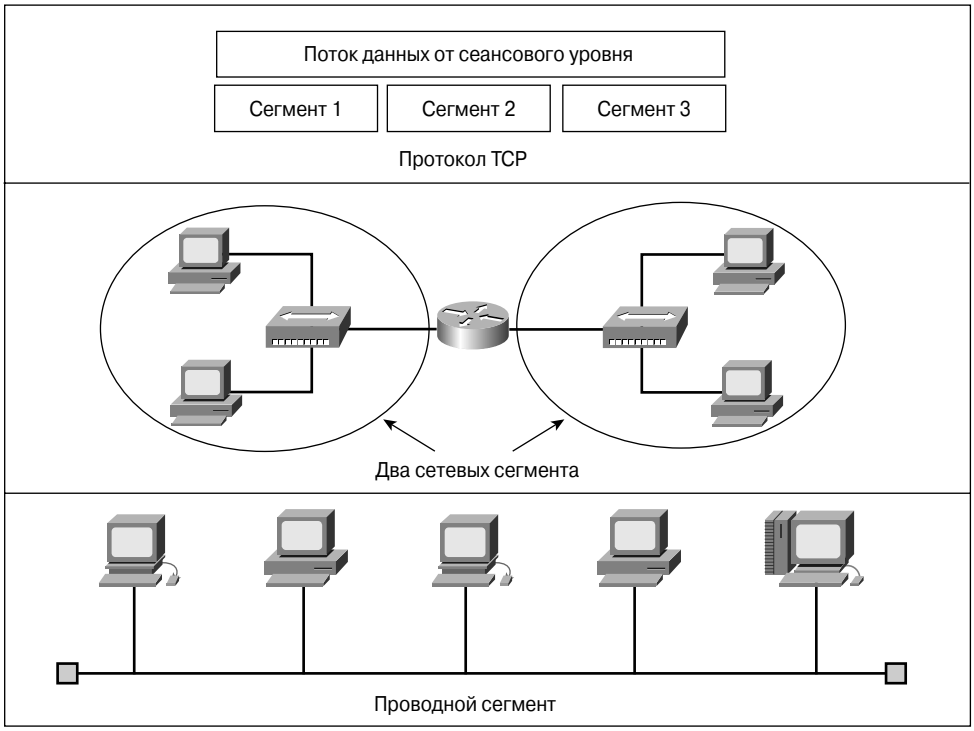


Рис. 8.26. Сегменты

Резюме

В этой главе были рассмотрены следующие ключевые понятия:

- коммутаторы предоставляют выделенную полосу пропускания к инфраструктуре, что совершенствует технологию сетей с разделяемым доступом;
- коммутатор делит локальную сеть на микросегменты. Микросегментация сводит количество коллизий к минимуму и повышает эффективную пропускную способность;
- коммутаторы позволяют достичь высокой скорости передачи и строят таблицу коммутации посредством определения MAC-адресов отправителей во фрейме;
- дуплексный режим передачи позволяет двум устройствам одновременно взаимодействовать друг с другом, что позволяет эффективно удвоить пропускную способность коммутатора локальной сети;
- коммутаторы могут поддерживать множество одновременных диалогов в сети;
- в коммутаторах для передачи фреймов могут использоваться три режима коммутации: с промежуточным хранением, сквозной и бесфрагментный;

- основная задача протокола распределенного связующего дерева состоит в том, чтобы предотвратить появление кольцевых маршрутов в сети на втором уровне;
- порты в мостах или коммутаторах находятся в одном из пяти состояний: “блокировка”, прослушивание”, “самообучение”, “передача” и “отключен”;
- базовой совокупностью устройств в совместно используемой среде передачи является домен коллизий. Домены коллизий могут быть сегментированы, для того чтобы уменьшить вероятность заторов и повысить эффективность работы сети;
- домены коллизий могут быть сегментированы с помощью устройств второго и третьего уровней;
- широковещательные сообщения предназначаются для всех устройств всех доменов коллизий и могут отрицательно повлиять на эффективность работы сети;
- для сегментации широковещательных доменов используются устройства третьего уровня.

Для закрепления материала воспользуйтесь относящимися к главе интерактивными материалами, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в данной главе.

Ключевые термины

Задержка — интервал времени между моментом получения фрейма устройством и моментом, когда фрейм пересылается через порт назначения.

Домен коллизий (collision domain). В сетях Ethernet — это область сети, в которой распространяются фреймы, претерпевшие коллизию. Повторители и концентраторы распространяют коллизии, а коммутаторы, мосты LAN-сетей и маршрутизаторы останавливают их.

Коллизия (collision). В сетях Ethernet коллизия представляет собой результат одновременной передачи данных двумя узлами. При встрече в физической среде отправленные этими устройствами фреймы сталкиваются и повреждаются. См. также *домен коллизий (collision domain).*

Микросегментация (microsegmentation) представляет собой деление сети на более мелкие сегменты для увеличения суммарной пропускной способности сетевых устройств.

Модуль данных мостового протокола (Bridge Protocol Data Unit — BPDU) представляет собой специальное сообщение, используемое в протоколе STP и рассылаемое через определенные интервалы времени для обмена информацией между мостами в сети.

Протокол распределенного связующего дерева (STP — Spanning Tree Protocol) представляет собой используемый в мостах и коммутаторах протокол, в котором задействован алгоритм связующего дерева для обеспечения динамического самообучения мостов и предотвращения образования кольцевых маршрутов. Мосты обмениваются BPDU-сообщениями, которые позволяют обнаружить кольцевые маршруты и устранить их посредством отключения отдельных интерфейсов.

Режим бесфрагментной коммутации (Fragment-free switching) — это режим коммутации, при котором перед пересылкой фреймов фильтруются фрагменты коллизий, являющиеся основным источником ошибок в сети.

Режим коммутации с промежуточным хранением (Store-and-forward switching) — это техника коммутации, при которой фрейм перед пересылкой в порт назначения полностью записывается в память устройства и обрабатывается. Обработка включает в себя подсчет контрольной суммы и проверку адреса получателя. Дополнительно фрейм должен быть временно сохранен до тех пор, пока сетевые ресурсы (например, канал) не станут доступны для пересылки фрейма.

Режим сквозной коммутации (Cut-through switching). Устройства, использующие этот метод коммутации, читают, обрабатывают и пересылают фреймы сразу после того, как будет прочитан адрес получателя и определен порт назначения. См. также *режим коммутации с промежуточным хранением*.

Сегмент (segment) — это часть сети, ограниченная мостами, маршрутизаторами или коммутаторами.

Широковещание (Broadcast) — это рассылка пакетов сразу всем узлам сети. Широковещательная передача характеризуется наличием широковещательных адресов в поле адреса получателя.

Широковещательный домен (broadcast domain) — это совокупность всех устройств, которые получают широковещательные фреймы от любого из устройств этой совокупности. Границы широковещательного домена обычно определяются маршрутизаторами (или, в коммутируемых сетях, виртуальными сетями VLAN), поскольку маршрутизаторы не пересылают широковещательные фреймы.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Какой из предложенных ниже вариантов *не является* следствием микросегментации?

а) Предоставляет выделенный доступ.
б) Поддерживает множество одновременных диалогов.
в) Увеличивает полосу пропускания для каждой подключенной к сети рабочей станции.
г) Увеличивает количество коллизий.

2. Что из указанного ниже используется коммутатором для принятия решения о пересылке фрейма?

а) IP-адрес.

б) MAC-адрес.

в) Сетевой адрес.

г) Адрес узла.

3. Какое из перечисленных свойств присуще дуплексному режиму передачи?

а) Позволяет передавать данные на скоростях 10 и 1 Гбит/с.

б) Вдвое увеличивает пропускную способность соединения между узлами.

в) Обеспечивает передачу данных без коллизий.

г) Все вышеперечисленное.

4. Тремя общими режимами коммутации являются _____, _____ и _____.

5. Что из перечисленного ниже позволяет выполнить протокол STP?

а) Позволяет мостам обмениваться информацией третьего уровня.

б) Позволяет создавать резервные сетевые маршруты без риска возникновения петель.

в) Позволяет обеспечить статический сетевой путь передачи данных для предотвращения петлевых маршрутов.

г) Ничего из вышеперечисленного.

6. Что из перечисленного ниже *не является* состоянием STP-порта?

а) Блокировка.

б) Самообучение.

в) Прослушивание.

г) Транспортировка.

7. Какое из утверждений относится к мостам и описывает принятие решения о пересылке?

а) Мосты работают на втором уровне эталонной модели и используют IP-адреса для принятия решения о пересылке данных.

б) Мосты работают на третьем уровне эталонной модели и используют IP-адреса для принятия решения о пересылке данных.

в) Мосты работают на втором уровне эталонной модели и используют MAC-адреса для принятия решения о пересылке данных.

г) Мосты работают на третьем уровне эталонной модели и используют MAC-адреса для принятия решения о пересылке данных.

8. Какая функция из указанных ниже является функцией мостов?

а) Мосты работают на втором уровне эталонной модели OSI.

б) Мосты являются более “интеллектуальными” устройствами, чем концентраторы.

в) Мосты не принимают решений о перенаправлении потоков данных.

г) Мосты создают и поддерживают таблицы адресов.

9. Какое из указанных ниже утверждений правильно описывает микросегментацию?

а) Каждой рабочей станции предоставляется собственный выделенный виртуальный сегмент в сети.

б) Все рабочие станции сгруппированы в один сегмент.

в) Микросегментация увеличивает количество коллизий в сети.

г) Ни одно из утверждений не верно.

10. Что из указанного ниже правильно описывает коммутаторы локальных сетей?

а) Они восстанавливают сетевые фрагменты, которые называются микросегментами.

б) Коммутаторы — это выскокоскоростные многопортовые мосты.

в) Коммутаторы уменьшают полосу пропускания, что приводит к увеличению задержки в сети.

г) Они требуют установки новых сетевых интерфейсов в подключенных к ним узлах.

11. Как называется область сети, в которой два или более узла соединенные посредством Ethernet-линий, разделены мостом или коммутатором второго уровня и в которой были созданы и претерпели коллизию фреймы?

а) Домен коллизий.

б) Сетевой домен.

в) Широковещательный домен.

г) Сетевой сегмент.

12. Использование повторителей _____коллизионный домен.

а) Уменьшает.

б) Не оказывает влияния.

в) Расширяет.

г) Ничто из вышеперечисленного.

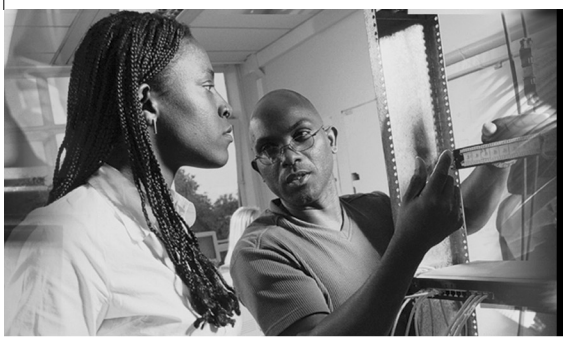
13. Процесс использования сложных сетевых устройств, таких, как мосты, коммутаторы или маршрутизаторы, для разбиения коллизионного домена называется _____.

а) Разбиением на секции.

б) Сегментацией.

в) Уменьшением домена коллизий.

г) Ничто из вышеперечисленного.



ГЛАВА 9

Стек протоколов TCP/IP и IP-адресация

В этой главе...

- дано описание компонентов модели TCP/IP;
- описаны четыре уровня стека протоколов TCP/IP, порядок их следования и взаимодействие между уровнями;
- описаны функции уровня приложений и перечислены наиболее распространенные сетевые приложения;
- описаны функции транспортного уровня и указаны его основные службы;
- описаны функции Internet-уровня и рассмотрены его основные протоколы;
- описаны функции уровня доступа к сети и перечислены его основные механизмы;
- рассмотрена взаимосвязь набора протоколов TCP/IP и модели OSI;
- приведено объяснение роли каждого компонента IP-сети: IP-адреса, классов IP-адресов, зарезервированного адресного пространства, адресов, используемых в частных сетях, и IP-подсети;
- описано, как для заданной схемы адресации вычислять соответствующие номер и маску подсети с учетом потребностей сети и пользователей;
- приведено объяснение развития схем IP-адресации и необходимости увеличения адресного пространства;
- рассмотрены отличия между адресациями IPv4 и IPv6;
- рассказано о том, какие схемы адресации и форматы адресов будут использоваться в будущем;
- описан метод статической IP-адресации;
- рассмотрен протокол ARP и описан принцип его работы.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

стек протоколов управления передачей и Internet-протокол, с. 438,
Internet-протокол версии 6, с. 440,
уровень приложений, с. 440,
транспортный уровень, с. 442,
Internet-уровень, с. 444,
уровень доступа к сети, с. 445,
точечно-десятичный формат, с. 453,
пять классов IP-адресов, с. 459,
адреса класса A, с. 460,
адреса класса B, с. 461,
адреса класса C, с. 461,
адреса класса D, с. 461,
многоадресатный IP-адрес, с. 462,
адреса класса E, с. 462,
широковещательный адрес, с. 463.

В этой главе рассматривается *стек протоколов управления передачей и Internet-протокол* (*Transmission Control Protocol/Internet Protocol — TCP/IP*). Прежде всего будет описана история и этапы развития стека протоколов TCP/IP. Далее будет приведено сравнение модели протоколов TCP/IP и стандартной модели взаимодействия открытых систем (OSI), а также подробно описаны и проанализированы все уровни стека протоколов TCP/IP и их взаимосвязь со структурой сети Internet.

В главе также подробно анализируется тема IP-адресации. Мы расскажем, как преобразовать двоичные адреса в десятичные и каким образом различить классы IP-адресов: классы A, B, C, D и E. На смену протоколу IPv4 (Internet-протокол версии 4), долгие годы являвшемуся стандартом адресации, приходит намного более совершенная схема под названием IPv6 (Internet-протокол версии 6). В этой главе дается описание и сравнение обоих протоколов IPv4 и IPv6.

В процессе изучения материала главы рекомендуется также обратить внимание на дополнительные материалы, которые связаны с рассматриваемыми темами: электронные лабораторные работы (e-Lab), мультимедийные презентации (PhotoZoom). Их можно найти на прилагаемом к книге компакт-диске. Упражнения помогут закрепить теоретический материал, изложенный в главе.

Введение в TCP/IP

Сеть Internet разрабатывалась как общая телекоммуникационная сеть, основная задача которой — выстоять в случае войны. Несмотря на то что эта сеть развивалась и продолжает развиваться совсем не так, как представляли себе ее создатели, сегодня она работает, как и многие годы назад, на основе стека протоколов TCP/IP. Структура и принцип построения протокола набора TCP/IP обеспечивает децентрализацию

и уровень устойчивости, которые требуются от современных распределенных сетей, таких, например, как сеть Internet. Многие из использующихся сегодня протоколов были разработаны в рамках четырехуровневой модели TCP/IP.

Специалисту будет полезно знать обе модели: стека протоколов TCP/IP и эталонную модель взаимодействия открытых систем OSI. В каждой модели используется своя собственная структура, которая объясняет, как работает сеть; тем не менее, в обеих моделях есть много общего. Без знания обеих моделей системному администратору может не хватить знаний для того, чтобы понять, как именно работает сеть.

История и развитие стека TCP/IP

Модель стека протоколов TCP/IP, которая схематически проиллюстрирована на рис. 9.1, была разработана Министерством обороны США в процессе создания сети, способной сохранять работоспособность в любых условиях. Чтобы немного прояснить это, представим себе реальный мир с бесчисленным множеством возможных сетевых соединений — медных проводов, оптических кабелей, коротковолновых и спутниковых каналов. Предположим также, что данные непременно должны быть доставлены по назначению вне зависимости от состояния узлов, образующих сеть. Именно такую задачу — гарантировать доставку пакетов в любое время, при любых условиях и в любую точку сети — поставило перед собой Министерство обороны. Решение этой непростой проблемы привело к созданию набора протоколов TCP/IP, впоследствии ставшего стандартом де-факто при построении сети Internet.

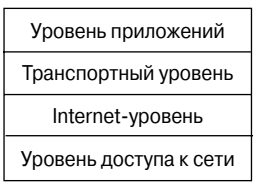


Рис. 9.1. Уровни стека протоколов TCP/IP

В процессе изучения уровней модели TCP/IP не лишним будет вспомнить, для чего изначально разрабатывалась сеть Internet. Такой подход поможет понять, почему соответствующие решения устроены определенным образом. Модель TCP/IP состоит из четырех уровней: уровня приложений (access layer), транспортного уровня (transport layer), уровня Internet и уровня сетевого доступа (network access layer). Стоит отметить, что некоторые из них имеют те же названия, что и уровни в модели OSI. Однако не следует путать назначения уровней в обеих моделях. Номера уровней в них различны, поэтому функции, выполняемые на втором уровне модели OSI, могут отличаться от функций того же уровня модели TCP/IP. Например, в модели OSI третий уровень соответствует протоколу IP, в то время как для модели TCP/IP протокол IP располагается на втором уровне. Еще один пример: протоколы TCP и UDP принадлежат четвертому уровню (транспортному) модели OSI и в то же время соответствуют третьему уровню (транспортному) в модели TCP/IP.

Современная версия стека TCP/IP имеет солидный возраст. Протокол IP версии 4 (IPv4) был стандартизован еще в 1981 году. В 1992 году при поддержке проблемной группы проектирования Internet (Internet Engineering Task Force — IETF) был разработан протокол Internet (IP) нового поколения, часто обозначаемый как IPng (IP next generation — протокол IP следующего поколения). Сейчас аббревиатурой IPng принято обозначать *Internet-протокол версии 6* (IPv6). Протокол IPv6 еще не получил широкого распространения, но уже сегодня его поддержка реализована в продуктах большинства производителей сетевого оборудования (рис. 9.2).

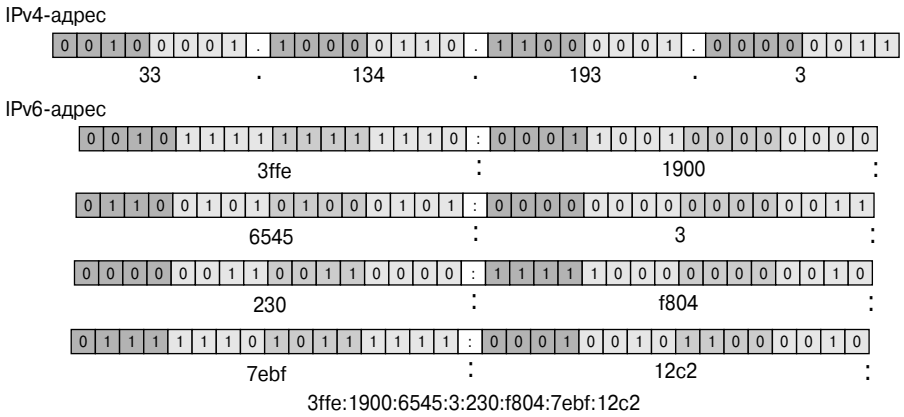


Рис. 9.2. Сравнение протоколов IPv4 и IPv6

Уровень приложений

Модель TCP/IP включает протокол верхнего уровня, использующий сеансовый уровень (session), уровень представления (presentation) и уровень приложений (application) модели OSI. *Уровень приложений*, показанный на рис. 9.3, обслуживает протоколы верхних уровней и решает задачи представления, кодирования данных и контроля взаимодействия между конечными системами.

Набор протоколов TCP/IP решает задачи, связанные с приложениями, и гарантирует, что данные будут надлежащим образом подготовлены для использования на следующем уровне. Стандарт TCP/IP описывает спецификации не только для средств Internet-уровня и транспортного уровня (например, таких, как протоколы IP и TCP), но также и правила разработки общих пользовательских приложений. В набор TCP/IP входят протоколы для передачи файлов, электронной почты и удаленной регистрации, а также приложения, перечисленные ниже.

- **Протокол передачи гипертекстовых файлов (Hypertext Transfer Protocol — HTTP)** — это базовый протокол для работы Web-служб. Протокол HTTP описывает способы передачи и формат сообщений, а также регламентирует действия Web-серверов и браузеров в ответ на различные команды.

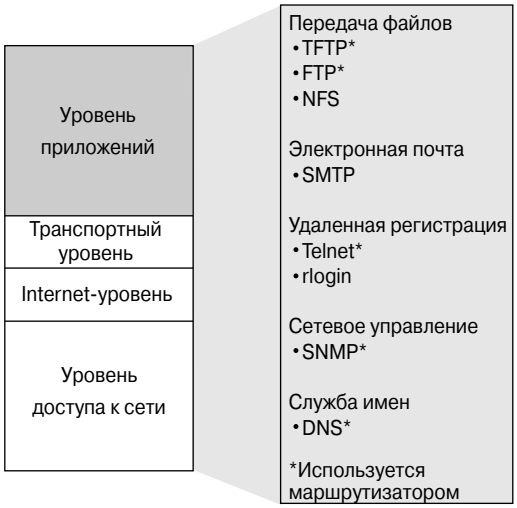


Рис. 9.3. Протоколы уровня приложений модели TCP/IP

- **Простейший протокол передачи файлов (Trivial File Transfer Protocol — TFTP)** — это служба без установления соединения, использующая протокол пользовательских дейтаграмм (протокол UDP). Эта служба используется в маршрутизаторах для передачи конфигурационных файлов и образов операционной системы Cisco IOS, а также для передачи файлов между системами, поддерживающими протокол TFTP. Этот протокол бывает полезен в локальных сетях, поскольку в стабильных условиях работает быстрее, чем протокол FTP.
- **Протокол передачи файлов (File Transfer Protocol — FTP)** — надежная служба, которая работает с установлением соединения и использует протокол TCP для передачи файлов между системами, поддерживающими протокол FTP. Этот протокол обеспечивает двунаправленный обмен как бинарными файлами, так и файлами в тестовом формате ASCII[1].
- **Сетевая файловая система (Network File System — NFS)** — набор протоколов распределенной файловой системы, позволяющий предоставлять удаленный доступ к файлам по сети. Разработан компанией Sun Microsystems.
- **Простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP)** — это служба, которая управляет передачей сообщений по электронной почте в компьютерных сетях и поддерживает передачу только текстовых данных.
- **Стандартный протокол виртуального терминала (telnet)** — это служба, которая предоставляет удаленный доступ к компьютеру. Позволяет пользователям регистрироваться на Internet-узлах и выполнять команды операционной

[1] *American standard code for information interchange — американский стандартный код обмена информацией. — Прим. ред.*

системы. Telnet-клиент называется локальным узлом, а Telnet-сервер — удаленным.

- **Простой протокол управления сетью (Simple Network Management Protocol — SNMP)** — это протокол, предоставляющий средства мониторинга и контроля над сетевыми устройствами, механизмы управления конфигурацией, статистическими данными, производительностью и безопасностью.
- **Служба доменных имен (Domain Name System — DNS)** — это служба, используемая в сети Internet для преобразования доменных имен открытых сетевых узлов в IP-адреса.

Транспортный уровень

Транспортный уровень, как следует из его названия, предоставляет транспортные услуги от узла отправителя к узлу получателя. Он поддерживает логическое соединение между конечными точками сетевого маршрута. Транспортный протокол, который показан на рис. 9.4, сегментирует (т.е. разбивает на блоки) данные, отправленные приложениями верхнего уровня, формируя таким образом трафик между конечными узлами. Поток данных транспортного уровня предоставляет сквозные транспортные услуги (т.е. из одного конца сети в другой) вдоль всего маршрута.

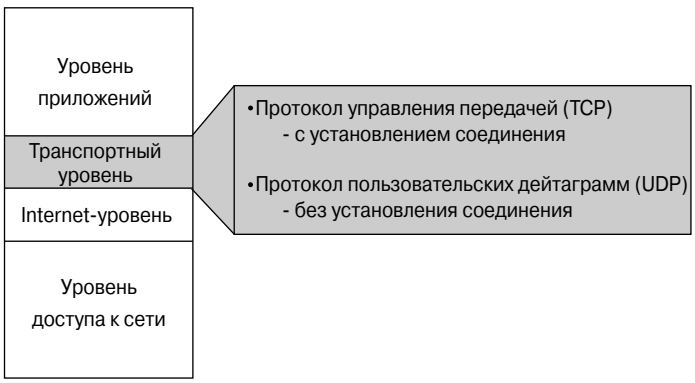


Рис. 9.4. Протоколы транспортного уровня модели TCP/IP

Поток данных транспортного уровня использует логическое соединение между передающим и принимающим узлами сети. При использовании протокола UDP основной задачей транспортного уровня является негарантированная доставка данных от отправителя получателю. Протокол транспортного уровня TCP гарантирует контроль над сквозной передачей благодаря применению метода скользящего окна с использованием последовательной нумерации и подтверждений. Транспортный уровень организует сквозную связь между приложениями, выполняемыми на удаленных системах. Транспортные механизмы, которые используют протокол TCP, включают все из перечисленных ниже служб, в то время как приложения, использующие протокол UDP, предоставляют только первые две службы.

Службы протокола TCP:

- сегментация данных от приложений верхнего уровня;
- передача сегментов от одного конечного устройства другому;
- установление двунаправленного взаимодействия;
- контроль потока с использованием метода скользящего окна;
- гарантированная доставка, которая обеспечивается использованием последовательной нумерации и подтверждений.

Транспортный уровень предполагает, что он может использовать всю сеть как единую среду передачи, пересылая пакеты данных от отправителя конечному получателю, как это показано на рис. 9.5. Вопросы о том, какому из нескольких возможных маршрутов отдать предпочтение, для заданного получателя решаются на уровне сетевой среды (рис. 9.6).

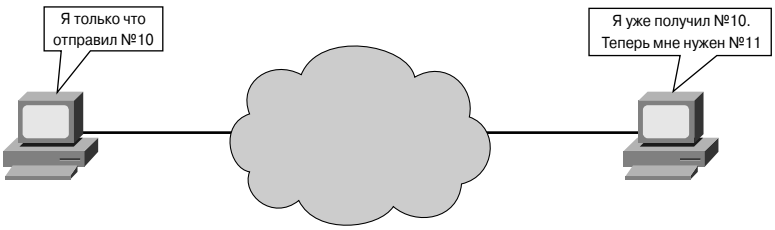


Рис. 9.5. Сетевая среда Internet

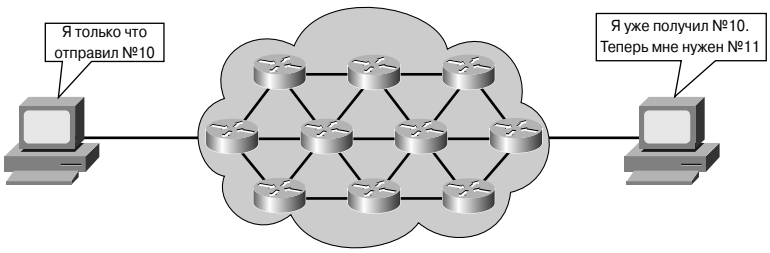


Рис. 9.6. Маршруты в сети Internet

Internet-уровень

В модели OSI сетевой уровень управляет сетевыми соединениями и освобождает протоколы более высоких уровней от необходимости непосредственного взаимодействия с физической инфраструктурой сети. Протокол IP обычно называют сетевым уровнем модели TCP/IP. Поскольку сетевой уровень стека TCP/IP в первую очередь отвечает за межсетевое взаимодействие, его часто называют *Internet-уровнем* модели TCP/IP (рис. 9.7). Протокол IP задействован во всех процессах взаимодействия верхних и нижних уровней, поскольку обычно они задействуют весь стек протоколов TCP/IP. Internet-уровень обеспечивает отправку пакетов сетевыми устройствами

посредством соответствующего протокола. На этом уровне происходит выбор наилучшего маршрута и пересылка пакета. Данный уровень можно сравнить с традиционной почтовой службой: не важно, каким образом письмо достигнет пункта своего назначения (маршруты могут быть разными), главное, чтобы оно было доставлено.

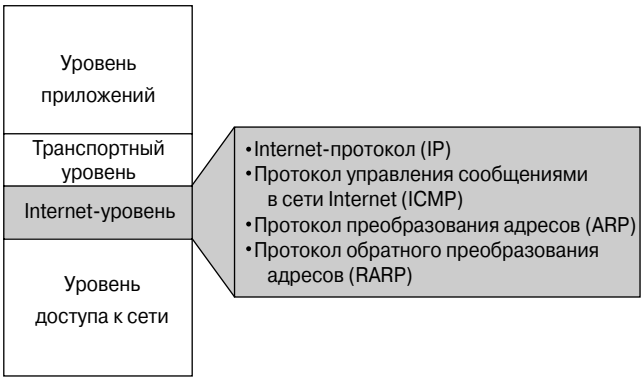


Рис. 9.7. Протоколы Internet-уровня

Перечисленные ниже протоколы работают на Internet-уровне набора TCP/IP.

- **Протокол IP** — это протокол без установления соединения, обеспечивающий выбор наилучшего маршрута для доставки пакетов. Он не заботится о содержимом пакетов, а лишь находит наилучший способ направить пакеты в пункт назначения.
- **Протокол управляющих сообщений в сети Internet (Internet Control Message Protocol — ICMP)** предоставляет функции контроля и управления сообщениями.
- **Протокол преобразования адресов (Address Resolution Protocol — ARP)** определяет адреса канального уровня (MAC-адреса) по известным IP-адресам.
- **Протокол обратного преобразования адресов (Reverse Address Resolution Protocol — RARP)** определяет IP-адреса для известных адресов канального уровня (т.е. MAC-адресов).

Протокол IP выполняет следующие функции:

- определяет формат пакета и схему адресации;
- осуществляет передачу данных от уровня Internet уровню доступа к сети;
- осуществляет маршрутизацию к удаленным узлам.

И, наконец, следует пояснить, почему некоторые разработчики считают, что IP не является надежным протоколом. Это не означает, что протокол не гарантирует доставку данных; имеется ввиду, что протокол IP не осуществляет проверку данных и коррекцию ошибок. Обе функции выполняются на более высоких уровнях: транспортном и уровне приложений.

Уровень доступа к сети

Уровень доступа к сети (рис. 9.8) еще называют уровнем соединения узла и сети. Он "занимается вопросами", связанными с организацией физической связи между IP-пакетами и сетевой средой передачи данных. Этот уровень описывает методы построения локальных (Local Area Network — LAN) и распределенных (Wide Area Network — WAN) вычислительных сетей и соответствует физическому и канальному уровням модели OSI.

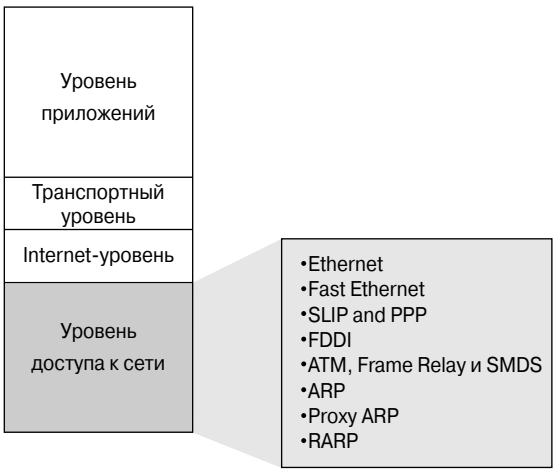


Рис. 9.8. Протоколы уровня сетевого доступа TCP/IP

Программное обеспечение и драйверы специфических устройств, таких, как, сетевые адаптеры (Network Interface Card — NIC) технологий Ethernet, Tocken Ring, ISDN и модемы, обычно работают именно на уровне сетевого доступа. Многие протоколы описываются другими стандартами и при этом фактически располагаются на рассматриваемом уровне, что часто приводит к путанице и недопониманию. Протоколы транспортного уровня и уровня Internet (протоколы IP, TCP и UDP) обычно сразу же ассоциируются с набором протоколов TCP/IP, а вот с привязкой протоколов уровня приложений (SMTP, HTTP и FTP) часто бывают проблемы.

К функциям уровня сетевого доступа относятся преобразование IP-адресов в аппаратные адреса и инкапсуляция IP-пакетов во фреймы (frames). Уровень сетевого доступа отвечает за физическую связь со средой передачи данных для данного аппаратного типа сетевого интерфейса.

Хорошим примером настройки уровня сетевого доступа является установка драйверов сетевого адаптера для операционной системы Windows. Сетевой адаптер будет автоматически распознан операционной системой и, в зависимости от версии операционной системы Windows, будет установлен соответствующий драйвер. Если используется одна из старых версий операционной системы, то необходимо будет указать вручную местоположение драйвера сетевого адаптера. Обычно производитель адаптера поставляет необходимые драйверы на дискете или компакт-диске.

Сравнение уровней моделей OSI и TCP/IP

На рис. 9.9 приведены модели OSI и TCP/IP для сравнения.

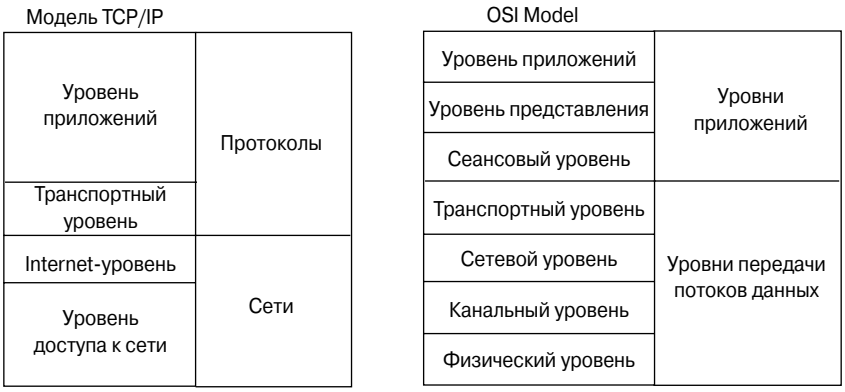


Рис. 9.9. Сравнение модели OSI с моделью TCP/IP

Следует обратить внимание, что модели имеют как сходства, так и отличия.

- Сходства обеих моделей:
  - обе модели содержат уровни;
  - обе модели имеют уровень приложений, хотя в них входят разные службы;
  - обе модели имеют практически одинаковые транспортный и сетевой уровни;
  - в обоих случаях подразумевается использование технологии коммутации пакетов (а не коммутации каналов);
  - профессионалы в области сетевых технологий обязаны знать обе модели.
- Различия моделей OSI и TCP/IP:
  - в модели TCP/IP уровень представлений и сеансовый уровни объединены в один — уровень приложений TCP/IP;
  - в модели TCP/IP уровень канального доступа и физический уровень модели OSI объединены в один уровень сетевого доступа;
  - модель TCP/IP выглядит проще, поскольку содержит меньше уровней;
  - транспортный уровень модели TCP/IP, использующий протокол UDP, в отличие от транспортного уровня модели OSI, не гарантирует доставку пакетов.

Благодаря тому, что протоколы TCP/IP являются стандартами, по которым была создана сеть Internet, модель TCP/IP приобрела известную степень доверия. В большинстве случаев существующие сети построены не в строгом соответствии с эталонной моделью OSI; она служит лишь руководством для понимания коммуникационных процессов.

Интерактивная презентация: модель TCP/IP и модель OSI
Эта презентация позволит идентифицировать и закрепить знания о двух моделях, в частности, запомнить их основные отличия.

Структура сети Internet

При всей сложности сети Internet можно выделить несколько базовых идей, на которых построена работа этой глобальной сети. В текущей главе исследуются базовые принципы построения сети Internet, в частности, рассматривается простая на первый взгляд идея о том, что такая сеть представляет из себя объединение множества сетей и позволяет практически мгновенно обмениваться информацией в глобальных масштабах между любыми пользователями где угодно и когда угодно. На рис. 9.10 показано, что компьютеры X и Y подключены к такой сети и могут обмениваться информацией, находясь в разных точках земного шара.

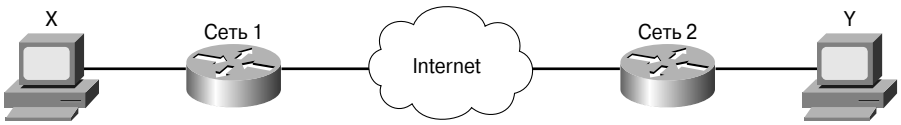


Рис. 9.10. Маршрутизаторы, соединяющие две сети

Одним из недостатков локальных сетей являются ограничения, связанные с их масштабируемостью:

- по количеству рабочих станций;
- по географической протяженности сети.

Выдающийся прогресс был достигнут в вопросе о допустимом количестве узлов, которые эффективно могут быть подключены к иерархической сети благодаря использованию преимуществ таких технологий, как Metro Optical (магистральные оптические сети), Gigabit- и 10-Gigabit-Ethernet. Однако каждая из станций в конечном итоге нуждается в службе глобального взаимодействия или службе распределенной сети, т.е. в технологии коммутации пакетов.

Основой структуры сети Internet является принцип независимости подробностей работы компьютеров и сетей, к которым они подключены, от механизмов доставки сообщений между отдельными сетями.

Одним из подходов к глобальному принципу построения сети Internet являлась идея взаимодействия уровней приложений передающего и принимающего компьютеров, а также всех компьютеров на пути их взаимодействия. Идентичные приложения, работающие на всех компьютерах, могли бы осуществить доставку сообщений в глобальных масштабах. Однако такой подход плохо расширяем. Добавление новых функций в используемые приложения потребовало бы обновления программного обеспечения на всех компьютерах, работающих в сети; новые возможности аппаратных платформ требовали бы изменений в программных приложениях. Сбой в работе одного из компьютеров или выполняемого в нем приложения могут вызвать обрыв цепочки, по которой следует сообщение.

Вместо описанного выше подхода в сети Internet применяется принцип взаимодействия сетевых уровней. Используя в качестве руководства эталонную модель OSI, ставится цель создать сеть, состоящую из независимых модулей. Такой мотив продиктован желанием сохранить разнообразие допустимых технологий локальных сетей на уровнях 1 и 2. В приложениях, функционирующих на уровнях 5, 6 и 7, также используются разнообразные технологии. Необходимо реализовать систему, где подробности организации верхних и нижних уровней будут скрыты от промежуточных сетевых устройств, передающих сетевой трафик, которым нет необходимости заботиться о тонкостях технологий локальных сетей (управляемых локально, так что вся сеть выглядит глобальной) или приложений, инициирующих сетевой обмен.

Перечисленные идеи являются основой концепции *межсетевого взаимодействия* — объединения малых сетей в крупные. Сеть, состоящая из других сетей, называется *internet* (с маленькой буквы). Большая заглавная "I" используется, когда подразумевают сеть, изначально созданную Министерством Обороны США (Department of Defense — DoD), в которой работают службы WWW, — Internet. Межсетевое взаимодействие обязано отвечать следующим требованиям:

- оно должно быть масштабируемым по количеству используемых сетей и подключенных компьютеров;
- должно содержать механизмы транспортировки данных на огромные расстояния, включая всю Землю и околоземное пространство;
- должно быть гибким и обеспечивать использование постоянно развивающихся новых и изменяющихся старых технологий;
- оно должно уметь приспосабливаться к динамическому характеру сети;
- должно быть экономически выгодным;
- обязано быть системой, позволяющей передать данные в любой момент времени, откуда и куда угодно.

На рис. 9.10 показано соединение двух физических сетей посредством специально предназначенного для этой цели устройства, называемого маршрутизатором. Эта диаграмма приближенно описывает суть проблемы, которая в 1984 году привела к созданию в Стэнфордском университете (Stanford University) корпорации Cisco Systems и впоследствии — изобретению маршрутизатора как такового. Показанные на рисунке сети называются *непосредственно подключенными* (directly connected) к маршрутизатору. В этой схеме маршрутизатор выполняет все необходимые преобразования для обмена данными между сетями. Однако, поскольку пользователи всегда и везде нуждаются в соединении с произвольными точками в глобальной сети, такая схема соединения только двух сетей быстро стала неадекватной.

На рис. 9.11 изображены два маршрутизатора, объединяющие три физические сети. В такой ситуации маршрутизаторы должны принимать более сложное решение. Поскольку все пользователи хотят передавать данные друг другу, даже не будучи подключенными напрямую, маршрутизатор должен иметь средства для перенаправления пакетов.

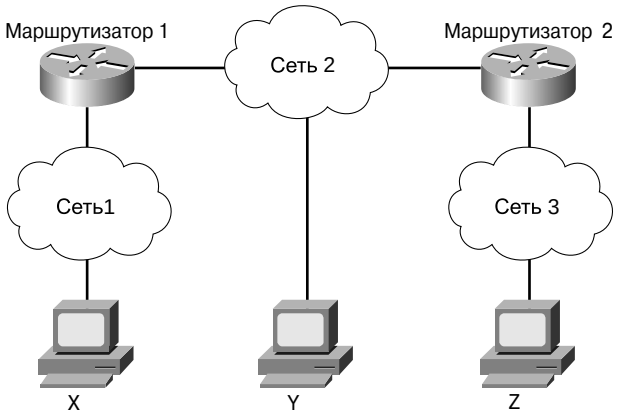


Рис. 9.11. Локальные и удаленные сети

Одним из вариантов решения могло бы быть использование хранящегося у маршрутизатора списка всех компьютеров и путей к ним. Таким образом маршрутизатор получил бы возможность принимать решения о необходимости пересылки данных, принимая во внимание список всех пользователей и информацию о компьютере-получателе. Однако очень быстро такой подход вызвал бы существенные проблемы по мере роста числа пользователей — он не масштабируем. Что произойдет, если маршрутизатор вместо полного списка будет хранить только список всех сетей, а проблемой локальной доставки предоставит заниматься локальной физической сети? Такое решение лучше и более масштабируемо — пересылка осуществляется на основе информации о сети назначения. В таком случае маршрутизаторы только передают сообщения. В принципе описанная идея может быть распространена и на большое количество маршрутизаторов, если они могут обмениваться необходимой информацией о том, с какими сетями соединены.

На рис. 9.12 представлен результат использованного расширенного подхода и проиллюстрирована наиболее предпочтительная для потребителей ситуация: осуществляется универсальное межсетевое взаимодействие; информация, которую необходимо знать о конечных пользователях для доставки их данных через сетевую среду, минимальна. Тем не менее, физическая и логическая иерархия подобной структуры могут быть чрезвычайно сложны. Действительно, сеть Internet растет экспоненциально. Протоколы и устройства, на основе которых функционирует глобальная сеть, находятся в постоянном развитии, чтобы позволить подключение новых пользователей, число которых постоянно растет. Тот факт, что сеть Internet разрослась до огромных размеров и содержит более 90 000 узловых маршрутизаторов и более 300 000 000 конечных пользователей, безоговорочно говорит в пользу базовых идей, лежащих в основе структуры Internet.

Таким образом, два компьютера, расположенные в произвольных точках мира, имеющие определенное аппаратное и программное обеспечение, соответствующие спецификациям необходимых протоколов, могут надежно взаимодействовать друг с другом (“где угодно/когда угодно/кто угодно”). Даже когда устройства не подключены

напрямую (например, прямое подключение принципиально невозможно), инструменты для совместной работы и различные средства передачи данных по сети Internet позволяют обмениваться информацией так, как если бы компьютеры были расположены в одной комнате.

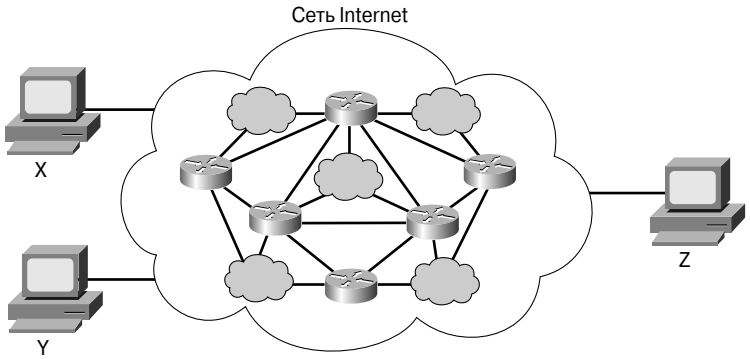


Рис. 9.12. Физические детали сети скрыты от пользователя

Адреса сети Internet

Сетевой уровень отвечает за навигацию данных по сети, и его задача заключается в нахождении наилучшего маршрута. Устройства используют схему адресации сетевого уровня для определения адреса пункта назначения информации при ее передаче по сети. В этом разделе описаны IP-адресация и пять классов IP-адресов, а также подсети, маски подсетей и их роль в схемах IP-адресации. Кроме того, обсуждаются отличия между публичными и частными адресами, IPv4- и IPv6-адресацией, а также одноадресными и широковещательными сообщениями.

IP-адреса

Чтобы любые две системы могли взаимодействовать между собой, они должны иметь возможность однозначно идентифицировать друг друга, как это показано на рис. 9.13. Несмотря на то что показанные адреса не являются фактическими сетевыми адресами, они демонстрируют концепцию группировки адресов. Буквы А и Б идентифицируют сеть, последовательность номеров идентифицирует сетевую станцию. Комбинация из буквы (номер сети) и последовательности цифр (адрес станции) создает уникальный адрес для любого устройства в сети. В повседневной жизни имена или номера (такие, как номера телефонов) часто используются в качестве уникальных идентификаторов. Аналогично этому каждый компьютер в TCP/IP-сети обязан иметь как минимум один уникальный идентификатор или адрес. Такой адрес позволяет одному компьютеру в сети находить другой.

Компьютеры могут быть подключены к более чем одной сети, например, так, как показано на рис. 9.14. Двойное подключение реализовано посредством использования двух сетевых адаптеров. Устройство с двумя соединениями называется устройством с двойной привязкой, или двухканальным устройством (dual-homed). Следует

отметить, что два интерфейса компьютера находятся в абсолютно разных сетях и, как следствие, имеют разные идентификаторы сети в своих адресах. Еще одно важное замечание: такой компьютер пересылает данные, если только он не сконфигурирован для этого специально; он просто имеет доступ к обеим сетям. В подобной ситуации системе должно быть присвоено более одного адреса, каждый из которых идентифицирует его соединение с отдельной сетью. Строго говоря, не самой системе присваивается адрес, а каждому из модулей, которые используются для подключения узла к сети (т.е. интерфейсам), что позволяет остальным компьютерам находить его в соответствующих сетях.

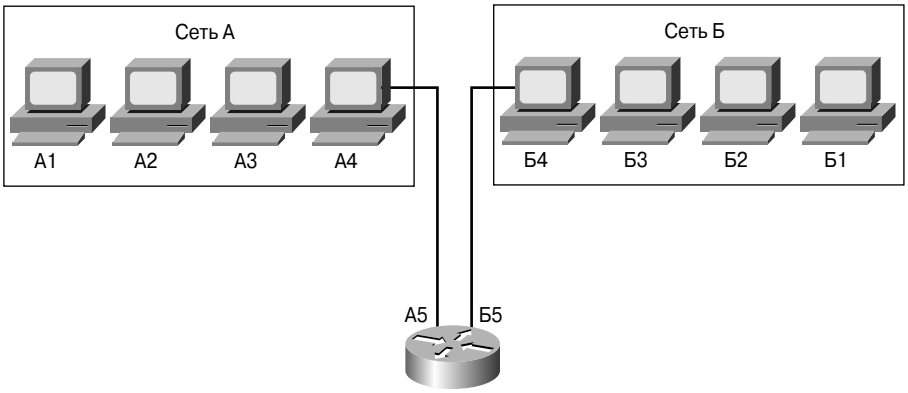


Рис. 9.13. Адреса узлов

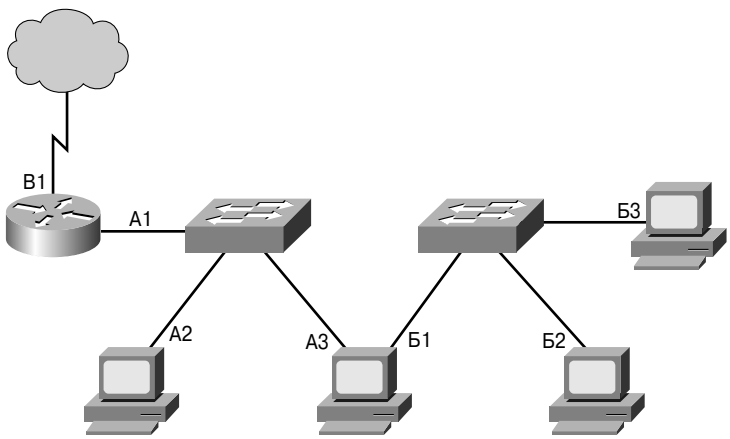


Рис. 9.14. Компьютеры с двойной привязкой

Компьютеры хранят IP-адрес в виде 32-битовой последовательности единиц и нулей (рис. 9.15). Для простоты использования IP-адрес обычно записывается в виде четырех десятичных номеров, разделенных точками. Предположим, адрес одного из компьютеров — 192.168.1.2. Второй компьютер может иметь адрес 128.10.2.1. Такой

способ написания адреса называется *точечно-десятичным форматом*. В таком виде каждый IP-адрес состоит из четырех частей, разделенных точками. Каждая из частей называется *октетом*, поскольку состоит из восьми двоичных цифр. Например, адресу 192.168.1.8 соответствует запись 11000000.10101000.00000001.00001000 в двоичном представлении. Человек легче воспринимает точечно-десятичный формат, чем двоичные ноли и единицы. Этот формат помогает также избежать ошибок из-за перестановки цифр, что часто случается при использовании двоичных номеров.

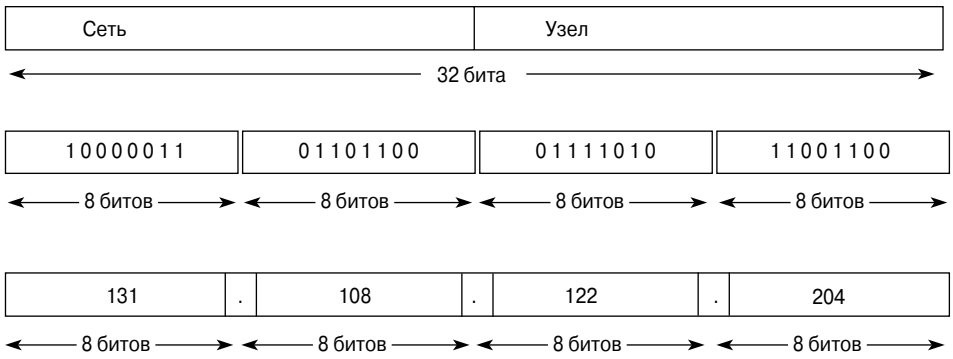


Рис. 9.15. Формат IP-адреса

Точечно-десятичный формат позволяет намного быстрее различить цифровые составляющие адреса (рис. 9.15). И двоичный, и десятичный номера на рисунке соответствуют одному и тому же адресу, но в десятичном формате он выглядит намного проще и, что несомненно, короче. Ошибки — одна из наиболее общих проблем при работе с двоичными адресами. В длинных последовательностях из нолей и единиц легко ошибиться, поменять цифры местами или что-либо пропустить. Иными словами, намного проще увидеть связь между такими двумя номерами:

192.168.1.8 и
192.168.1.9,

чем распознать ту же связь в двоичных эквивалентах тех же адресов:

11000000.10101000.00000001.00001000 и
11000000.10101000.00000001.00001001.

Глядя на двоичную форму записи двух адресов, практически невозможно понять, что они представляют из себя последовательные номера узлов.

Презентация: основы IP-адресации
В этой презентации представлен видеоролик, который повествует о структуре IP-адресов и их глобальной уникальности. В нем также рассказано о разных классах IP-адресов и о том, как их можно различить.

Преобразование адресов из двоичной формы в десятичную

Зачастую существует несколько способов решения математической задачи, и преобразование из десятичной формы в двоичную — не исключение. В текущем разделе описан один из способов, но, конечно же, допустимо использовать и другие, если они кажутся вам более удобными.

Основной прием при преобразовании десятичного номера в двоичный заключается в поиске ближайшего числа с наибольшей степенью двойки, не превышающего искомого десятичного, как это показано в табл. 9.1. Поскольку такой процесс разработан для работы с компьютерами, наиболее логично начать с наибольшего числа, которое укладывается в 1 и 2 байта.

Таблица 9.1. Подсчет количества доступных адресов узлов

Степени числа 2 и соответствующие им десятичные значения															
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
32678	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Как уже отмечалось, чаще всего биты группируются по 8, что соответствует одному байту. Иногда наибольшее значение, которое может быть представлено одним байтом (255), меньше необходимого числа. В таком случае байты объединяются, т.е. вместо двух восьмибитовых чисел используется одно шестнадцатибитовое, а вместо трех восьмибитовых — одно 24-битовое. Для больших чисел используются те же правила, что и для восьмибитовых чисел: чтобы получить текущее значение, необходимо предыдущее умножить на 2. В табл. 9.1 показаны такие значения (для двухбайтового, т.е. шестнадцатибитового числа): они пригодятся при изучении механизма организации подсетей.

Поскольку при работе с компьютерами чаще всего приходится оперировать байтами, логично будет начать с расчета чисел в пределах байта и произвести все необходимые вычисления, результат которых приведен в табл. 9.2. Для более наглядной демонстрации рассмотрим следующие примеры, в первом из которых будет преобразовано десятичное число 6 783. Поскольку это число больше 255 — максимального числа для одного байта, необходимо использовать двухбайтовое число. Начнем подсчет с 2^{15}. В результате расчетов получится, что десятичному числу 6 783 соответствует двоичное 00011010 01111111.

Второй пример — число 104. Поскольку оно меньше 255, преобразование может быть сделано в пределах одного байта, как это показано в табл. 9.3.

Таким образом, десятичное число 104, преобразованное в двоичное, выглядит так: 01101000.

Таблица 9.2. Диаграмма для преобразования десятичного числа в двоичное

Степень 2 (по позиции)	Десятичное	Значение степени (по позиции)	Двоичное	Остаток
2^{15}	6783	32678	0	6783
2^{14}	6783	16384	0	6783
2^{13}	6783	8192	0	6783
2^{12}	6783	4096	1	2687
2^{11}	2687	2048	1	639
2^{10}	639	1024	0	639
2^{9}	639	512	1	127
2^{8}	127	256	0	127
2^{7}	127	128	0	127
2^{7}	127	64	1	63
2^{6}	63	32	1	31
2^{5}	31	16	1	15
2^{3}	15	8	1	7
2^{2}	7	4	1	3
2^{1}	3	2	1	1
2^{0}	1	1	1	0

Таблица 9.3. Преобразование восьмибитового числа

Степень 2 (по позиции)	Десятичное	Значение степени (по позиции)	Двоичное	Остаток
2^{7}	104	128	0	104
2^{6}	104	64	1	40
2^{5}	40	32	1	8
2^{4}	8	16	0	8
2^{3}	8	8	1	0
2^{2}	0	4	0	0
2^{1}	0	2	0	0
2^{0}	0	1	0	0

Приведенный выше метод подходит для любых десятичных чисел. Рассмотрим десятичное число 1000000. Поскольку 1000000 больше, чем наибольшее число,

содержащееся в двух байтах (65535), потребуется использовать как минимум 3 байта. Последовательно умножая числа на 2, пока не будет достигнуто 24 бита, мы получим число 8388608, при этом максимальное десятичное число, которое может содержаться в 24 битах, равно 16777215. Таким образом, начиная с 24-го бита, необходимо повторять расчет до тех пор, пока не будет получен 0 в остатке. Выполнив эту процедуру, нетрудно подсчитать, что десятичное число 1000000 равно двоичному 00001111 01000010 01000000.

Преобразование из двоичного в десятичный формат является обратной процедурой. Для этого необходимо поместить двоичное число в такую же таблицу, как та, что использовалась в предыдущих примерах. В табл. 9.4 проиллюстрирован такой пример. В ней показано преобразование двоичного числа 00000100 00011101 в десятичное число 1053.

Таблица 9.4. Преобразование шестнадцатибитового двоичного числа в десятичное

Степень 2 (по позиции)	Десятичное	Значение степени (по позиции)	Двоичное	Остаток
2^{15}	0	32678	0	0
2^{14}	0	16384	0	0
2^{13}	0	8192	0	0
2^{12}	0	4096	0	0
2^{11}	0	2048	0	0
2^{10}	0	1024	1	1024
2^{9}	1024	512	0	1024
2^{8}	1024	256	0	1024
2^{7}	1024	128	0	1024
2^{6}	1024	64	0	1024
2^{5}	1024	32	0	1024
2^{4}	1024	16	1	1040
2^{3}	1040	8	1	1048
2^{2}	1048	4	1	1052
2^{1}	1052	2	0	1052
2^{0}	1052	1	1	1053

Адресация IPv4

Протокол IP пересылает пакеты, порожденные в одной из сетей, в другую, т.е. в сеть назначения, используя некоторые уникальные параметры (рис. 9.16). Следовательно, в этой схеме должны быть заданы идентификаторы сети-отправителя и сети-получателя. Используя идентификатор сети назначения, протокол IP доставляет

пакеты в сеть, которой они адресованы. Когда пакет достигает интерфейса маршрутизатора, подключенного к сети получателя, протокол IP должен идентифицировать определенный компьютер, подключенный к этой же сети, которому адресован пакет. Такая схема очень похожа на работу обычной почтовой службы. Решение о том, в каком направлении будет отправлена корреспонденция, принимается на основе почтового индекса, и письмо приходит в почтовое отделение того города, которому соответствует индекс. Далее почтовое отделение принимает решение о доставке сообщения внутри города непосредственному адресату на основе его почтового адреса. Описанный процесс состоит из двух этапов.

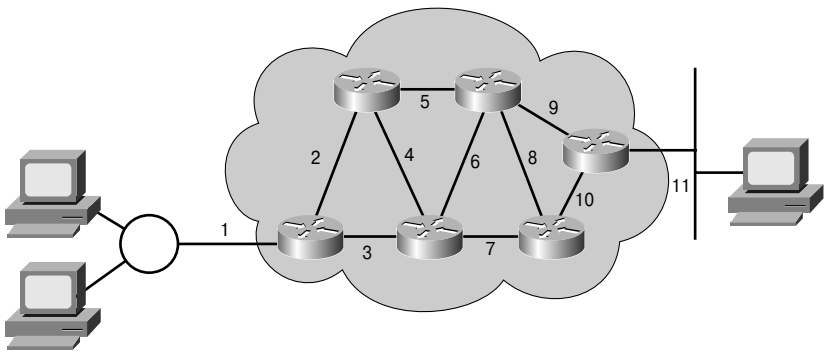


Рис. 9.16. Коммуникационный маршрут

Аналогично IP-адреса состоят из двух частей, как это показано на рис. 9.17. Одна часть идентифицирует сеть, к которой подключена система, вторая же служит идентификатором самой системы. Такая адресация называется иерархической, поскольку включает несколько уровней, как показано на рис. 9.18. Как уже обсуждалось выше, значения любого октета находятся в диапазоне от 0 до 255. В рассматриваемом примере второй октет может быть разбит на 256 подгрупп, каждая из которых в свою очередь также может быть разбита на 256 подгрупп с 256-ю адресами в каждой. Адрес группы, находящийся в иерархической схеме (рис. 9.18) непосредственно над группой, является идентификатором для всей порождаемой ветви адресов и сетей и может рассматриваться как единое целое. IP-адрес объединяет оба идентификатора в один адрес. Такой номер должен быть уникальным, поскольку дублирование адресов не допускается; его первая часть идентифицирует адрес сети, а вторая — адрес узла — однозначно задает машину в этой сети.

Каким же образом пользователь может отличить, какая часть адреса задает адрес сети, а какая — адрес узла? Впервые этот вопрос задали себе создатели сети Internet, полагавшие, что будут создаваться сети разного размера, исходя из необходимого числа компьютеров, входящих в ее состав, что проиллюстрировано в табл. 9.5.

При разработке такой схемы предполагалось, что очень больших сетей, содержащих миллионы подключенных компьютеров, будет сравнительно мало. Разработчики предвидели большое количество сетей среднего масштаба с тысячами компьютеров в каждой из них. И, конечно же, они предполагали, что будет создано огромное количество мелких сетей с несколькими сотнями машин или даже меньше. Исходя

из этого, разработчики разделили доступные IP-адреса на классы и задали таким образом размер сетей: большие (класс A), средние (класс B) и мелкие (класс C) (табл. 9.6). Информация о классе адреса — это первая подсказка, которая используется, чтобы определить, какая часть адреса описывает сеть, а какая — адрес узла.

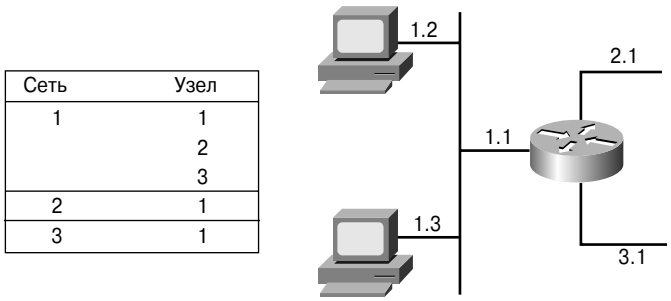


Рис. 9.17. Две части IP-адреса

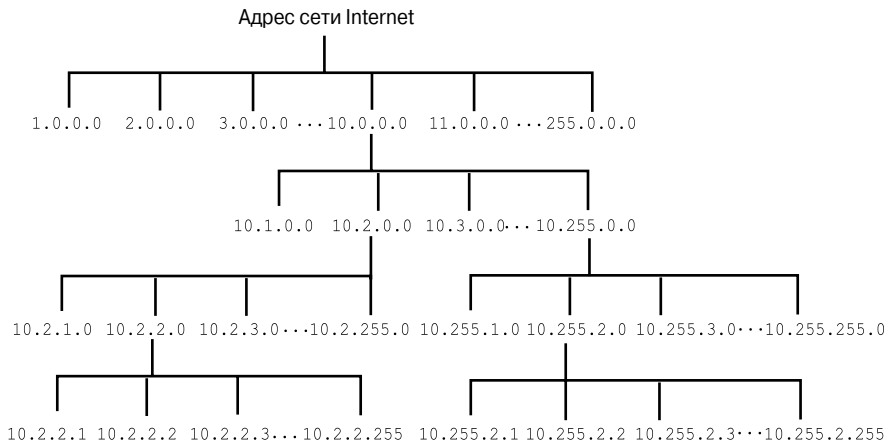


Рис. 9.18. Иерархические IP-адреса

Таблица 9.5. Классы IP-адресов

Класс адреса	Количество сетей	Количество узлов
A	126[2]	16777216
B	16384	65535
C	2097152	254
D (многоадресатный)	-	-

[2] *Диапазон адресов 127.x.x.x зарезервирован в качестве так называемого петлевого (loopback) адреса, который используется для тестирования и диагностики. — Прим. ред.*

Таблица 9.6. Определение классов адресов

Класс адреса	Начальные биты адреса	Диапазон значений первого октета адреса	Количество битов в сетевой части адреса
A	0	от 0 до 127[3]	8
B	10	от 128 до 191	16
C	110	от 192 до 223	24
D (многоадресатный)	1110	от 224 до 239	28

Классы IP-адресов: A, B, C, D и E

Чтобы иметь возможность описать сети разного размера и облегчить их классификацию, IP-адреса были разделены на группы, называемые классами (рис. 9.19). Такая схема адресации называется *классовой*. Каждый полный 32-битовый IP-адрес делится на две части, описывающие сеть и узел. Бит или последовательность битов в начале каждого адреса задают его класс (рис. 9.20). Существуют пять *классов IP-адресов*.

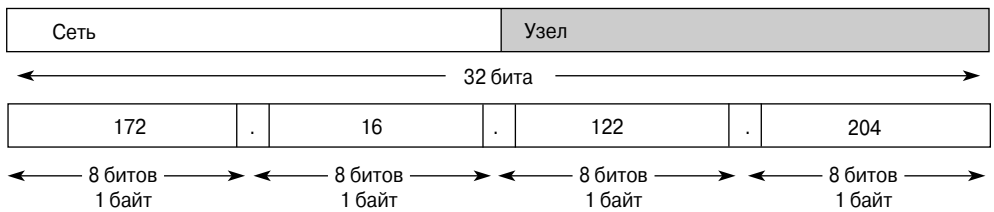


Рис. 9.19. Разделение адреса на сетевую и узловую части

Адреса класса A

Адреса класса A (рис. 9.21) предназначены для очень больших сетей. В адресе класса A используется только первый октет в качестве идентификатора сети. Оставшиеся три октета выделены для перечисления адресов узлов.

Первый бит в адресе класса A всегда равен 0. Учитывая это, наименьшее допустимое число будет равно 00000000 (десятичный 0), а наибольшее — 01111111 (десятичное число 127). Следует заметить, что оба номера, 0 и 127, являются зарезервированными и не могут быть использованы в качестве сетевых адресов. Любые адреса, начинающиеся с числа в диапазоне от 1 до 126 в первом октете, являются адресами класса A.

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

[3] *127 (01111111) — набор адресов класса A, зарезервирован для тестирования и диагностики и не может быть присвоен устройствам или реальной сети. — Прим. ред.*

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

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

Количество начальных битов префикса	3	21	8
Класс C: значение префикса	110	Сетевые биты	Биты узла

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

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

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

Адреса класса E зарезервированы для исследовательских целей.

Рис. 9.20. Начальные биты, образующие классы адресов

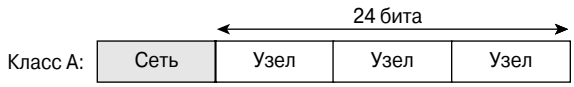


Рис. 9.21. Адреса класса A

Адреса класса B

Адреса класса B используются для сетей среднего и крупного размера (рис. 9.22). В IP-адресе класса B используются два первых октета для сетевого адреса. Оставшиеся два октета представляют адрес узла.

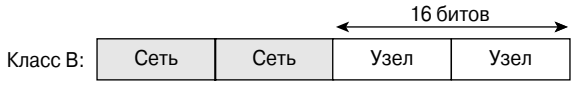


Рис. 9.22. Адреса класса B

Первые два бита первого октета всегда равны 10, оставшиеся 6 битов могут содержать любые комбинации нулей и единиц. Таким образом, наименьшее число, которое может быть использовано для адресов этого класса, равно 10000000 (десятичное 128), и наибольшее — 10111111 (десятичное значение равно 191). Любые адреса, содержащие в первом октете числа от 128 до 191, являются адресами класса B.

Адреса класса C

Адреса класса C (рис. 9.23) — это наиболее часто используемые из исходных классов адресов. Данный класс адреса предназначен для использования в малых сетях.

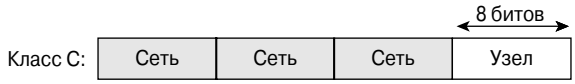


Рис. 9.23. Адреса класса C

Адрес этого класса начинается с двоичной комбинации 110. Таким образом, наименьшее доступное число — 11000000 (десятичное 192), а наибольшее — 11011111 (десятичное значение 223). Если адрес в первом октете содержит числа от 192 до 223, значит, он относится к классу C.

Адреса класса D

Адреса класса D (рис. 9.24) были созданы для реализации в IP-адресах механизма многоадресатной рассылки. *Многоадресатным, или групповым, адресом (multicast address*) называется уникальный сетевой адрес, используемый для отправки пакетов, содержащих адрес рассматриваемого класса в поле получателя, предопределенным группам сетевых устройств. Таким образом, одна сетевая станция может передавать один поток данных нескольким получателям.

Рис. 9.24. Адреса класса D

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

Адреса класса E

Адреса класса E (рис. 9.25) также были описаны в стандартах и выделены в отдельный блок. Однако они были зарезервированы проблемной группой проектирования Internet (Internet Engineering Task Force — IETF) для собственных исследовательских нужд. В результате адреса класса E никогда не использовались в сети Internet. Первые четыре бита адресов класса E всегда содержат 1. Следовательно, значение первого октета находится в диапазоне от 11110000 до 11111111 или от 240 до 255 — в десятичном виде.

Рис. 9.25. Адреса класса E

Диапазоны значений первого октета в IP-адресах для каждого из классов приведены в табл. 9.7.

Таблица 9.7. Классы IP-адресов: диапазон значений первого октета

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

Практическое задание 9.2.7. Основы IP-адресации
Это практическое задание содержит упражнения, которые помогут понять, что такое IP-адреса, и разобраться в принципах функционирования стека TCP/IP.

Зарезервированные IP-адреса

Некоторые адреса являются зарезервированными и не могут быть присвоены сетевым устройствам. К ним относятся следующие:

- сетевые адреса, идентифицирующие саму сеть (рис. 9.26). Верхний прямоугольник на рисунке обозначает сеть с адресом 198.150.11.0. Данные, адресованные любому из узлов, находящихся в этой сети (198.150.11.1 или 198.150.11.254), вне этой сети выглядят как данные, которые отправлены на адрес 198.150.11.0. Адрес узла принимается во внимание только тогда, когда пакет с данными нужно адресовать получателю внутри локальной сети. Нижний прямоугольник на рисунке обозначает другую такую же локальную сеть, но с адресом 198.150.12.0;

- как следует из названия, *широковещательный адрес* используется для широковещательной рассылки всем сетевым устройствам (рис. 9.27). Верхний прямоугольник схематически поясняет широковещательный адрес 198.150.11.255. Данные, отправленные по этому адресу, будут получены каждым из узлов в сети (от 198.150.11.1 до 198.150.11.254). Нижний прямоугольник иллюстрирует подобную ситуацию для широковещательного адреса 198.150.12.255.

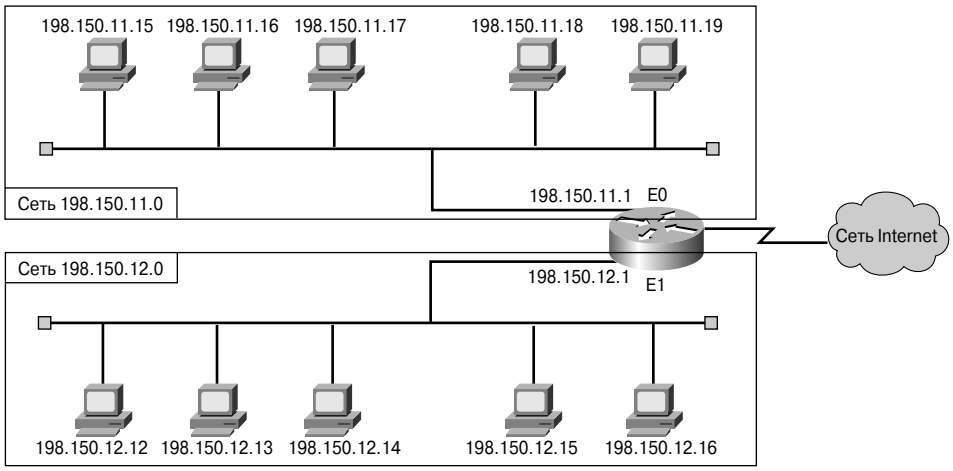


Рис. 9.26. Адрес сети

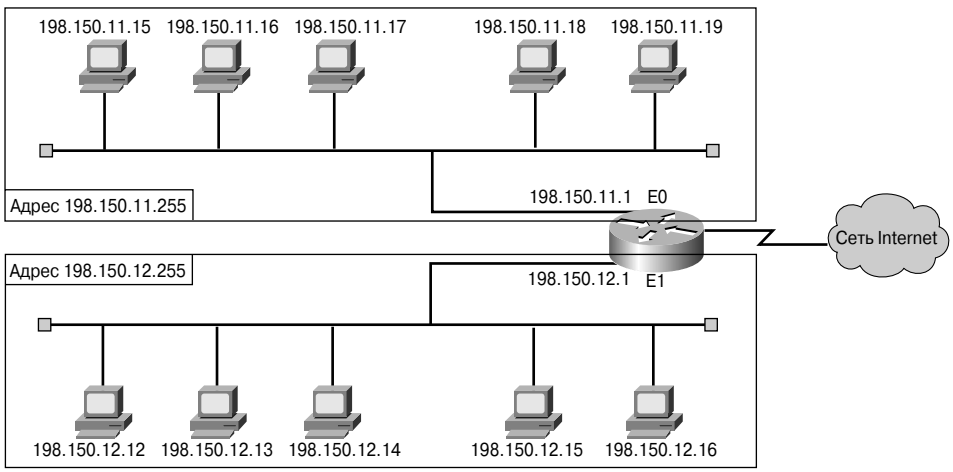


Рис. 9.27. Широковещательный адрес

IP-адрес, у которого все биты, отведенные под адрес узла, заполнены нулями, зарезервирован под *адрес сети* (рис. 9.28). Показанный адрес класса B имеет нули во всех битах, отведенных под адрес узла. Таким образом, в примере для сети класса A

число 113.0.0.0 является адресом сети, содержащей узел 113.1.2.3. Маршрутизатор использует IP-адрес сети при пересылке данных через сеть Internet. Примером для сети класса B может служить адрес 176.10.0.0, показанный на рис. 9.28.

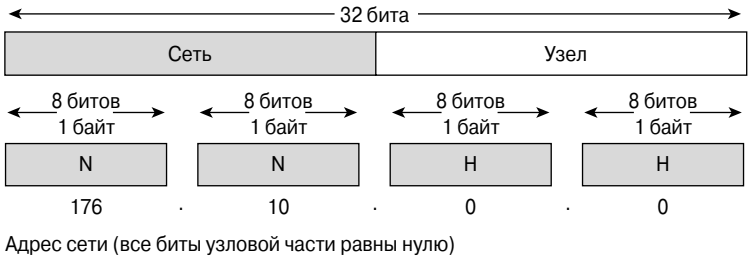


Рис. 9.28. Структура адреса сети

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

Для передачи данных всем узлам в сети требуется широковещательный адрес. Широковещательная рассылка используется, когда отправитель пересылает данные всем устройствам в сети (рис. 9.29). Адрес класса B, который показан на рис. 9.29 внизу, является широковещательным для данной сети. Когда пакеты будут получены в соответствии с широковещательным адресом получателя, данные будут обработаны на каждом из компьютеров. Чтобы быть уверенным в том, что все устройства в сети получили и обработали пакеты широковещательной рассылки, отправитель должен использовать специальный IP-адрес, который будет понят и правильно обработан остальными устройствами. В широковещательных IP-адресах все биты, отведенные под адрес узла (поле узла), равны единице.

Для сети с адресом 176.10.0.0, в котором последние 16 битов формируют поле узла (или отведенную для узла часть адреса), адресом широковещательной рассылки, по которому пакеты будут отправлены всем сетевым устройствам, является адрес 176.10.255.255 (поскольку десятичное число 255 соответствует двоичному октету 11111111).

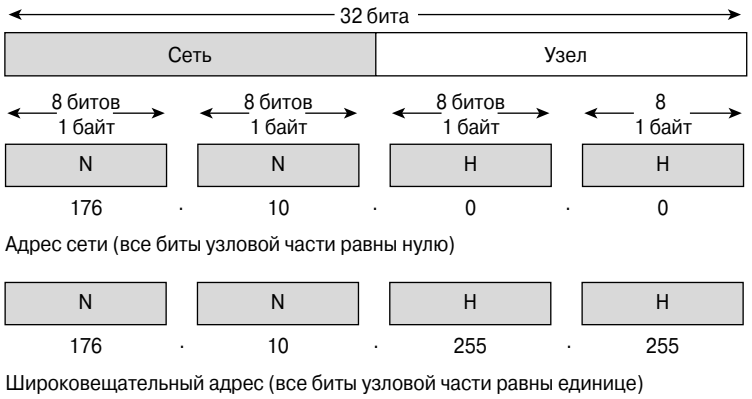


Рис. 9.29. Широковещательный адрес

Открытые и частные адреса

Стабильное функционирование сети Internet зависит от уникальности используемых в сети публичных адресов. Как показано на рис. 9.30, при использовании сетевой схемы адресации могут возникнуть некоторые проблемы. В проиллюстрированной на рисунке структуре обе сети имеют адрес 198.150.11.0. Когда данные приходят на маршрутизатор, в какую из сетей они должны быть перенаправлены? Схемы, подобные этой, могут значительно увеличить объем сетевого трафика и сделать невозможным выполнение основной функции маршрутизатора; следовательно, нужно предусмотреть какие-либо механизмы для проверки уникальности используемых адресов. Такие функции изначально были поставлены перед организацией InterNIC (Internet Network Information Center — Информационный Центр Internet). Сейчас функции этой организации переданы Агентству по выделению имен и уникальных параметров протоколов Internet (Internet Assigned Numbers Authority — IANA). Эта организация тщательно следит за тем, чтобы среди выдаваемых для публичного использования незадействованных адресов не встречались повторяющиеся. Наличие дублирующихся адресов могло бы привести к нестабильности работы сети Internet и дополнительной нагрузке на устройства из-за доставки пакетов сетям, использующим дублирующиеся адреса.

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

Вследствие быстрого роста сети Internet количество незанятых IP-адресов уменьшается, поэтому появляются новые схемы адресации, такие, как бесклассовая междоменная маршрутизация (Classless InterDomain Routing — CIDR) и IPv6, призванные помочь решить проблему исчерпания адресного пространства. Технологии CIDR и IPv6 подробно будут рассмотрены ниже.

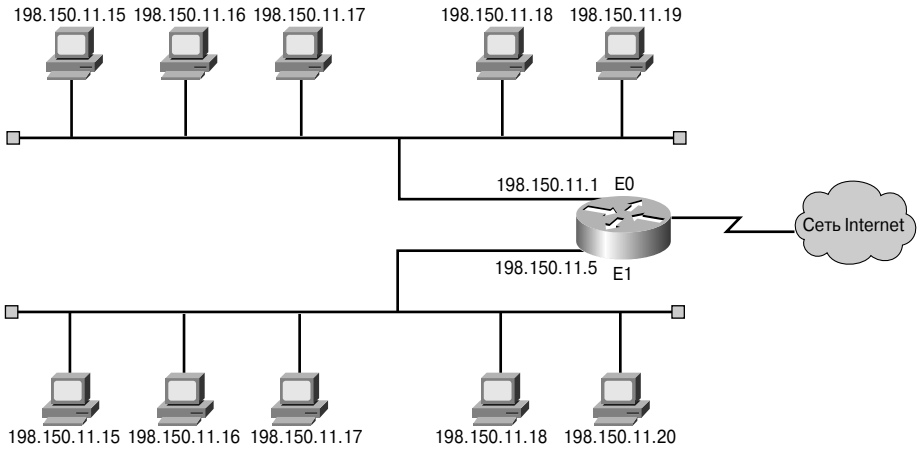


Рис. 9.30. Уникальность адресов

Чтобы частично решить проблему нехватки адресного пространства, был разработан альтернативный вариант — использование частных IP-адресов (табл. 9.8). Как уже говорилось, узлы в сети Internet должны иметь глобально-уникальные адреса. Однако частные сети, не подключенные к открытой сети, могут использовать любые действительные адреса, которые должны быть уникальны только внутри локальной сети. Многие частные сети используются совместно с открытыми сетями, поэтому использование выбранных произвольно адресов настоятельно не рекомендуется, поскольку однажды частная сеть может оказаться подключенной к глобальной сети Internet.

В спецификации RFC 1918[4] выделены три блока IP-адресов (один адрес класса A, серия адресов класса B и набор адресов класса C) для внутреннего использования в частных сетях. Адреса из этих диапазонов не передаются магистральными маршрутизаторами сети Internet, и пакеты с адресами из частных сетей немедленно будут отброшены такими устройствами.

Таблица 9.8. Частные IP-адреса

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

[4] *Requests for Comments — запросы на комментарии. Серия документов IETF, начатая в 1969 году и содержащая описания набора протоколов Internet и связанную с ними информацию. Самый последний документ, который описывает зарезервированные адреса, имеет номер RFC 3330. — Прим. ред.*

В том случае, когда нужно выбрать схему адресации для внутренней сети тестовой лаборатории или домашней сети, можно использовать диапазоны адресов, перечисленные в табл. 9.8, вместо глобально уникальных. Частные IP-адреса могут использоваться совместно с публичными для внутренних соединений, что позволяет экономить открытые уникальные адреса.

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

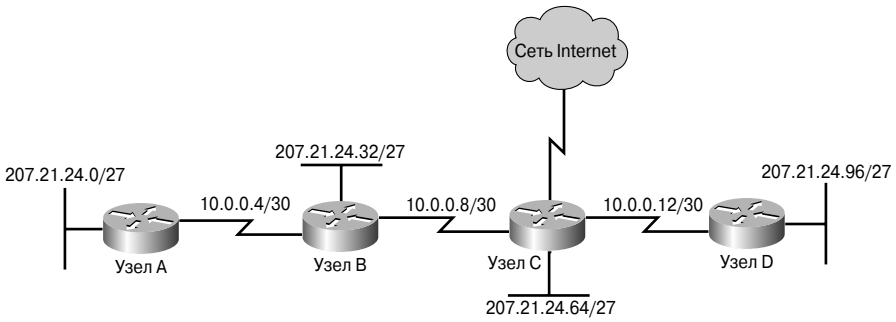


Рис. 9.31. Использование частных адресов в распределенной сети организации

Подсети

Еще одним способом экономии IP-адресов, который используется наряду с уже упомянутыми выше технологиями CIDR, адресацией IPv6 и частными адресами, является *механизм использования подсетей (subnetting*). Этот метод позволяет разбивать полные классовые блоки сетевых адресов на меньшие и помогает избежать полного исчерпания IP-адресов. На рис. 9.32 показана сеть класса B (131.108.0.0), которая разбита на три подсети. Каждый сетевой администратор должен понимать механизм создания подсетей как способ деления и идентификации отдельных сетей внутри локальной сети. Небольшие сети требуется разбивать на более мелкие подсети достаточно редко, но в случае использования больших блоков адресов и очень крупных сетей такое деление необходимо. Согласно определению, создание в сети подсетей означает использование маски подсети для разделения ее на более мелкие, более эффективные, легче управляемые сегменты, как показано на рис. 9.33. Такая схема похожа на используемую в телефонных сетях нумерацию, где состоит из телефонного кода страны, кода региона или города и телефона конечного абонента. Такие компоненты телефонных систем сравнимы с соответствующими элементами в IP-сетях — адресами сетей, подсетей и отдельных узлов.

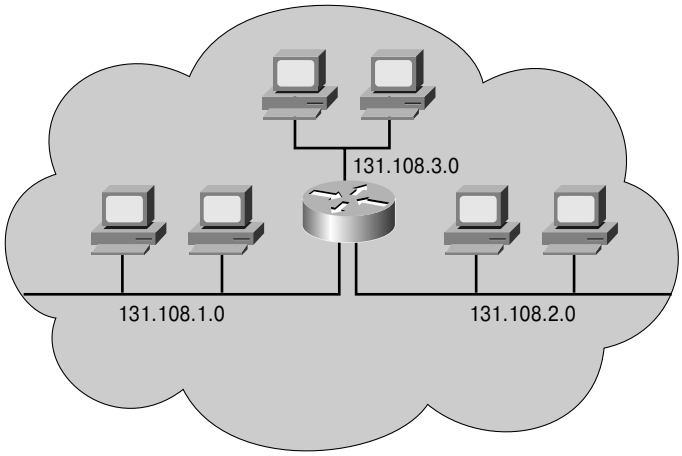


Рис. 9.32. Схема адресации с использованием подсетей

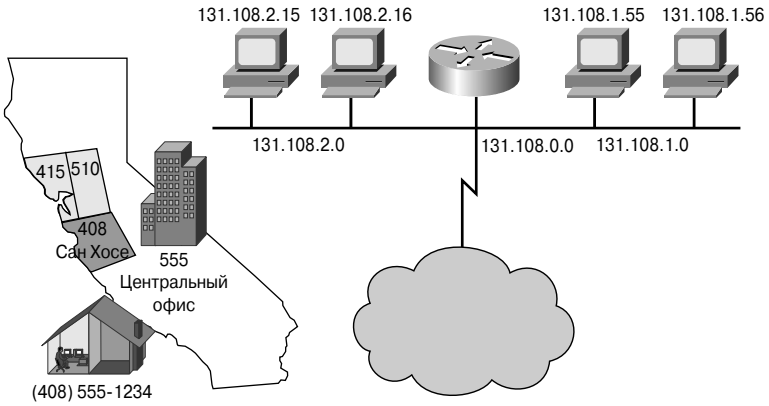


Рис. 9.33. Адреса подсетей

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

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

Чтобы создать подсеть, сетевой администратор заимствует биты из поля адресов узлов исходного адреса всей сети и назначает их в качестве адреса подсети (табл. 9.9). Минимальное число битов, которое может быть заимствовано, — два. Если использовать всего один бит, то после разбиения будет получен только один сетевой адрес (.0 — адрес сети) и один широковещательный (.255). Максимальное число битов, которые разрешено заимствовать, может быть любым (в рамках максимальной длины узловой части адреса), при условии, что останутся незадействованными не менее двух битов для адресов узлов. В табл. 9.9 показано, что для сети класса C может быть заимствовано не более 6 битов из поля адреса узла для создания подсети.

Таблица 9.9. Адреса подсетей

Первый октет адреса узла в десятичной нотации	Количество подсетей	Количество узлов класса A в каждой подсети	Количество узлов класса B в каждой подсети	Количество узлов класса C в каждой подсети
.192	2	4194302	16382	62
.224	6	2097150	8190	30
.240	14	1048574	4094	14
.248	30	524286	2046	6
.252	62	262142	1022	2
.254	126	131070	510	—
.255	254	65534	254	—

Сравнение протоколов IP версии 4 и IP версии 6

Когда в 1980 году был утвержден стандарт TCP/IP, он основывался на схеме двухуровневой адресации, которая в то время давала необходимую масштабируемость. К сожалению, создатели TCP/IP не могли предположить, что их протокол станет основой для глобальной сети обмена информацией, сети развлечений и коммерции. Более двадцати лет назад в протоколе IP версии 4 (IPv4) была предложена стратегия адресации, которая, будучи вполне подходящей для того времени, привела к неэффективному распределению адресов.

Как показано на рис. 9.34, адреса классов A и B покрывают 75% всего адресного пространства IPv4, но относительное число организаций, которые могли бы использовать сети этих классов, не превышает 17000. Сетей класса C значительно больше, чем сетей классов A и B, но количество доступных IP-адресов ограничивается всего 12,5% от их общего числа, равного 4 млрд.

К сожалению, в сетях класса C не может быть более 254 узлов, что не соответствует потребностям достаточно крупных организаций, но которые вместе с тем не настолько велики, чтобы получить адреса классов A и B. Даже если бы существовало больше адресов сетей классов A, B и C, слишком большое их число привело бы к тому, что маршрутизаторы сети Internet были бы вынуждены обрабатывать огромное количество таблиц маршрутизации, хранящих маршруты ко всем сетям.

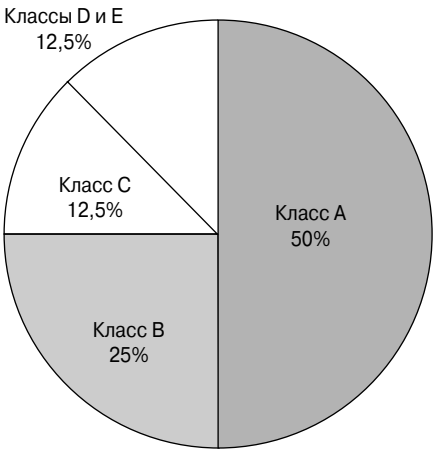


Рис. 9.34. Распределение IP-адресов

Еще в 1992 году проблемная группа проектирования Internet (IETF) обнаружила две специфические проблемы:

- **остаток нераспределенных адресов сетей IPv4 близок к исчерпанию**. В то время адреса класса B были практически израсходованы;
- **наблюдается быстрое и постоянное увеличение размеров таблиц маршрутизации сети Internet в связи с ее ростом.** Появление новых подключенных к структуре Internet сетей класса C порождает поток информации, способный привести к тому, что маршрутизаторы сети Internet перестанут эффективно справляться со своими задачами.

За последние два десятилетия был разработан ряд технологий, расширяющих IPv4 и направленных для модернизации существующей 32-битовой схемы адресации. Две наиболее значительные из них — это маски подсетей и маршрутизация CIDR (Classless InterDomain Routing — бесклассовая междоменная маршрутизация).

Приблизительно в то же время была разработана и одобрена еще более расширяемая и масштабируемая версия технологии IP — IP версии 6 (IPv6). Протокол IPv6 использует для адресации 128 битов вместо 32-х битов в IPv4 (рис. 9.35). В стандарте IPv6 используется шестнадцатеричная запись числа для представления 128-битовых адресов, и он позволяет использовать 16 млрд. IP-адресов. Эта версия протокола IP должна обеспечить необходимое количество адресов как на текущий момент, так и в будущем.

Для представления 128-битового адреса в протоколе IPv6 используется запись из восьми шестнадцатибитовых чисел, представляемых в виде четырех шестнадцатеричных цифр, как это показано на рис. 9.36. Группы из четырех шестнадцатеричных цифр разделены двоеточиями, нули в старших позициях могут быть опущены.

Internet-протокол версии 4 (IPv4) 4 октета
11010001.11011100.11001001.01110001
209.156.201.113
4,294,467,295 IP-адресов

Internet-протокол версии 6 (IPv6) 16 октетов
11010001.11011100.11001001.01110001.11010001.11011100. 110011001.01110001.11010001.11011100.11001001. 01110001.11010001.11011100.11001001.01110001
A524:72D3:2C80:DD02:0029:EC7A:002B:EA73
3.4 x 10^{38} IP-адресов

Рис. 9.35. Сравнение стандартов IPv4 и IPv6

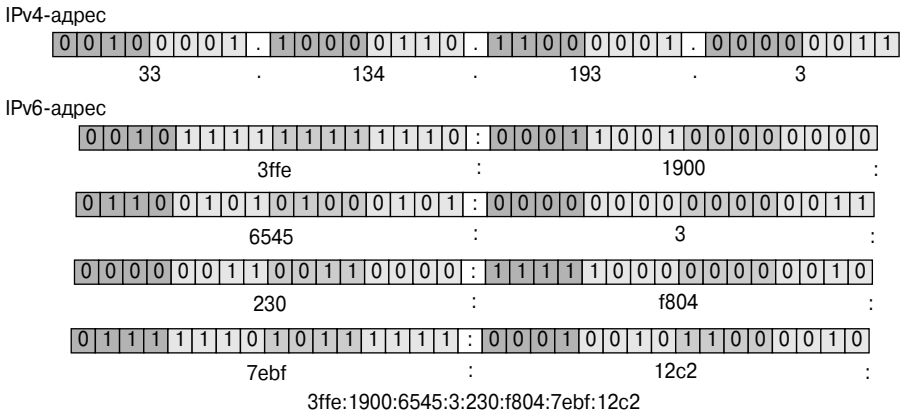


Рис. 9.36. Форматы адресов IPv4 и IPv6

Разработка и планирование технологии заняли годы, прежде чем протокол IPv6 постепенно начал использоваться в отдельных сетях. В перспективе стандарт IPv6 может заменить IPv4 в качестве доминирующего протокола в сети Internet.

Присвоение IP-адресов

В этом разделе рассказывается, каким образом сетевым устройствам присваиваются IP-адреса. Для нормального функционирования сети IP-адреса должны назначаться в соответствии с определенной иерархией. IP-адреса могут выделяться статически или динамически, оба варианта присвоения адресов рассмотрены ниже.

Получение Internet-адреса

Чтобы узел мог функционировать в сети Internet, ему необходимо присвоить глобально уникальный адрес. Физический, или MAC-адрес (Media Access Control — адрес протокола управления доступом к передающей среде) важен только для локальных

взаимодействий. Это означает, что с помощью такого адреса узел может быть идентифицирован только в пределах его собственной локальной сети, и адрес не имеет никакого значения для устройств, в ней не расположенных.

IP — это наиболее распространенная схема адресации. Она является иерархической и позволяет отдельным адресам быть ассоциированными с группами других, как показано на рис. 9.37. Подобные группы позволяют организовывать эффективную передачу информации в сети Internet.

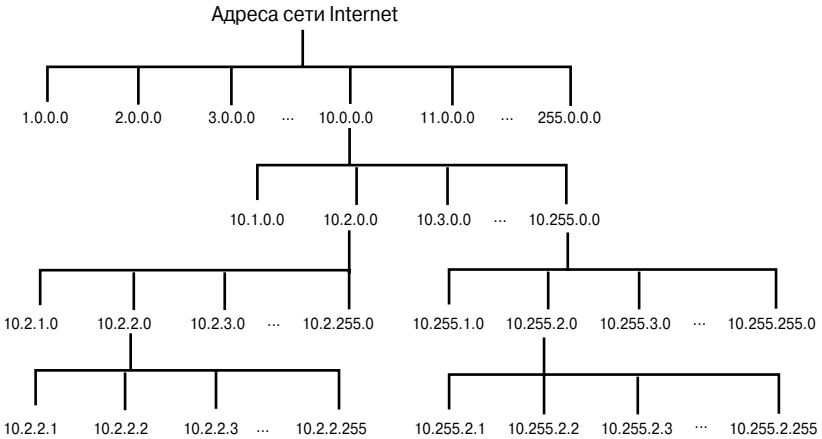


Рис. 9.37. Иерархия адресов сети Internet

Существуют два метода назначения IP-адресов — *статическая адресация (static addressing)* и *динамическая (dynamic addressing)*. Независимо от выбранной схемы, не могут существовать два интерфейса с одинаковыми адресами, поскольку подобная ситуация может привести к конфликту, в котором ни один из вовлеченных в него узлов не сможет нормально функционировать.

Статическое назначение IP-адресов

Когда IP-адреса распределяются статически, каждое устройство обязано иметь свой адрес. Операционные системы по-разному конфигурируют стек протоколов TCP/IP. При использовании этого метода необходимо хранить записи о назначенных IP-адресах, поскольку использование дублирующихся адресов может вызвать проблемы в работе сети. Некоторые операционные системы, такие, как Windows 95 и Windows NT корпорации Microsoft, рассылают ARP-запросы, проверяя уникальность назначенных адресов при попытке инициализации средств набора TCP/IP. Если обнаружено дублирование, протокол инициализирован не будет, что вызовет соответствующее сообщение об ошибке. Не все операционные системы идентифицируют дублирующиеся адреса. Эта особенность опять-таки подчеркивает необходимость иметь подробные записи об адресации устройств.

Основной причиной, по которой устройству может быть выделен постоянный адрес, является необходимость предоставить другим устройствам возможность ссылаться на него. Хорошим примером может служить Web-сервер. Если бы Web-сервер каждый раз при запуске получал новый IP-адрес, его было бы сложно найти. Как наглядный пример того, к чему могут привести подобные изменения адреса, можно представить себе ситуацию, когда в городе постоянно меняются названия улиц и адреса домов. Поиск нужного дома станет невозможен, поскольку ни одна карта не будет соответствовать действительности. Если нужное здание невозможно найти, люди перестанут даже пытаться его искать.

Устройства определенного типа нуждаются в использовании статических IP-адресов. Web-серверы, сетевые принтеры, серверы приложений и маршрутизаторы являются примерами устройств, требующих для своей работы постоянных IP-адресов.

Назначение IP-адресов по протоколу RARP

Протокол определения сетевого адреса по местоположению узла (Reverse Address Resolution Protocol — RARP) устанавливает соответствие между MAC-адресами и IP-адресами. Такая привязка позволяет некоторым сетевым устройствам инкапсулировать данные до их отправки через сеть. Возможна ситуация, когда сетевому устройству или рабочей станции известен MAC-адрес, но не известен собственный IP-адрес. Для устройств, использующих протокол RARP, требуется присутствие RARP-сервера, как показано на рис. 9.38.

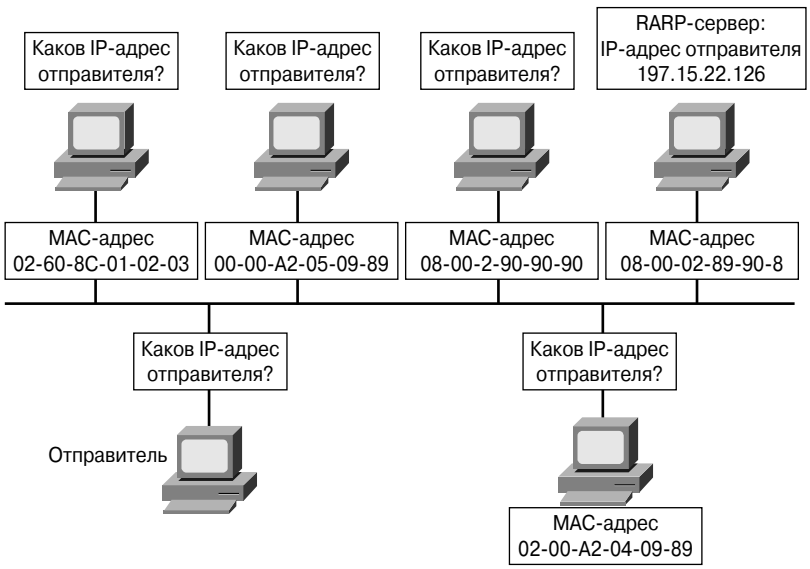


Рис. 9.38. Назначение IP-адресов с помощью протокола RARP

Рассмотрим пример, в котором устройство-отправитель передает данные некоторому устройству. Отправитель знает MAC-адрес получателя, но не может найти

собственный IP-адрес в ARP-таблице. С другой стороны, устройству-получателю, чтобы принять данные, передать их протоколам верхнего уровня модели OSI и ответить отправителю, должны быть известны как MAC-, так и IP-адрес отправителя. Поэтому отправитель инициирует процесс, называемый RARP-запросом, который поможет определить ему свой IP-адрес. Устройство создает пакет RARP-запроса (рис. 9.39) и отправляет его через сеть. Для того чтобы все устройства в сети могли получить пакеты RARP-запроса, используется широковещательный MAC-адрес.

<table>
<tr><th colspan="2">0-15 битов</th><th>16-31 битов</th></tr>
<tr><td colspan="2">Аппаратный тип</td><td>Тип протокола</td></tr>
<tr><td>HLen (1 байт)</td><td>Plen (1 байт)</td><td>Операция</td></tr>
<tr><td colspan="3">HA отправителя (Байтов 1-4)</td></tr>
<tr><td colspan="2">HA отправителя (5-6 байта)</td><td>PA отправителя (1-2 байта)</td></tr>
<tr><td colspan="2">PA отправителя (3-4 байта)</td><td>HA получателя (1-2 байта)</td></tr>
<tr><td colspan="3">HA получателя (3-6 байт)</td></tr>
<tr><td colspan="3">PA получателя (1-4 байта)</td></tr>
<tr><td colspan="3">Структура заголовка RARP</td></tr>
</table>

Рис. 9.39. Структура сообщений ARP/RARP

Составные части заголовка RARP:

- **аппаратный тип** (**Hardware type**) задает тип аппаратного интерфейса, для которого отправитель ожидает ответ;
- **тип протокола** (**Protocol type**) — задает тип адреса для протокола верхнего уровня;
- **поле Hlen (сокращение от Hardware length)** — длина аппаратного адреса;
- **поле Plen (сокращение от Protocol length) —** длина адреса соответствующего протокола;
- **поле Operation —** операция; может принимать следующие значения:
  - 1 — ARP-запрос,
  - 2 — ARP-ответ,
  - 3 — RARP-запрос,
  - 4 — RARP-ответ,
  - 5 — динамический RARP-запрос,
  - 6 — динамический RARP-ответ,
  - 7 — сообщение об ошибке динамического протокола RARP,
  - 8 — InARP-запрос,
  - 9 — InARP-ответ;

- **Sender HA (Sender Hardware Address)** — аппаратный адрес отправителя, который имеет длину, равную HLen байтам;
- **Sender PA (Sender Port Address)** — протокольный адрес отправителя, который имеет длину, равную PLen байтам;
- **Target HA (Target Hardware Address)** — аппаратный адрес получателя, который имеет длину, равную HLen байтам;
- **Target PA (Target Port Address) —** протокольный адрес получателя, который имеет длину, равную PLen байтам.

Протокол RARP использует тот же формат пакета, что и протокол ARP. Однако значения MAC-заголовка и кода операции для RARP-запроса отличаются от аналогичных полей ARP-запроса. Формат пакета RARP содержит позиции для MAC-адресов отправителя и получателя, поле IP-адреса отправителя пусто. Широковещательный запрос адресуется всем абонентам в сети, для этого адрес получателя состоит из одних единиц. Станция, использующая протокол RARP, содержит в своем ПЗУ программный код, который запускает процесс поиска адреса RARP (рис. 9.40).

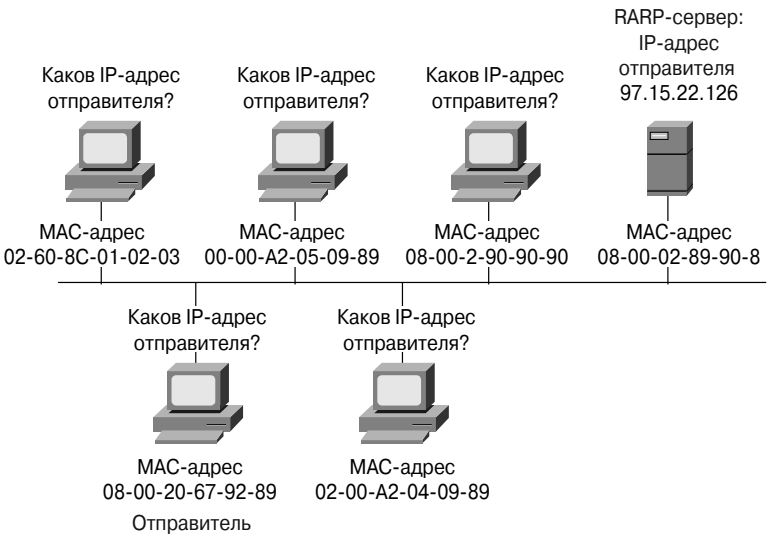


Рис. 9.40. Схема работы протокола RARP

Назначение IP-адресов с использованием протокола BOOTP

Подобно протоколу RARP, протокол начальной загрузки BOOTP работает в клиент-серверном окружении, и для получения необходимой информации требуется обмен всего одним пакетом. Однако в отличие от механизма RARP, возвращающего только лишь четырехоктетный IP-адрес, пакет протокола BOOTP, помимо IP-адреса, может содержать также адрес стандартного шлюза, адрес сервера и дополнительную информацию, определяемую производителем оборудования (рис. 9.41).

Одна из проблем протокола BOOTP связана с тем, что он не был разработан для динамического назначения адресов. При использовании этого протокола работа по созданию конфигурационного файла, хранящего необходимые параметры, ложится на администратора. Он должен сам добавлять узлы и обслуживать базу данных протокола BOOTP. Несмотря на то что адреса назначаются динамически, существует взаимно однозначное соответствие между количеством IP-адресов и количеством узлов в сети. Фактически это означает, что для каждого компьютера в сети должен существовать соответствующий BOOTP-профиль, определяющий предназначенный для него IP-адрес. Не могут существовать два профиля с одинаковыми IP-адресами, поскольку они могут быть востребованы одновременно, что означало бы использование в сети двух компьютеров с одинаковыми IP-адресами.

0-7 биты	8-15 биты	16-24 биты	25-31 биты
Op (1)	Htype (1)	Hlen (1)	Hops (1)
Xid (4 байта)			
Секунды (2 байта)		Не используется	
Ciaddr (4 байта)			
Yiaddr (4 байта)			
Siaddr (4 байта)			
Giaddr (4 байта)			
Chaddr (16 байтов)			
Имя сервера (32 байта)			
Имя загрузочного файла (64 байта)			
Область, зависящая от производителя (32 байта)			
Структура сообщения BOOTP			

Рис. 9.41. Структура BOOTP-сообщения

Устройство использует BOOTP-протокол во время загрузки для получения IP-адреса. Инкапсулируемые в IP-пакетах BOOTP-сообщения используют протокол UDP. Компьютер использует протокол BOOTP для отправки широковещательного IP-пакета (используя адрес получателя, в котором установлены двоичные единицы во всех позициях адреса, — 255.255.255.255 в точечно-десятичном формате). BOOTP-сервер, отвечая на широковещательный пакет, отправляет широковещательное сообщение. Клиент, получив ответ, проверяет MAC-адрес. Если он находит соответствие между адресом получателя в широковещательном пакете, полученном от сервера, и собственным физическим адресом, он сохраняет IP-адрес и другую полезную информацию, хранящуюся в сообщении BOOTP-ответа.

Выделение адресов с помощью протокола DHCP

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol — DHCP) является преемником протокола BOOTP. В отличие от последнего, протокол DHCP позволяет динамически получить IP-адрес, не прибегая к создаваемым администратором профилям для каждой конкретной машины. Все, что нужно, — это назначить диапазон доступных адресов на DHCP-сервере. Соединяющиеся с сетью узлы подключаются к DHCP-серверу и запрашивают необходимые им IP-адреса. Сервер выбирает один из незанятых адресов и выделяет его узлу. С помощью протокола DHCP вся необходимая информация о конфигурации протокола TCP/IP может быть передана клиенту в одном сообщении. Она включает все сведения, которые может передавать протокол BOOTP, плюс выделенный IP-адрес и маску подсети.

Основное преимущество протокола DHCP перед BOOTP заключается в том, что этот протокол дает пользователям мобильность. Они могут свободно перемещаться с места на место, меняя точку подключения к сети. При использовании сервера DHCP больше нет необходимости в создании жестких профилей для каждого сетевого устройства, как это было в BOOTP-системах. Такая гибкость достигается благодаря тому, что протокол DHCP может выделять IP-адрес одному устройству, а после его освобождения — передавать другому. Такой механизм работы означает, что для IP-адресов выполняется отношение “один ко многим” и, следовательно, адрес может быть доступен любому устройству, подключенному к сети.

Дополнительная информация: сообщения и состояния протокола DHCP

Протокол DHCP использует тот же формат сообщения, что и BOOTP, но с несколькими исключениями (рис. 9.42). Поле, которое не используется в механизме BOOTP, в данном протоколе зарезервировано в качестве поля флага. Наиболее значимым битом является флаг: он задает широковещательное сообщение. Протокол DHCP, как и BOOTP, хранит следующую задаваемую производителем информацию:

- однобайтовое поле опций;
- однобайтовое поле длины;
- поле переменной длины (задается в поле длины) данных опции.

Для разных типов DHCP-сообщения допустимы следующие значения:

- число 53 в поле опций указывает на DHCP-сообщение;
- единица в значении длины поля указывает на то, что поле данных имеет длину 1 байт.

В процессе загрузки DHCP-клиент входит в режим инициализации. Он посылает широковещательное сообщение DHCPDISCOVER, являющееся UDP-пакетом, с номером порта, таким же, как у протокола BOOTP. После отправки пакетов DHCPDISCOVER клиент переходит в режим прослушивания ответов DHCPOFFER от сервера и выбора сервера. Клиент обрабатывает первый полученный ответ и начинает процедуру утверждения времени действия выбранного адреса, отправляя DHCP-серверу пакет DHCPREQUEST. На следующем этапе сервер подтверждает запрос клиента с помощью пакета DHCPACK. После этого клиент переходит в так называемое связанное состояние и может начинать использование выделенного ему IP-адреса. На рис. 9.43 проиллюстрирована обобщенная информация о DHCP-режимах.

0-7 биты	8-15 биты	16-24 биты	25-31 биты
Op (1)	Htype (1)	Hlen (1)	Hops (1)
Xid (4 байтов)			
Секунды (2 байта)		Флаги (2 байта)	
Ciaddr (4 байта)			
Yiaddr (4 байта)			
Siaddr (4 байта)			
Giaddr (4 байта)			
Chaddr (16 байтов)			
Имя сервера (32 байта)			
Имя загрузочного файла (64 байта)			
Область, зависящая от производителя (32 байта)			
Структура сообщения DHCP			

Рис. 9.42. Структура DHCP-сообщения

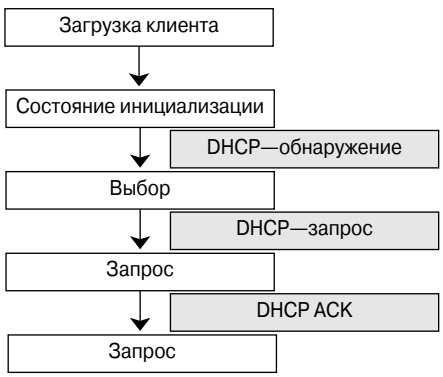


Рис. 9.43. Режимы протокола DHCP

Практическое задание 9.3.5. Настройка DHCP-клиента
В этом задании предлагается установить в сети компьютер в качестве DHCP-клиента для использования службы DHCP.

Проблемы при определении адресов

Одной из основных проблем сетевых технологий является вопрос о том, как организовать взаимодействие между сетевыми устройствами. В TCP/IP-взаимодействиях дейтаграмма в локальной сети обязана содержать как MAC-адрес, так и IP-адрес получателя. На рис. 9.44 компьютер с адресом 176.10.16.1 хочет передать информацию компьютеру с адресом 176.10.16.4. Каким же образом он получает необходимый для такого обмена данными MAC-адрес?

Все адреса должны быть корректными и в точности соответствовать MAC- и IP-адресу узла, в противном случае получатель просто отвергнет неправильные пакеты. Таким образом, в локальной сети должен существовать механизм автоматического разрешения (или трансляции) IP-адресов в адреса физического уровня — MAC. Выполнить такую задачу вручную было бы для пользователей обременительно и потребовало бы много времени. Такое решение применимо только для локальных сетей; в случае, когда данные адресуются за пределы локальной сети, появляются новые проблемы.

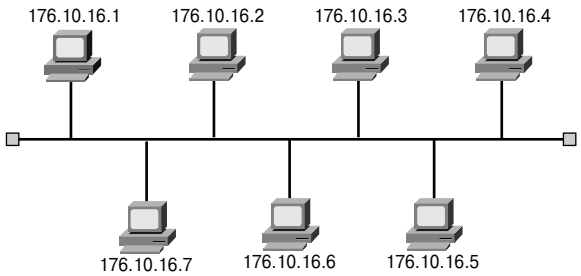


Рис. 9.44. Проблемы преобразования адресов

При взаимодействии с устройствами, не находящимися в локальном сетевом сегменте, возникают два вопроса:

- как получить MAC-адреса промежуточных устройств;
- как передавать пакеты с данными из одного сетевого сегмента в другой до тех пор, пока они не достигнут получателя.

Пример, приведенный на рис. 9.45, служит иллюстрацией такой проблемы. Компьютеру с адресом 192.168.10.34 необходимо передать информацию другому компьютеру с адресом 192.168.1.1. Каким образом он может получить MAC-адрес для IP-адреса 192.168.1.1? Следует помнить, что MAC-адрес может быть использован только в пределах локальной сети. От него будет мало пользы вне сети с адресом 192.168.10.0. Значит, для того чтобы передать данные из локальной сети в сеть глобальную, необходимо знать MAC-адрес маршрутизатора.

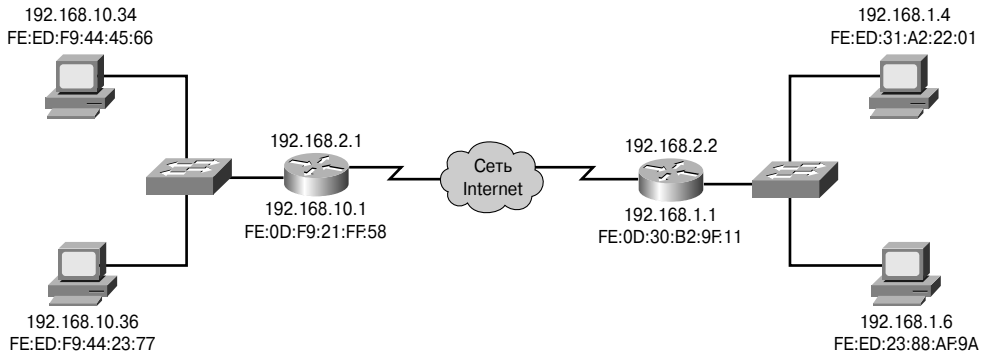


Рис. 9.45. Проблемы преобразования удаленных адресов

Дополнительная информация: кэширование ARP-запросов

На маршрутизаторах могут быть запущены кэширующие агенты протокола ARP (proxy ARP), которые перехватывают все ARP-пакеты. В ответ на ARP-запросы, в которых IP-адреса находятся вне диапазона адресов локальной сети, в качестве ответа они выдают свой собственный MAC-адрес. В примере, который проиллюстрирован на рис. 9.46, если узел A посылает ARP-запрос узлу F, маршрутизатор, обслуживая этот запрос, возвращает устройству A свой собственный MAC-адрес, связывая его с IP-адресом узла F. Выше говорилось о том, что информация может быть передана в другую подсеть благодаря использованию соответствующим образом настроенного стандартного шлюза. Если же у отправителя отсутствует конфигурационная запись о стандартном шлюзе, он посылает ARP-запрос. Маршрутизатор сравнивает IP-адрес получателя с адресом подсети, чтобы определить, находится ли получатель в той же подсети, что и отправитель. Если это так, маршрутизатор отбрасывает такой пакет; пакет отбрасывается потому, что IP-адрес получателя находится в том же сегменте сети, что и IP-адрес получателя. Такое поведение предполагает, что на ARP-запрос в этом случае должен ответить сам получатель, а не маршрутизатор. Исключением является ситуация, когда IP-адрес еще не назначен, в результате чего отправитель получит сообщение об ошибке.

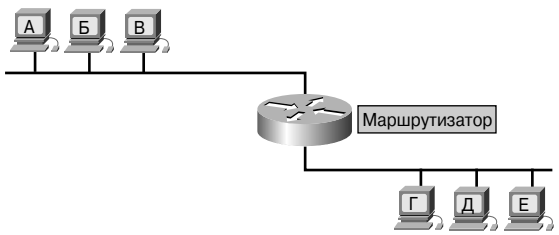


Рис. 9.46. Пример кэширования протокола ARP

Протокол преобразования адресов (ARP)

Для взаимодействия устройств друг с другом необходимо, чтобы у передающего устройства был IP- и MAC-адреса получателя. Когда одно из устройств пытается установить связь с другим, с известным IP-адресом, ему необходимо определить

MAC-адрес получателя. Набор протоколов TCP/IP имеет в своем составе специальный протокол, называемый ARP (Address Resolution Protocol — протокол преобразования адресов), который позволяет автоматически получить MAC-адрес. На рис. 9.47 проиллюстрирован процесс, позволяющий определить MAC-адрес, связанный с известным IP-адресом.

Некоторые устройства хранят специальные ARP-таблицы, в которых содержится информация о MAC- и IP-адресах других устройств, подключенных к той же локальной сети. ARP-таблицы позволяют установить однозначное соответствие между IP- и MAC-адресами. Такие таблицы хранятся в определенных областях оперативной памяти и обслуживаются автоматически на каждом из сетевых устройств (табл. 9.10 и 9.11). В редких случаях приходится создавать ARP-таблицы вручную. Обратите внимание, что каждый компьютер в сети поддерживает свою собственную ARP-таблицу.

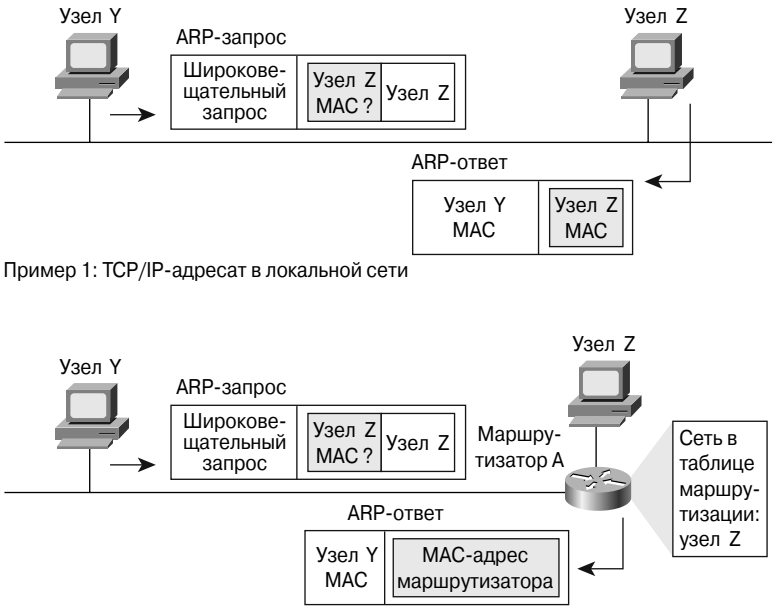


Рис. 9.47. Получение IP-адресов через MAC-адреса

Таблица 9.10. Запись в ARP-таблице

Internet-адрес	Физический адрес	Тип
68.2.168.1	00-50-57-00-76-84	Динамический

Таблица 9.11. ARP-таблица для адреса 198.150.11.36

MAC-адрес	IP-адрес
FE:ED:F9:44:45:66	198.150.11.34
DD:EC:BC:AB:04:AC	198.150.11.33
DD:EC:BC:00:94:D4	198.150.11.35
FE:ED:F9:23:44:EF	198.150.11.36

Куда бы не передавались сетевым устройством данные, для их пересылки всегда используется информация, хранящаяся в ARP-таблице (рис. 9.48; одно из устройств хочет передать данные другому устройству).

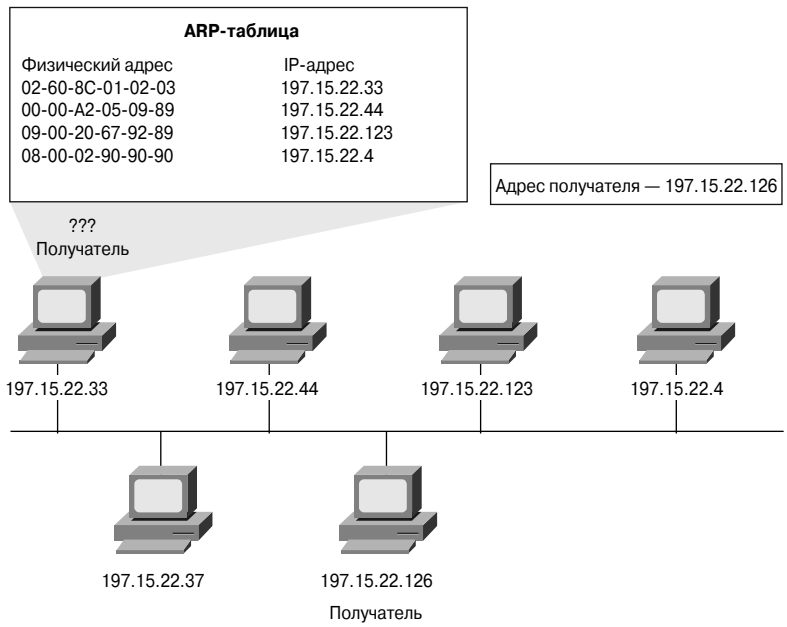


Рис. 9.48. ARP-таблицы

Функционирование протокола ARP в подсетях

Для передачи данных от одного узла другому отправитель должен знать IP- и MAC-адрес получателя. Если он не может получить искомый физический адрес из собственной ARP-таблицы, инициируется процесс, называемый ARP-запросом, который проиллюстрирован на рис. 9.48.

ARP-запрос позволяет узлу определить MAC-адрес получателя. Узел создает фрейм ARP-запроса и рассылает его всем сетевым устройствам. Фрейм ARP-запроса состоит из двух частей:

- заголовка фрейма;
- сообщения ARP-запроса.

Для того чтобы все устройства могли получить ARP-запрос, используется широковещательный MAC-адрес. В схеме MAC-адресации широковещательный адрес содержит во всех битах шестнадцатеричное число F и имеет, таким образом, вид FF-FF-FF-FF-FF-FF[5]. Поскольку пакеты ARP-запроса передаются в широковещательном режиме, все сетевые устройства, подключенные к локальной сети, могут получить такие пакеты и передать их протоколам более высоких уровней для последующей обработки. Если IP-адрес устройства совпадает с IP-адресом получателя в широковещательном ARP-запросе, это устройство отвечает отправителю, сообщая свой MAC-адрес. Такое сообщение называется *ARP-ответом*.

После получения ARP-ответа устройство-отправитель широковещательного ARP-запроса извлекает MAC-адрес из поля аппаратного адреса отправителя и обновляет свою ARP-таблицу. Теперь это устройство может надлежащим образом адресовать пакеты, используя как MAC-, так и IP-адрес. Полученная информация используется для инкапсуляции данных на втором и третьем уровнях перед их отправкой по сети. Когда данные достигают пункта назначения, на канальном уровне проводится проверка на соответствие адреса, отбрасывается канальный заголовок, который содержит MAC-адреса, и данные передаются на сетевой уровень. На сетевом уровне проверяется соответствие собственного IP-адреса и IP-адреса получателя, содержащегося в заголовке третьего уровня. На сетевом уровне отбрасывается IP-заголовок, и инкапсулированные данные передаются на следующий уровень модели OSI —транспортный (уровень 4). Подобный процесс повторяется до тех пор, пока оставшиеся, частично распакованные, данные не достигнут приложения (уровень 7), в котором будет прочитана пользовательская часть данных.

Стандартный шлюз

Стандартным шлюзом называется IP-адрес интерфейса маршрутизатора, подключенного к локальной сети, в которой находится передающий узел. IP-адрес стандартного шлюза должен находиться в том же сетевом сегменте, в котором находится передающий узел (рис. 9.49).

Практическое задание 9.3.7. Изучение протокола ARP
В этом задании используется ARP-таблица рабочей станции и команда **`arp –a`** для проверки успешного преобразования компьютером сетевых адресов (третьего уровня) в MAC-адреса (второго уровня).

Презентация: протокол ARP
В этой презентации представлен видеоролик, который иллюстрирует работу протокола ARP и механизм обнаружения MAC-адресов станций.

[5] *Такая запись MAC-адреса называется канонической, в ней части адреса разделены дефисом (-); существует также альтернативная запись, в которой части адреса разделены двоеточием (:). — Прим. ред.*

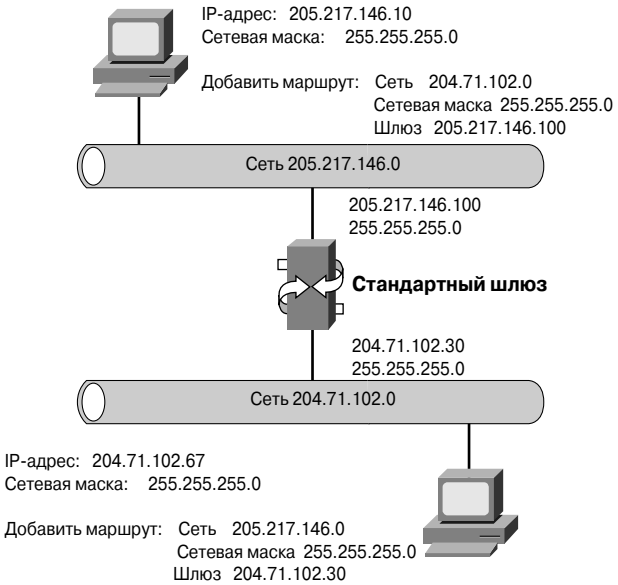


Рис. 9.49. Стандартный шлюз

Резюме

В этой главе были рассмотрены следующие ключевые понятия:

- министерство обороны США разработало эталонную модель и стек протоколов TCP/IP для реализации сети, которая выстоит и сохранит работоспособность в любых условиях;
- уровень приложений модели TCP/IP отвечает за взаимодействие с протоколами верхних уровней, представление данных, кодирование и управление диалогом;
- функции межсетевого взаимодействия Internet-уровня включают в себя сетевую адресацию и выбор наилучшего маршрута доставки сетевого трафика;
- уровень доступа к среде сети должен обеспечить обработку всех запросов IP-пакетов на доступ к физической среде передачи данных, а также обеспечить установление физического канала между узлами сети;
- чтобы облегчить администрирование и повысить гибкость, сети, в особенности большие, часто делятся на более мелкие, называемые подсетями. Использование подсетей позволяет администраторам обойти ограничения, связанные с адресацией протокола IPv4; они разделяют один сетевой адрес на множество подсетей, которые различимы только в пределах главной сети;
- функция маски подсети состоит в указании той части адреса, которая является адресом сети, включая подсеть, и части, отведенной для адреса узла;

- сетевой уровень эталонной модели взаимодействия открытых систем призван обеспечить сетевую адресацию и выбор наилучшего маршрута доставки для сетевого трафика;
- в главе была рассмотрена эволюция IP-адресации, включая необходимость увеличения размера адресного пространства IP и увеличения длины адреса;
- были описаны IP-адресация, классы IP-адресов, зарезервированный набор IP-адресов, пространство частных IP-адресов и IP-подсетей;
- компьютеру для взаимодействия с узлами в сети Internet необходим IP-адрес (иерархический адрес);
- существуют два способа задания IP-адресов: статический и динамический;
- есть несколько способов динамического назначения IP-адресов: когда устройству не известен собственный IP-адрес, оно использует RARP, BOOTP или DHCP. Когда устройство получает RARP-ответ на сделанный RARP-запрос, оно копирует свой IP-адрес в кэш памяти для хранения на протяжении всего сеанса;
- протокол DHCP предоставляет клиентам мобильность, позволяя, если требуется, подключаться ко множеству различных сетей.

После прочтения этой главы обратитесь к соответствующим интерактивным материалам, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom).

Ключевые термины

Адреса класса A разработаны для поддержки очень больших сетей. В адресе этого класса используется только первый октет для описания адреса сети. Остальные три октета служат для указания адресов узлов.

Адреса класса B разработаны для поддержки больших и средних сетей. В адресе этого класса используются два октета из четырех для описания адреса сети. Остальные два служат для указания адресов узлов.

Адреса класса C — это наиболее широко используемый класс адресов. Данное адресное пространство предполагалось использовать для поддержки большого числа малых сетей.

Адреса класса D созданы для поддержки механизма многоадресатной рассылки.

Адреса класса E были зарезервированы проблемной группой проектирования Internet (Internet Engineering Task Force — IETF) для собственных исследовательских нужд. Таким образом, адреса этого класса никогда не были использованы в сети Internet.

Класс IP-адреса — 32-битовый адрес, делится на сетевую и узловую части. Бит или последовательность битов в начале любого адреса задают его класс.

Механизм создания подсетей (subnetting) — метод деления полного адреса любого из классов на более мелкие части. Этот механизм позволил избежать полного исчерпания доступных IP-адресов (версии 4).

Многоадресатный адрес (multicast address) — уникальный сетевой адрес, позволяющий направить пакеты предопределенной группе узлов.

Протокол IP версии 6 (IPv6) — замена текущей версии протокола IP версии 4 (IPv4). Протокол IPv6 включает поддержку механизма идентификации потока (flow ID) в заголовке пакета. Изначально его называли IPng (IP next generation — IP нового поколения).

Протокол управления передачей/Internet-протокол (Transmission Control Protocol/Internet Protocol — TCP/IP) — общее название набора протоколов, разработанных в 1970 году Министерством обороны США для создания глобальной распределенной сети. TCP и IP — два наиболее известных протокола этого набора.

Точечно-десятичный формат. В этом формате IP-адреса записываются в виде четырех частей, разделенных точками.

Транспортный уровень предоставляет транспортные услуги на всем пути от отправителя до получателя. Он занимается установкой логического соединения между конечными точками сетевого взаимодействия: узлом-отправителем и получателем.

Уровень приложений обслуживает протоколы верхнего уровня и выполняет функции, связанные с обработкой данных и контролем взаимодействия. Набор протоколов TCP/IP объединяет все функции, относящиеся к работе приложений (уровень приложений, представления и сеансовый), в один уровень и гарантирует необходимую упаковку данных для передачи другим уровням.

Уровень сетевого доступа (network access layer) — уровень, обслуживающий все запросы, связанные с организацией физической связи между IP-пакетами и средой передачи.

Широковещательный адрес используется для широковещательной рассылки пакетов всем сетевым устройствам.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Какой транспортный механизм использует протокол TFTP?

а) TCP.

б) IP.

в) UDP.

г) CFTP.

2. Какой из предложенных ниже вариантов является основной функцией транспортного уровня?

а) Благодаря использованию механизмов упорядоченной нумерации и уведомлений уровень гарантирует доставку информации.

б) Разбивает данные приложений верхнего уровня на сегменты.

в) Устанавливает и поддерживает сквозное взаимодействие.

г) Все перечисленное выше.

3. Какие из перечисленных протоколов работают на Internet-уровне модели TCP/IP?

а) IP.

б) ICMP.

в) ARP.

г) Все перечисленные выше.

4. Какое сообщение отправляется первым при загрузке DHCP-клиента?

а) DHCPREQUEST.

б) DHCPBOOT.

в) DHCPDISCOVER.

г) Ни одно из перечисленных.

5. Каким образом сетевой уровень организует пересылку пакетов от отправителя получателю?

а) На основе записей в таблице маршрутизации.

б) Используя ARP-ответ.

в) Используя запрос к серверу имен.

г) Обращаясь к мосту.

6. Если устройство не знает MAC-адрес устройства из смежной сети, кому оно адресует ARP-запрос?

а) Стандартному шлюзу.

б) Ближайшему маршрутизатору.

в) Интерфейсу маршрутизатора.

г) Всем устройствам в сети.

7. Из каких двух частей состоит IP-адрес?

а) Из адреса сети и адреса узла.

б) Из адреса сети и MAC-адреса.

в) Из адреса узла и MAC-адреса.

г) Из MAC-адреса и маски подсети.

8. Какой Internet-протокол используется для установления соответствия между известным IP-адресом и неизвестным MAC-адресом?

а) UDP.

б) ICMP.

в) ARP.

г) RARP.

9. Что из перечисленного ниже инициирует ARP-запрос?

а) Устройство, которое может найти IP-адрес получателя в своей ARP-таблице.

б) RARP-сервер в ответ на сообщение неверно функционирующего устройства.

в) Бездисковая станция, кэш которой пуст.

г) Устройство, которое не может найти IP-адрес получателя в своей ARP-таблице.

10. Какое из утверждений лучше всего описывает ARP-таблицу?

а) Способ уменьшения сетевого трафика посредством использования списка кратчайших маршрутов до пунктов назначения.

б) Способ маршрутизации данных внутри сетей, разделенных на подсети.

в) Протокол, преобразовывающий информацию на уровне приложений при ее передаче от одного стека другому.

г) Область оперативной памяти на каждом устройстве, с помощью которой устанавливается соответствие между IP- и MAC-адресами.

11. Какой из перечисленных ниже вариантов лучше всего описывает ARP-ответ?

а) Устройство отправляет свой MAC-адрес в ответ на ARP-запрос.

б) Кратчайший маршрут между отправителем и получателем.

в) Обновление ARP-таблицы посредством перехвата и чтения пакетов, передаваемых по сети.

г) Способ нахождения IP-адреса на основе MAC-адреса, используемый в основном RARP-серверами.

12. Почему важно иметь актуальные, обновленные ARP-таблицы?

а) Они нужны для проверки сетевых связей.

б) Они необходимы для уменьшения количества широковещательных рассылок.

в) Чтобы сократить время, которое администратор тратит на поддержку сети.

г) Для разрешения конфликтов адресов.

13. Что из перечисленного ниже наилучшим образом описывает стек TCP/IP?

а) Это набор протоколов, который может быть использован для организации взаимодействия внутри группы объединенных сетей.

б) Это набор протоколов, позволяющий подключить локальные сети к глобальным.

в) Это набор протоколов, позволяющий организовать передачу информации через множество сетей.

г) Это набор протоколов, дающий возможность совместно использовать различные устройства в объединенных сетях.

14. Что из перечисленного ниже не является описанием набора протоколов TCP/IP?

а) Он точно соответствует описанию верхних уровней модели OSI.

б) Он поддерживает все стандартные протоколы физического доступа и канального уровня.

в) Он передает данные посредством последовательностей дейтаграмм.

г) Он собирает дейтаграммы в исходное сообщение в пункте назначения.

15. Для каких уровней модели OSI набор протоколов TCP/IP имеет спецификации?

а) С 1 по 3.

б) С 1 по 4 и 7.

в) Для 3, 4 и с 5 по 7.

г) Для 1, 3 и 4.

16. Что из перечисленного ниже **не** является функцией сетевого уровня?

а) Протокол RARP определяет сетевые адреса. когда известны адреса канального уровня.

б) Протокол ICMP предоставляет возможности контроля и передачи сообщений.

в) Протокол ARP определяет адреса канального уровня для известных IP-адресов.

г) Протокол UDP предоставляет механизм обмена дейтаграммами без подтверждений о доставке и без установления соединения.

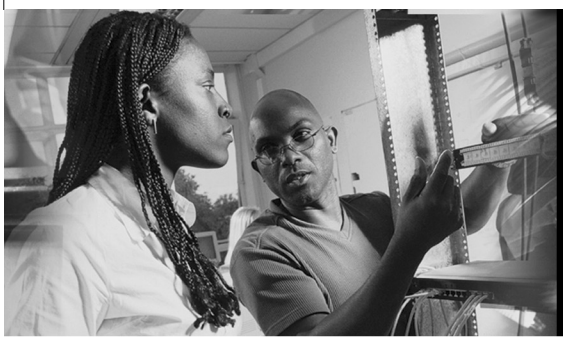
17. Какой из перечисленных ниже протоколов относится к транспортному уровню?

а) UCP.

б) UDP.

в) TDP.

г) TDC.



ГЛАВА 10

Основы маршрутизации и принципы построения подсетей

В этой главе...

- описано назначение маршрутизируемых протоколов и протоколов маршрутизации, как, например, механизмы протокола IP;
- рассмотрены функции протокола IP и проведено сравнение механизмов передачи данных с установлением и без установления соединения;
- объясняется работа маршрутизаторов на третьем уровне модели OSI;
- описан формат сообщений и назначение полей в сообщениях протоколов маршрутизации;
- проведен сравнительный анализ коммутации второго уровня и маршрутизации третьего в модели OSI;
- дано определение протокола маршрутизации, описаны механизмы поиска наилучшего маршрута для потока данных и рассмотрены механизмы, которые обеспечивают актуальность таблиц маршрутизации;
- описаны различия между статической и динамической маршрутизацией;
- объясняется, как маршрутизаторы используют функции выбора маршрута и коммутации для передачи пакетов через объединенные сети;
- описаны различия дистанционно-векторных протоколов маршрутизации и протоколов маршрутизации с учетом состояния каналов, а также рассмотрены особенности их конвергенции;
- рассмотрены различия протоколов маршрутизации внешних и внутренних шлюзов, а также приведены примеры каждого из типов протоколов;
- объяснены особенности и преимущества разбиения сетей на подсети;
- описано, как создавать подсети с помощью сетевой маски и рассчитывать количество узлов и сетей;
- Показано, как рассчитать адрес сети с использованием логической операции AND.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

протокол, с. 491,
маршрутизируемый протокол, с. 491,
пакет, с. 491,
протокол маршрутизации, с. 492,
IP-адрес, с. 493,
протокол без установления соединения, с. 494,
дейтаграмма, с. 494,
домен коллизий, с. 496,
система доставки с установлением соединения, с. 499,
маршрутизатор, с. 501,
метрика маршрутизации, с. 502,
широковещательный домен, с. 504,
подсети, с. 504,
таблица маршрутизации, с. 505,
MAC-адрес, с. 513,
широковещательные рассылки, с. 514,
счетчик транзитных узлов, с. 516,
алгоритмы маршрутизации, с. 517,
протоколы внутренних шлюзов, с. 519,
протоколы внешних шлюзов, с. 519,
автономная система, с. 519,
алгоритм дистанционно-векторной маршрутизации, с. 520,
протокол маршрутной информации, с. 521,
протокол маршрутизации внутреннего шлюза, с. 521,
усовершенствованный протокол маршрутизации внутреннего шлюза, с. 521,
алгоритм с учетом состояния каналов, с. 521,
бесклассовая междоменная маршрутизация, с. 525,
октет, с. 527,
адрес подсети, с. 528.

Эта глава посвящена вопросам, связанным с работой фундаментального протокола сети Internet (Internet Protocol — IP). В ней обсуждаются вопросы доставки сообщений IP, процессы модификации заголовка устройствами третьего уровня и фактическая структура IP-пакета. В главе также обсуждается связь между сетевыми службами с установлением и без установления соединения и объясняется разница между протоколами маршрутизации и маршрутизируемыми протоколами, а также механизмы, используемые маршрутизаторами для определения расстояния между удаленными точками. Глава ознакомит читателя с технологиями маршрутизации по вектору расстояния (distance-vector), состоянию канала (link-state) и гибридной (hybrid) технологией и расскажет о том, как каждая из них решает общие проблемы маршрутизации.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Маршрутизируемые протоколы

Протокол IP (Internet-протокол) является маршрутизируемым протоколом сети Internet. Пакеты маршрутизируются по оптимальному пути от отправителя к получателю на основе уникальных идентификаторов — IP-адресов. Данные могут быть правильно доставлены получателю в том случае, если в сети требуемым образом работают механизмы пересылки пакетов, устройства, преобразующие данные из одного формата в другой, а также протоколы с установлением и без установления соединения. В первой части главы основное внимание уделено именно перечисленным выше компонентам сети передачи данных.

Маршрутизируемые и маршрутизирующиеся протоколы

Протоколом называется основанный на стандартах набор правил, определяющий принципы взаимодействия компьютеров в сети. Протокол также задает общие правила взаимодействия разнообразных приложений, сетевых узлов или систем, создавая таким образом единую среду передачи. Взаимодействующие друг с другом компьютеры обмениваются данными; чтобы принять и обработать сообщения с данными, компьютерам необходимо знать, как сформированы сообщения и что они означают. Примерами использования различных форматов сообщений в разных протоколах могут служить установление соединения с удаленной машиной, отправка сообщений по электронной почте или передача файлов и данных; интуитивно понятно, что разные службы используют разные сообщения.

Протокол описывает:

- формат сообщения, которому приложения обязаны следовать;
- способ обмена сообщениями между компьютерами в контексте определенного действия, такого, как отправка сообщений по сети.

Схожее звучание терминов “маршрутизируемый протокол” и “протокол маршрутизации” нередко приводит к путанице. Приведенные ниже определения помогут прояснить ситуацию.

- *Маршрутизируемый протокол* — это любой сетевой протокол, адрес сетевого уровня которого предоставляет достаточное количество информации для доставки пакета от одного сетевого узла другому на основе используемой схемы адресации. Такой протокол задает форматы полей внутри *пакета*. Пакеты обычно передаются от одной конечной системы другой. Маршрутизируемый протокол использует таблицу маршрутизации для пересылки пакетов. Примеры маршрутизируемых протоколов приведены на рис. 10.1. В их число входят:

- Internet-протокол (IP);
- протокол межсетевого пакетного обмена (Internetwork Packet Exchange — IPX);
- протокол AppleTalk.

Легче всего запомнить, что такое маршрутизируемые протоколы, если помнить, что это протоколы, которые связаны с передачей данных.

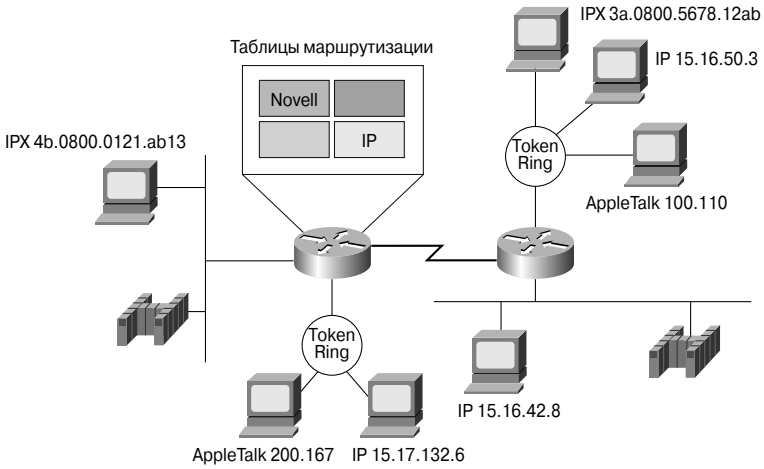


Рис. 10.1. Маршрутизируемые протоколы

- *Протокол маршрутизации* — это протокол, который поддерживает маршрутизируемые протоколы и предоставляет механизмы обмена маршрутной информацией. Сообщения протокола маршрутизации передаются между маршрутизаторами. Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией друг с другом для обновления записей и поддержки таблиц маршрутизации. Ниже приводятся некоторые примеры протоколов маршрутизации TCP/IP:
  - протокол маршрутной информации (Routing Information Protocol — RIP);
  - протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP);
  - усовершенствованный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP);
  - протокол первоочередного обнаружения кратчайших маршрутов (Open Shortest Path First — OSPF).

  Легче всего запомнить, что такое протоколы маршрутизации, если представлять себе, что это протоколы обмена маршрутной информацией.

Чтобы протокол был маршрутизируемым, в нем должны наличествовать механизмы назначения как номера сети, так и номера узла для каждого отдельного сетевого устройства. В некоторых протоколах, таких, как, например, IPX, необходимо назначить только адрес сети, поскольку в качестве адреса устройства эта технология использует физический адрес (MAC-адрес) устройства. Другие протоколы, такие, как IP, требуют, чтобы явно был задан весь адрес и сетевая маска.

Для создания маршрутизируемой сети необходимы как *IP-адрес*, так и *маска сети*. Сетевая маска делит 32-битовый IP-адрес на сетевую часть и адрес узла. Протокол IPX использует MAC-адрес, объединенный с установленным администратором номером сети, для создания полного адреса и не требует использования сетевой маски. При использовании IP-технологий адрес сети вычисляется путем сравнения полного адреса и маски подсети.

Сетевая маска позволяет рассматривать группу последовательных IP-адресов как единое целое. Без такой возможности группировки адресов потребовался бы механизм маршрутизации для каждого отдельного узла. Такая схема была бы непригодна для миллионов узлов, работающих в сети Internet. На рис. 10.2 показано, что все 254 адреса в диапазоне от 192.168.10.1 до 192.168.10.254 могут быть представлены одним сетевым адресом 192.168.10.0. Такая возможность позволяет адресовать информацию любому из этих узлов, используя соответствующий адрес сети. Таким образом, таблицы маршрутизации должны содержать всего одну запись — 192.168.10.0 — вместо 254 записей для каждого отдельного узла. Описанный выше подход стандартизован Консорциумом программного обеспечения сети Internet (Internet Software Consorcium — `http://www.isc.org`). Чтобы маршрутизация могла правильно функционировать, рекомендуется использовать группирование адресов.

В последующих разделах описано, как в маршрутизаторах реализованы базовые функции третьего уровня в рамках эталонной модели взаимодействия открытых систем (Open Systems Interconnection — модель OSI). Показано, в чем состоит разница между протоколами маршрутизации и маршрутизируемыми протоколами и реализованными в маршрутизаторах механизмами определения расстояния между удаленными точками. В конце главы подробно описаны технологии маршрутизации по вектору расстояния (distance-vector), состоянию канала (link-state) и гибридная маршрутизация (hybrid), рассказано о том, как каждый тип маршрутизации решает общие проблемы поиска маршрутов и взаимодействия.

Презентация: сравнение маршрутизируемых протоколов и протоколов маршрутизации
В этой видеопрезентации рассматриваются основные различия между протоколами маршрутизации и маршрутизируемыми протоколами. В ней также проиллюстрированы сферы применения протоколов обоих типов.

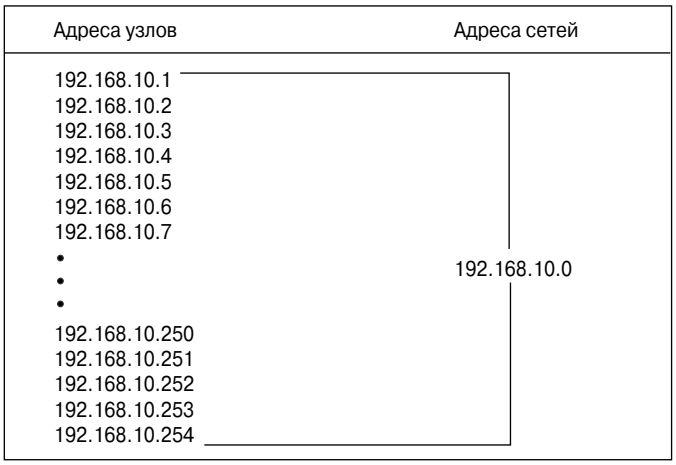


Рис. 10.2. Адреса сетей и узлов

IP как маршрутизируемый протокол

Протокол IP является наиболее широко распространенной реализацией иерархической схемы сетевой адресации. Используемый в сети Internet, протокол IP не отвечает за установку соединений, не является надежным и позволяет реализовать только негарантированную доставку данных. Термин *протокол без установления соединения (connectionless*) означает, что для взаимодействия не требуется выделенный канал, как это происходит во время телефонного звонка, и не существует процедуры вызова перед началом передачи данных между сетевыми узлами. Протокол IP выбирает наиболее эффективный маршрут из числа доступных на основе решения, принятого протоколом маршрутизации. Отсутствие надежности и негарантированная доставка не означает, что система работает плохо и ненадежно, а указывает лишь на то, что протокол IP не предпринимает никаких усилий, чтобы проверить, был ли доставлен пакет по назначению. Эти функции делегированы протоколам верхних уровней.

Информация, проходя сверху вниз по уровням OSI-модели, на каждом из уровней надлежащим образом обрабатывается. На рис. 10.3 показано, что на сетевом уровне данные инкапсулируются внутрь *пакетов*, зачастую называемых *дейтаграммами*.

Протокол IP распознает формат заголовка пакета (включая адресную часть и другую служебную информацию), но никоим образом не заботится о фактических данных. Он принимает любые данные, переданные протоколами верхнего уровня (рис.10.4).

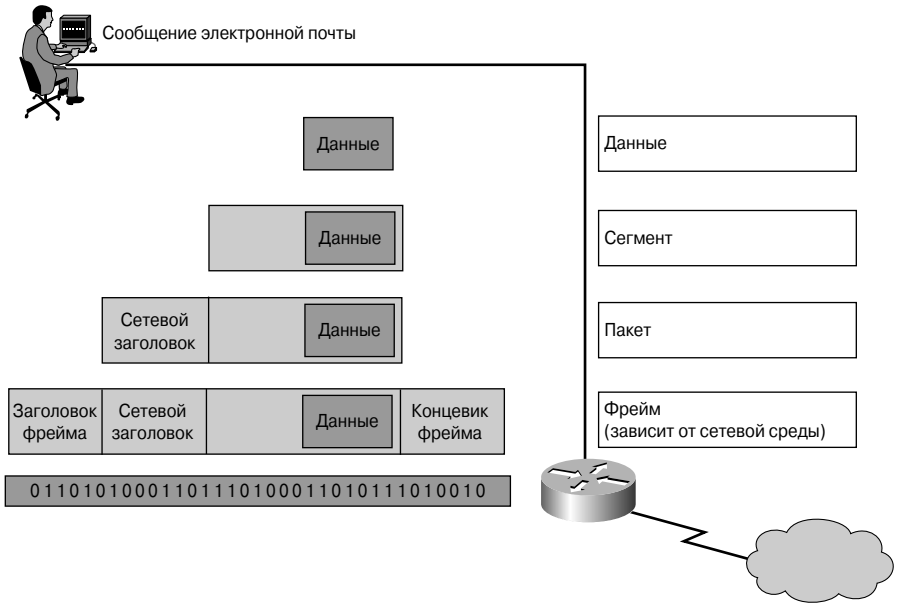


Рис. 10.3. Инкапсуляция

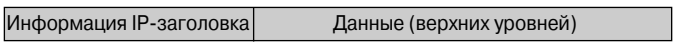


Рис. 10.4. IP-заголовок

Пересылка пакетов и коммутация внутри маршрутизатора

На рис. 10.5 показано, что заголовок и концевик фрейма отбрасываются и заменяются новыми каждый раз при прохождении движущимся по сети пакетом маршрутизирующего устройства третьего уровня. Причина этого состоит в том, что блоки информации второго уровня (фреймы) используются для локальной доставки информации, в то время как блоки третьего уровня (пакеты) предназначены для сквозной передачи данных согласно схеме адресации.

Ethernet-фреймы второго уровня предназначены для работы внутри широковещательных доменов с назначенными каждому сетевому устройству MAC-адресами. Фреймы второго уровня других типов, такие, как последовательные двухточечные соединения и Frame Relay распределенных сетей (сетей WAN), используют свою собственную схему адресации второго уровня. Принципиальным является то, что, независимо от используемой схемы адресации второго уровня, все они разработаны для использования внутри одного широковещательного домена второго уровня. При прохождении данными через устройство третьего уровня информация второго уровня изменяется.

Процессы, выполняемые устройствами третьего уровня, проиллюстрированы на рис. 10.6 и описаны в следующем абзаце.

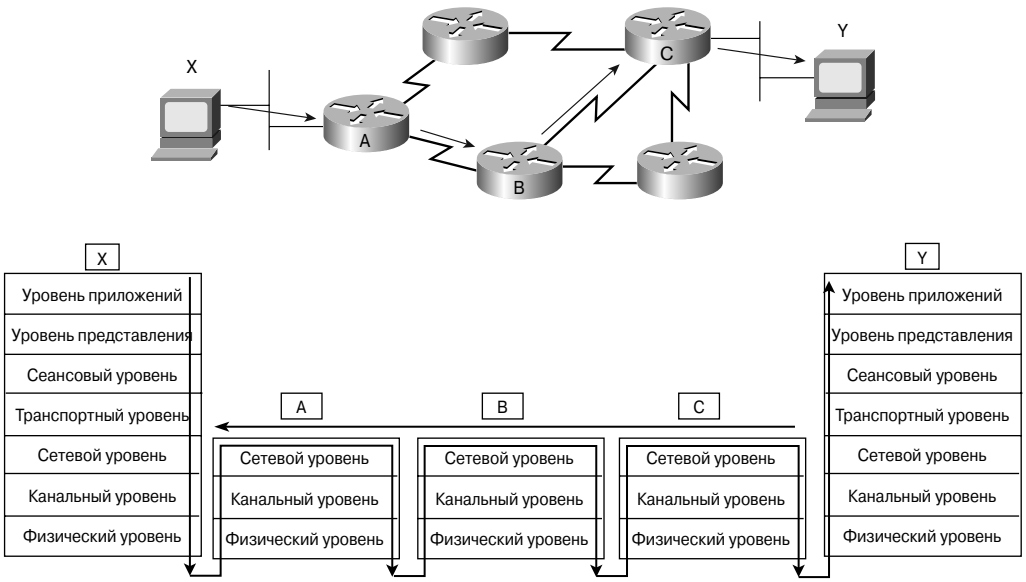


Рис. 10.5. Поток данных сетевого уровня

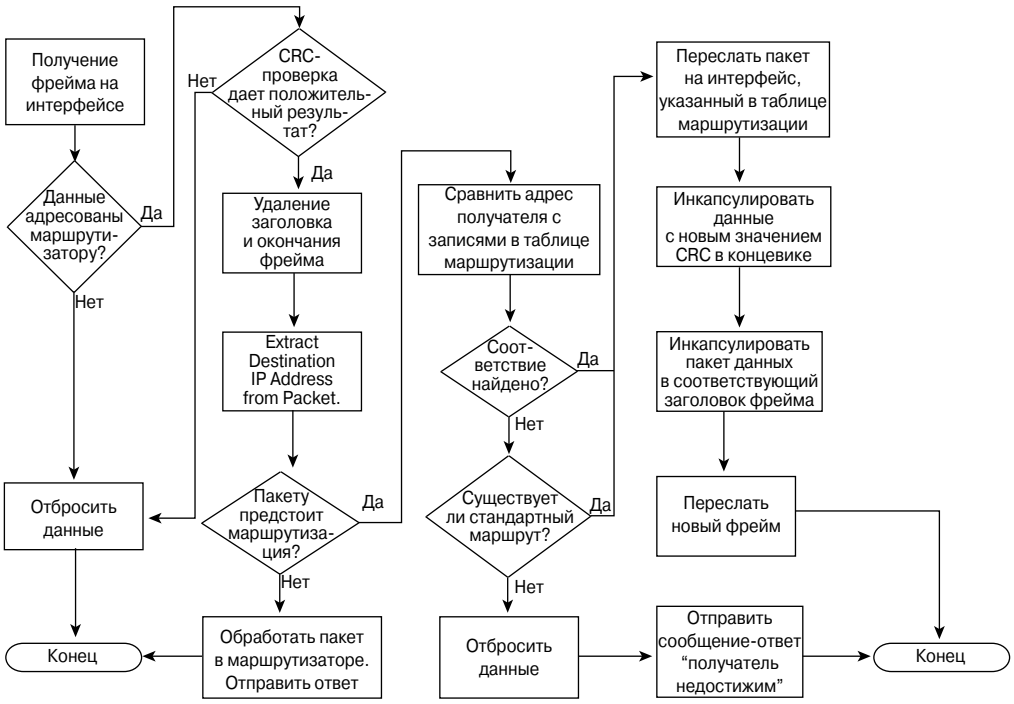


Рис. 10.6. Изменение пакета в процессе инкапсуляции в маршрутизаторе

Из пакета, приходящего на интерфейс маршрутизатора, извлекается MAC-адрес и проверяется, адресован ли этот пакет непосредственно какому-либо узлу либо интерфейсу или он является широковещательным; та же процедура выполняется всеми устройствами внутри *домена коллизий*. В любом из указанных вариантов пакет будет принят и обработан; в противном случае пакет будет отброшен, поскольку был адресован другому устройству в домене коллизий. Таким образом, домен коллизий — это разделяемая среда передачи данных, в которой устройства работают в режиме конкуренции. На основании значения, содержащегося в поле контрольной суммы, с помощью циклического избыточного кода (Cyclical Redundancy Check — CRC), извлеченного из окончания полученного фрейма, проверяется, не были ли данные повреждены. Если проверка дает отрицательный результат, такой фрейм отбрасывается. В случае положительного результата проверки заголовок и окончание фрейма удаляются, и пакет передается на третий уровень. Далее выполняется проверка, адресован ли пакет маршрутизатору или потребуется его дальнейшая маршрутизация на пути к пункту назначения. Пакеты, адресованные маршрутизатору в качестве IP-адреса получателя, содержат адрес одного из интерфейсов маршрутизатора. У таких пакетов удаляется заголовок, и они передаются на четвертый уровень. Если пакету предстоит маршрутизация, он сравнивается с записями в таблице маршрутизации. Если будет найдено точное соответствие или существует стандартный маршрут, пакет будет отправлен на интерфейс, указанный в соответствующей записи таблицы маршрутизации.

Когда пакет коммутируется на выходной интерфейс, новое значение CRC добавляется в конец фрейма и, в зависимости от типа интерфейса (Ethernet, Frame Relay или последовательный), пакету добавляется соответствующий заголовок. После этого фрейм пересылается в другой широковещательный домен, являющийся следующей частью маршрута к конечному пункту назначения.

Сетевые службы с установлением соединения и без

Большинство сетевых служб модели OSI используют системы доставки без установления соединения (протокол UDP), как это показано на рис. 10.7. Они работают с каждым пакетом в отдельности и пересылают их в нужном направлении через сеть. Пакеты могут быть переданы по сетевым маршрутам и будут собраны вместе в сообщение только тогда, когда достигнут своего пункта назначения. В системах без установления соединения перед отправкой пакета контакт с получателем не происходит. Хорошей аналогией систем без установления соединения может быть традиционная почтовая служба. Никто не связывается с получателем, перед тем как отправить ему письмо. Оно отправляется по некоторому маршруту, и получатель узнает о нем только в тот момент, когда получает письмо.

Сетевые службы без установления соединения часто называют процессами с *коммутацией пакетов*. В таких процессах пакеты могут проходить разными маршрутами от отправителя к получателю, а также (что вполне вероятно) прибывать в пункт назначения в другом порядке. Устройства выбирают маршрут для каждого пакета на основе различных критериев. Некоторые критерии (как, например, доступная полоса пропускания) могут быть разными для различных пакетов.

Сеть Internet — огромная объединенная сеть без установления соединения, в которой за доставку всех пакетов отвечает протокол IP. Протокол TCP (четвертый уровень модели) использует службы с установлением соединений поверх протокола IP (третьего уровня). Сегменты TCP инкапсулируются в IP-пакеты для передачи через сеть Internet.

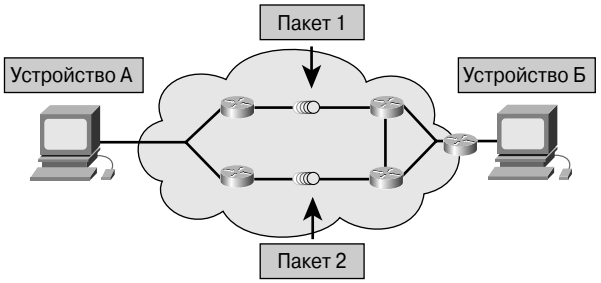


Рис. 10.7. Система доставки без установления соединения для сетевых служб

Протокол IP является системой без установления соединений: каждый пакет в ней обрабатывается отдельно. Например, при использовании FTP-клиента для передачи файлов протокол IP не посылает данные единым неразрывным потоком; он работает с каждым пакетом отдельно. Каждый пакет может пойти своим маршрутом; некоторые из них даже могут быть утеряны. Протокол IP полагается на протоколы транспортного уровня, чтобы определить, был ли доставлен пакет, и при необходимости организовать повторную передачу. Транспортный уровень также отвечает за сборку пакетов в сообщение в надлежащей последовательности.

В системах с *установлением соединения*, как следует из названия, соединение между отправителем и получателем устанавливается до начала передачи данных, как это показано на рис. 10.8. Примером сети с установлением соединения является телефонная система. Взаимодействие начинается только после того, как будет произведен звонок и установлено соединение. В сетях с установлением соединения вначале организуется соединение с получателем и только после этого начинается фактическая передача данных. Все пакеты передаются последовательно, с использованием одного и того же физического канала или, в самом общем случае, одного виртуального канала.

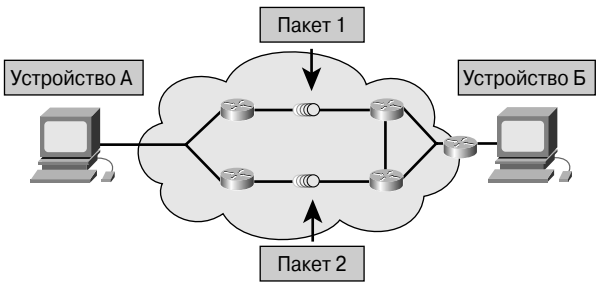


Рис. 10.8. Система доставки с установлением соединения для сетевых служб

Структура IP-пакета

Ранее было рассмотрено, как пакеты или дейтаграммы третьего уровня становятся данными второго уровня и инкапсулируются во фреймы.

Аналогично, как показано на рис. 10.9, IP-пакеты состоят из данных верхнего уровня и IP-заголовка.

- **Версия (Version) —** четырехбитовое поле, описывающее используемую версию протокола IP. Все устройства обязаны использовать протокол IP одной версии; устройство, использующее другую версию, будет отбрасывать пакеты.
- **Длина IP-заголовка (IP Header Length — HLEN) —** четырехбитовое поле, описывающее длину заголовка дейтаграммы в 32-битовых блоках. Данное значение — это полная длина заголовка с учетом двух полей переменной длины.
- **Тип обслуживания (Type of Service — TOS) —** восьмибитовое поле, указывающее на степень важности информации, которая присвоена определенным протоколом верхнего уровня.
- **Полная длина (Total Length) —** шестнадцатибитовое поле, описывающее полную длину пакета в байтах, включая данные и заголовок. Чтобы вычислить длину блока данных, нужно из полной длины вычесть значение поля HLEN.
- **Идентификация (Identification) —** шестнадцатибитовое поле, хранящее целое число, описывающее данную дейтаграмму. Это число представляет собой последовательный номер.
- **Флаги (Flags) —** трехбитовое поле, в котором два младших бита контролируют фрагментацию пакетов. Первый бит определяет, был ли пакет фрагментирован, а второй — является ли этот пакет последним фрагментом в серии фрагментированных пакетов.
- **Смещение фрагментации (Fragment Offset) —** тринадцатибитовое поле, помогающее собрать вместе фрагменты дейтаграммы. Это поле позволяет использовать 16 битов для поля флагов.
- **Время жизни (Time-to-Live — TTL) —** восьмибитовое поле, в котором хранится последовательно уменьшающееся значение счетчика, вплоть до нуля. В последнем случае (счетчик равен нулю) дейтаграмма будет отброшена — таким образом предотвращается бесконечная циклическая пересылка пакета. Аналогом этого поля является счетчик узлов в протоколах маршрутизации.
- **Протокол (Protocol) —** восьмибитовое поле, указывающее, какой протокол верхнего уровня получит пакет, после того как обработка протоколом IP будет закончена. Примерами значений в этом поле являются протоколы TCP и UDP.
- **Контрольная сумма заголовка (Header Checksum) —** шестнадцатибитовое поле, которое помогает проверить целостность заголовка пакета.
- **IP-адрес отправителя (Source IP address) —** 32-битовое поле, содержащее IP-адрес узла-отправителя.

- **IP-адрес получателя (Destination IP address) —** 32-битовое поле, содержащее IP-адрес узла-получателя.
- **Опции (Options) —** поле переменной длинны, позволяющее протоколу IP реализовать поддержку различных опций, например, средств безопасности.
- **Дополнение (Padding) —** поле, используемое для вставки дополнительных нулей, чтобы гарантировать кратность IP-заголовка 32 битам.
- **Данные (Data)** — поле переменной длины (максимум 64 Кбит), содержащее информацию верхних уровней.

Рис. 10.9. Структура IP-пакета

IP-пакет состоит из данных протокола верхнего уровня и заголовка, который имеет описанную выше структуру. Хотя до сих пор основное внимание в этой книге уделялось IP-адресам отправителя и получателя, именно другие части IP-заголовка делают его столь гибким и надежным. Информация, хранящаяся в полях заголовка, задает данные пакета и предназначена для протоколов верхних уровней. Выше, в нескольких предыдущих главах, обсуждалась идея о независимости уровней; информация заголовка — это механизм, реализующий такую независимость.

Протоколы IP-маршрутизации

Основным камнем преткновения для тех, кто только начинает изучать сетевые технологии, является отличие маршрутизируемых протоколов от протоколов маршрутизации. Два термина звучат очень похоже[1], тем не менее, они обозначают принципиально разные понятия. В следующем разделе основное внимание уделено протоколам маршрутизации, которые отвечают за построение таблиц маршрутизации маршрутизаторами и поиск оптимального маршрута к узлу в сети Internet.

[1] *Чаще всего два термина путают в английском написании:* routing *и* routed. *— Прим. ред.*

Обзор технологии маршрутизации

Маршрутизация является функцией третьего уровня модели OSI. Она основана на иерархической схеме, которая позволяет группировать отдельные адреса и работать с группами как с единым целым до тех пор, пока не потребуется установить индивидуальный адрес для окончательной доставки данных. Под термином "маршрутизация" подразумевают процесс определения наиболее эффективного пути от одного устройства к другому (рис. 10.10). Основным устройством, отвечающим за осуществление процесса маршрутизации, является *маршрутизатор.*

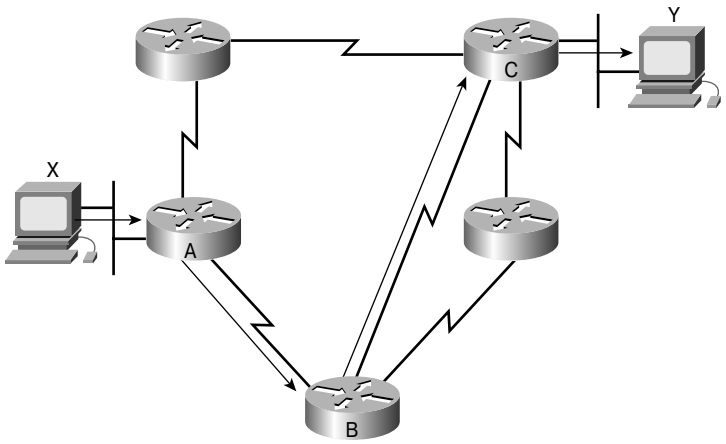


Рис. 10.10. Принцип работы протокола сетевого уровня

Маршрутизатор выполняет две ключевые функции:

- поддерживает таблицы маршрутизации и обменивается информацией об изменениях в топологии сети с другими маршрутизаторами. Эта функция реализуется с помощью одного или нескольких протоколов маршрутизации для передачи сетевой информации другим маршрутизаторам;
- когда пакеты приходят на один из интерфейсов, маршрутизатор, руководствуясь таблицей маршрутизации, должен определить, куда именно следует отправить пакет. Он перенаправляет пакеты на выбранный интерфейс, создает фреймы и затем пересылает их.

Маршрутизатор является устройством сетевого уровня и использует одну или несколько *метрик маршрутизации (routing metric*), для того чтобы установить оптимальный путь, по которому должен следовать сетевой трафик. Метрика маршрутизации — это параметр, по которому определяется наиболее предпочтительный маршрут. На рис. 10.11 показано, что протоколы маршрутизации используют различные комбинации параметров для расчета метрик.

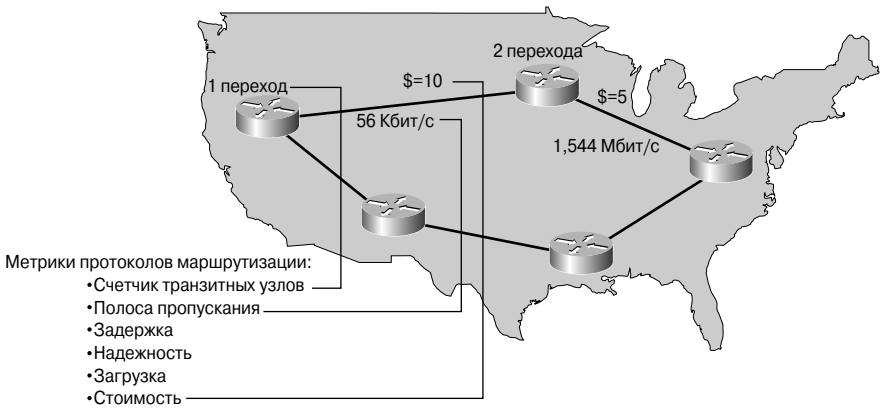


Рис. 10.11. Метрики протокола маршрутизации

Для определения наилучшего межсетевого маршрута вычисляются различные комбинации компонентов метрики: количество ретрансляций (т.е. транзитных узлов), полоса пропускания, задержки, надежность, загрузка и стоимость. Маршрутизаторы объединяют сетевые сегменты или целые сети. Фреймы данных они передают на основе информации протокола третьего уровня. Маршрутизаторы принимают логическое решение о наилучшем маршруте доставки данных между сетями и отправляют пакеты в соответствующий исходящий порт для последующей инкапсуляции и пересылки. Процессы инкапсуляции и декапсуляции происходят каждый раз, когда пакеты проходят через маршрутизатор и данные передаются от одного устройства другому (рис. 10.12). При выполнении инкапсуляции поток данных разбивается на сегменты, добавляются необходимые заголовки и концевики, после чего данные передаются по сети. Декапсуляция — это обратный процесс, при котором удаляются заголовки и концевики, а данные собираются в неразрывный поток. Маршрутизаторы принимают фреймы от устройств локальной сети (например, рабочих станций) и на основе информации третьего уровня пересылают их по сети.

Эта глава и остальная часть книги посвящены наиболее широко используемому маршрутизируемому протоколу — IP. Несмотря на то что далее обсуждается только протокол IP, следует знать, что существуют другие маршрутизируемые протоколы, такие, как IPX/SPX и AppleTalk.

В протоколах IPX/SPX и AppleTalk реализована поддержка средств третьего уровня, благодаря чему они могут маршрутизироваться. Протоколы, не поддерживающие третий уровень, называются немаршрутизируемыми. Наиболее распространенным из их числа является транспортный протокол, используемый всеми сетевыми ОС фирмы Microsoft (NetBIOS Extended User Interface — NetBEUI) — простой и эффективный протокол, область использования которого ограничена одним сегментом сети.

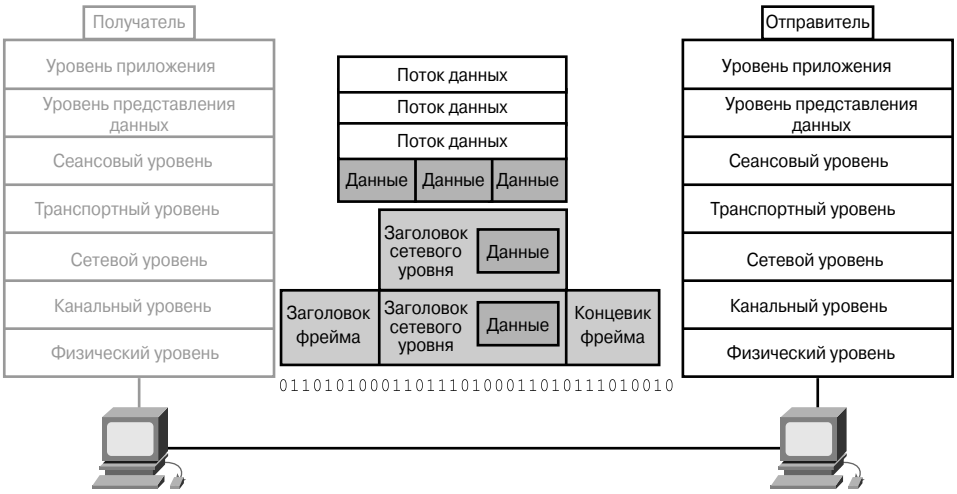


Рис. 10.12. Инкапсуляция данных

Сравнение маршрутизации и коммутации

Маршрутизацию часто путают с коммутацией второго уровня, которая, как может показаться при поверхностном рассмотрении, выполняет те же функции. Принципиальное различие состоит в том, что коммутация реализована на втором уровне модели OSI, а маршрутизация — на третьем. Такое принципиальное отличие означает, что маршрутизация и коммутация используют разную информацию для организации передачи данных от отправителя получателю.

Как коммутация соотносится с маршрутизацией, можно пояснить на примере местных и междугородних телефонных звонков. Для обслуживания местного телефонного звонка (с тем же кодом региона) используется местная телефонная станция. Понятно, что местная АТС хранит только местные номера и ничего не знает о телефонных номерах абонентов из других регионов. При получении звонка, номер которого находится вне компетенции местной станции, она коммутирует такой звонок станции более высокого уровня, которая хранит коды регионов. Станция более высокого уровня коммутирует звонок таким образом, что в конце концов он будет получен местной станцией, обслуживающей номера с кодом региона, по которому был сделан звонок.

Как показано на рис. 10.13, маршрутизатор выполняет функции, подобные тем, которые осуществляет телефонная станция высокого уровня в телефонной сети. Когда говорят о коммутации второго уровня, применяемой в локальных сетях, ее часто связывают с таким понятием, как *широковещательный домен (broadcast domain*). Маршрутизация третьего уровня предназначена для передачи данных между широковещательными доменами и требует иерархической схемы адресации, что и реализовано в протоколах третьего уровня, как, например, в протоколе IP. Коммутатор второго уровня ничего не знает об IP-адресах и может работать только с локальными MAC-адресами узлов. Когда узел отправляет информацию нелокальному получателю,

он адресует фрейм своему стандартному шлюзу-маршрутизатору, используя для этого MAC-адрес маршрутизатора.

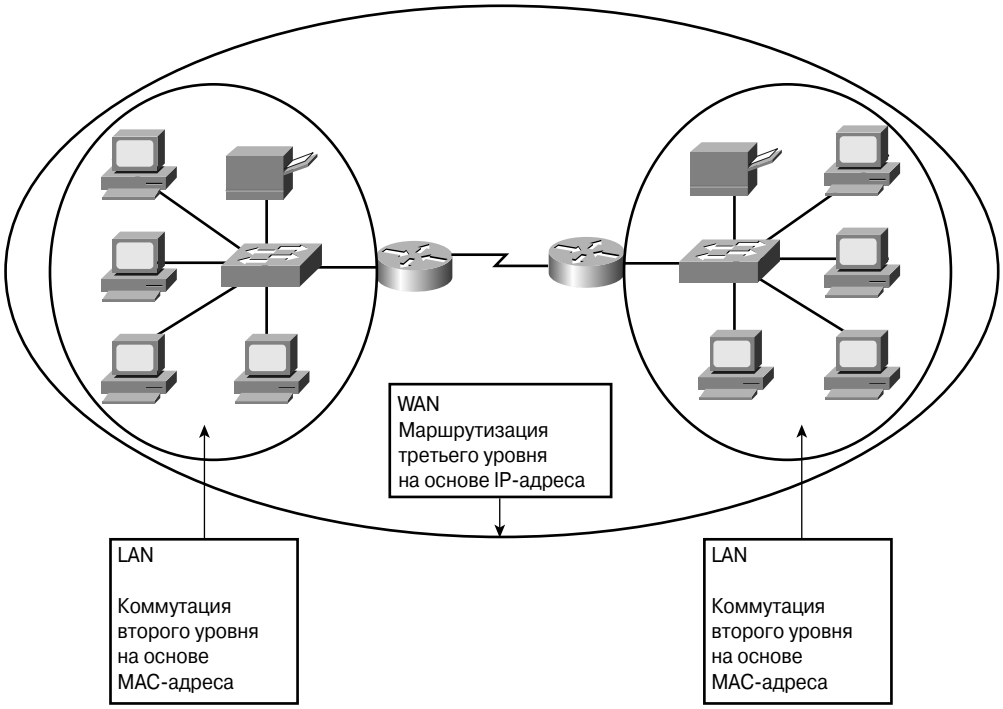


Рис. 10.13. Коммутация второго уровня и маршрутизация третьего

Коммутатор второго уровня объединяет сегменты, принадлежащие одной логической сети или *подсети (subnetwork*). Если узлу X необходимо переслать фрейм получателю из другой сети или подсети, он отправляет фрейм маршрутизатору, который тоже подключен к коммутатору. Узел X знает IP-адрес маршрутизатора, поскольку в его конфигурации протокола IP указан IP-адрес стандартного шлюза, но он ничего не знает о MAC-адресе шлюза. Используя протокол преобразования адресов (Address Resolution Protocol — ARP), который переводит IP-адреса в MAC-адреса, узел X выясняет MAC-адрес маршрутизатора. Коммутатор передает фрейм маршрутизатору на основе его MAC-адреса. Маршрутизатор анализирует адрес получателя третьего уровня в пакете для принятия решения о выборе маршрута. Стандартный шлюз — это маршрутизатор, находящийся в той же сети или подсети, что и узел X. Подобно тому, как коммутатор второго уровня хранит таблицу известных MAC-адресов, маршрутизатор работает с набором IP-адресов сетей, который формирует базу данных доступных ему сетей, называющуюся таблицей маршрутизации (рис. 10.14).

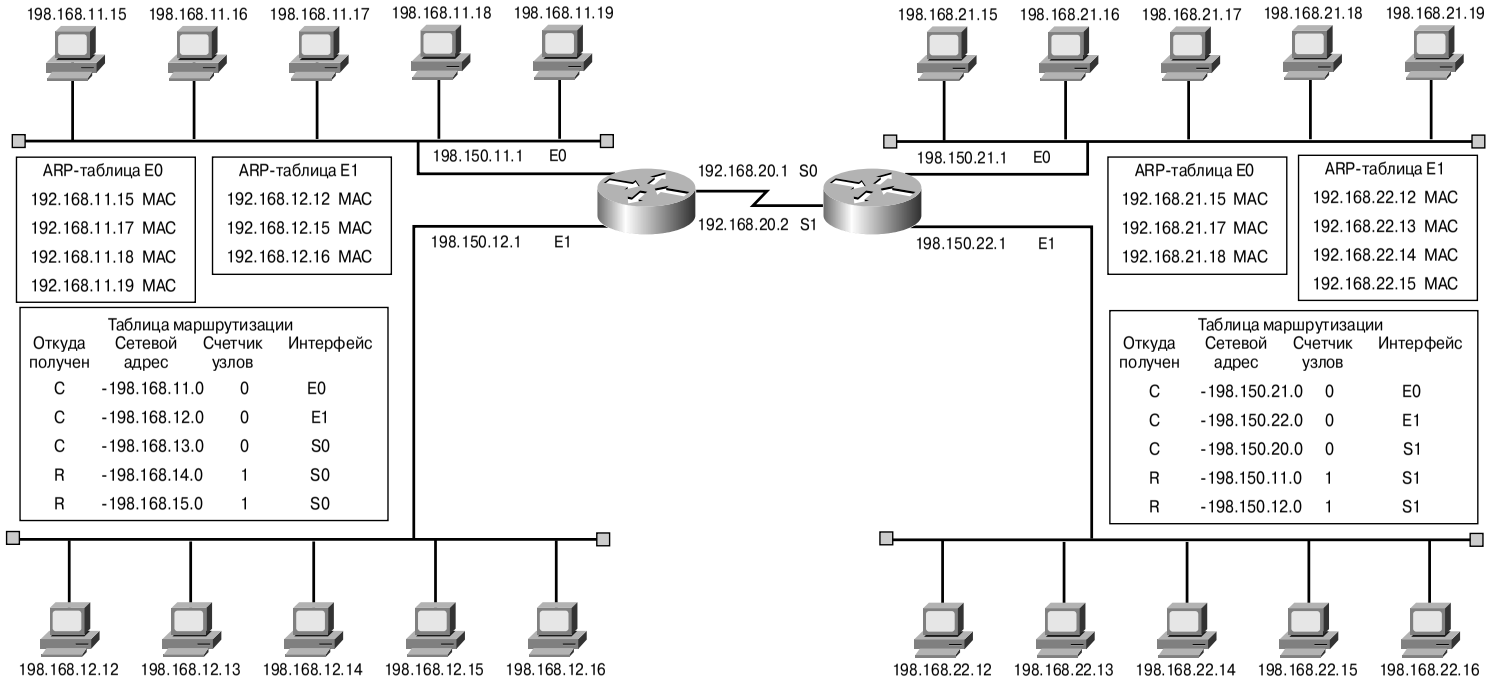


Рис. 10.14. Таблицы маршрутизации и ARP-таблицы маршрутизатора

Каждый компьютер и Ethernet-интерфейс маршрутизатора поддерживают ARP-таблицу для взаимодействий второго уровня; такие таблицы актуальны только для того широковещательного домена, к которому подключено данное устройство. Маршрутизатор, кроме этого, поддерживает еще и таблицу маршрутизации, которая дает возможность выбирать маршрут для доставки данных за пределы широковещательного домена. Каждая ARP-таблица содержит пары IP- и MAC-адресов. (На рис. 10.14 для краткости MAC-адреса представлены аббревиатурой MAC, поскольку фактические их значения имеют слишком длинную запись и не поместились бы на рисунке). *Таблица маршрутизации* содержит информацию о маршрутах; в данном случае — признак: непосредственно подключенная сеть (обозначена символом "C") и сеть, которая получена по протоколу RIP (обозначена символом "R"), IP-адреса доступных сетей, значение счетчика транзитных узлов до этих известных сетей и интерфейсы, через которые информация будет отправлена в нужную сеть. Разница между двумя рассмотренными типами адресов состоит в том, что MAC-адреса не организованы по какому-то определенному принципу. Однако этот недостаток не вызывает проблем с управлением сетями, поскольку отдельные сетевые сегменты не содержат большого количества узлов. Если бы IP-адреса подчинялись тем же правилам, сеть Internet просто не смогла бы функционировать. В том случае, если бы IP-адреса не были организованы (иерархически или как-либо еще), то не существовало бы способа определить маршрут для достижения каждого конкретного адреса. Иерархическая организация IP-адресов позволяет рассматривать группы адресов как единое целое до тех пор, пока не потребуется определить адрес индивидуального узла. Понять такой подход в адресации можно на примере библиотеки, хранящей миллионы отдельных страниц в одной большой кипе бумаг. В таком случае воспользоваться необходимым материалом будет невозможно, поскольку нет способа найти необходимый документ. Намного проще воспользоваться нужной информацией, если страницы пронумерованы, переплетены в книги и каждая внесена в каталог.

Еще одно отличие между коммутируемыми и маршрутизируемыми сетями заключается в том, что коммутируемые сети второго уровня не блокируют широковещательные рассылки третьего уровня. Вследствие этого они могут быть подвержены широковещательным штормам. Маршрутизаторы обычно блокируют широковещательные пакеты, ограничивая таким образом зону действия широковещательных штормов локальным широковещательным доменом. Дополнительно благодаря блокировке широковещательных рассылок маршрутизаторы предоставляют более высокий, чем коммутаторы, уровень защиты и контроль полосы пропускания.

Функции маршрутизации и коммутации сравниваются в табл. 10.1.

Интерактивная презентация: сравнение коммутации и маршрутизации
В этой презентации рассмотрены различия функций маршрутизации и коммутации.

Таблица 10.1. Сравнение функций маршрутизатора и коммутатора

Функция	Маршрутизатор	Коммутатор
Скорость	Медленнее	Быстрее
Уровень OSI	Уровень 3	Уровень 2
Используемая адресация	IP	MAC
Широковещательные рассылки	Блокируются	Пропускаются
Безопасность	Выше	Ниже
Сегментация сетей	Сегментирует сеть на широковещательные домены	Сегментирует сеть на домены коллизий

Сравнение маршрутизируемых протоколов и протоколов маршрутизации

Протоколы сетевого уровня делятся на две категории: маршрутизируемые и протоколы маршрутизации (рис. 10.15). Маршрутизируемые протоколы организуют передачу данных через сеть, а протоколы маршрутизации реализуют механизмы, с помощью которых маршрутизаторы определяют необходимое направление для доставки данных из одного пункта в другой.

Протоколы, способные передавать данные от одного узла другому, находящемуся за маршрутизатором, называются маршрутизируемыми, или просто протоколами передачи данных.

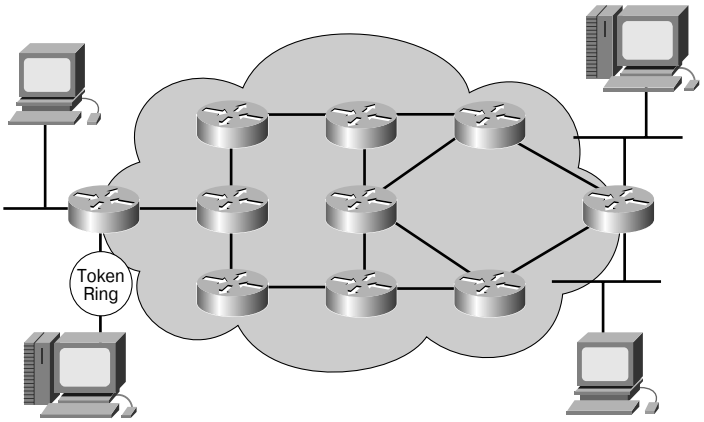
Принцип работы маршрутизируемого протокола проиллюстрирован на рис. 10.16.

- Маршрутизируемым является любой протокол или набор сетевых протоколов, которые предоставляют маршрутизаторам необходимую информацию в адресе сетевого уровня для передачи данных следующему узлу и конечному получателю.
- Маршрутизируемый протокол задает формат пакета и использование в нем отдельных полей. В большинстве своем пакеты передаются от одной конечной системы другой.

Примерами маршрутизируемых протоколов являются IP и IPX. Кроме того, примерами таких протоколов могут служить DECnet, AppleTalk, Banyan VINES и Xerox Networ System (XNS), но следует помнить, что эти протоколы уже устарели и на практике встречаются достаточно редко.

Маршрутизаторы используют протоколы маршрутизации для обмена таблицами маршрутизации и совместного использования информации о доступных маршрутах. Иными словами, *протоколы маршрутизации* дают возможность маршрутизаторам выбирать маршрут для *маршрутизируемых протоколов*, после того как будут обнаружены все возможные пути к получателю.

Маршрутизируемые протоколы используются для передачи трафика пользователя. Примерами таких протоколов являются IP и IPX.



Протоколы маршрутизации используются для обмена информацией и таблицами маршрутизации между маршрутизаторами. Примерами таких протоколов могут служить RIP, IGRP и OSPF.

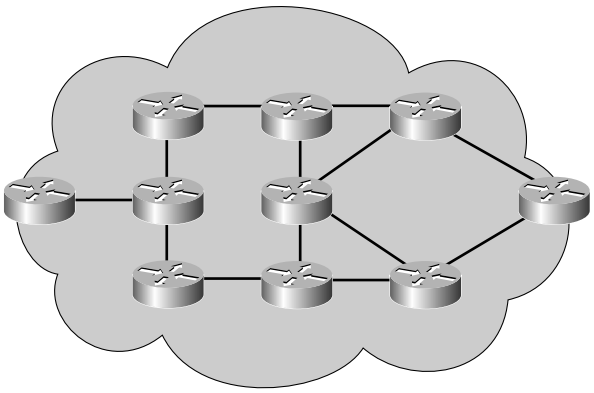


Рис. 10.15. Маршрутизируемый протокол и протокол маршрутизации

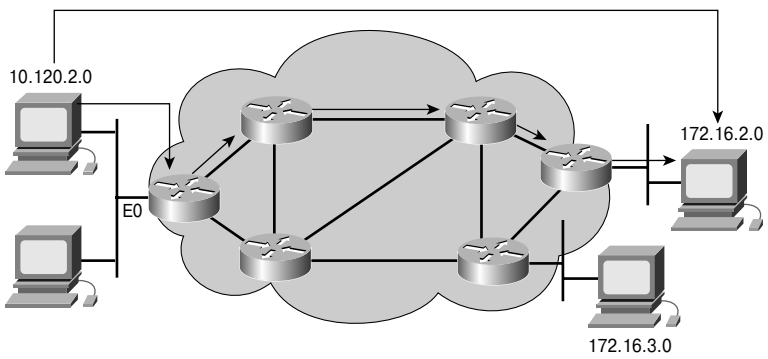
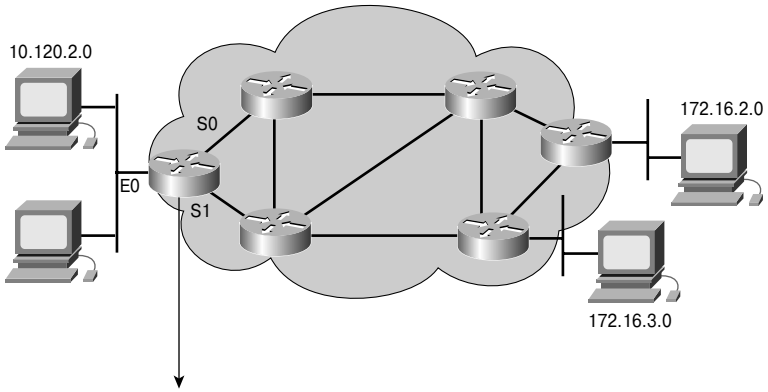


Рис. 10.16. Маршрутизируемый протокол

Принцип работы протокола маршрутизации проиллюстрирован на рис. 10.17.

- Протокол маршрутизации обеспечивает работу процесса совместного использования информации о доступных маршрутах.
- Протокол маршрутизации позволяет маршрутизаторам обмениваться информацией друг с другом для поддержки таблиц маршрутизации.

Примерами протоколов маршрутизации, которые поддерживают маршрутизируемый протокол IP, являются RIP, IGRP, OSPF, протокол граничного шлюза (Border Gateway Protocol — BGP) и EIGRP.



Сетевой протокол	Сеть-получатель	Выходной интерфейс
Подключена напрямую	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

Рис. 10.17. Протокол маршрутизации

Поиск оптимального маршрута

Процесс нахождения оптимального пути, по которому следует передать пакет, выполняется на третьем уровне эталонной модели OSI (сетевом). Эта процедура позволяет маршрутизатору оценить существующие маршруты к получателю и выбрать среди них наиболее предпочтительный. Как показано на рис. 10.18, службы маршрутизации используют информацию о топологии сети в процессе анализа сетевых маршрутов. Определением пути называют процесс, используемый маршрутизатором для выбора следующего узла на пути следования пакета к своему конечному пункту назначения. Этот процесс также называется *маршрутизацией* пакета.

Процесс поиска маршрута для пакета можно сравнить с поездкой из одной части города в другую. У водителя есть карта, где указаны улицы, выбирая которые, он движется к пункту назначения. Отрезок от одного перекрестка до другого аналогичен прохождению пакетом расстояния между двумя маршрутизаторами, который обычно называют *транзитным переходом*. Похожим образом маршрутизатор использует

"карту", на которой показано наличие доступных путей до пункта назначения. Маршрутизаторы могут принимать решения, основываясь на информации об интенсивности трафика и пропускной способности соединения, так же, как водитель может выбрать более быстрый путь (скоростное шоссе) или ехать по менее загруженным обходным улицам. В этом разделе показано, как маршрутизатор выбирает наилучший путь для пакета, следующего из одной сети в другую.

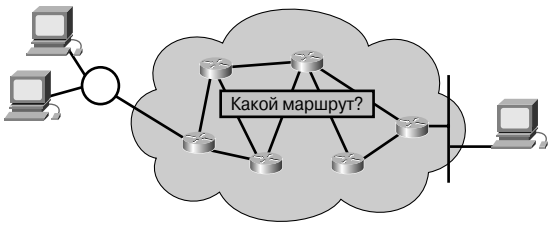


Рис. 10.18. Выбор маршрута

Решение, которое принимает водитель, определяется многими факторами: загруженностью дорог, количеством полос на дороге, стоимостью проезда по магистрали и тем, как часто дорога бывает закрыта. Иногда бывает значительно выгоднее проехать по более длинному маршруту, т.е. по более узкой, но менее загруженной дороге вместо широкой магистрали, по которой ездит огромное количество машин и где часто бывают пробки. Аналогично маршрутизаторы принимают решение о выборе оптимального пути на основании загрузки, полосы пропускания, задержки, стоимости и надежности какого-либо канала. Процесс выбора маршрута для каждого пакета включает в себя следующие компоненты:

- адрес получателя берется непосредственно из заголовка пакета;
- сетевая маска первой записи в таблице маршрутизации применяется к адресу получателя в пакете;
- после того как маска умножается на адрес получателя (логическая операция "И"), полученная величина сравнивается с записью в таблице маршрутизации;
- если оба значения совпали, пакет пересылается на интерфейс (порт) маршрутизатора, с которым связана данная запись в таблице маршрутизации;
- если же совпадений значений нет, описанным выше образом проверяется следующая запись в таблице маршрутизации;
- если адрес пакета не соответствует ни одной из записей в таблице маршрутизации, маршрутизатор проверяет, есть ли у него стандартный маршрут;
- если в маршрутизаторе сконфигурирован стандартный маршрут, пакет передается на соответствующий ему порт маршрутизатора. *Стандартный маршрут* (default route) — это маршрут, который конфигурирует в устройстве системный администратор и который будет использоваться устройством в том случае, если не найдены соответствия ни одной записи в таблице маршрутизации;

- если же стандартного маршрута нет, то пакет будет отброшен маршрутизатором. Зачастую в обратном направлении устройство отправляет сообщение, которое сигнализирует о том, что сеть получателя недоступна.

Дополнительная информация: функции сетевого уровня

Адресация сетевого уровня

Сетевой адрес помогает маршрутизатору находить путь в межсетевой среде, а также предоставляет иерархическую информацию или сведения о подсетях. Маршрутизатор использует сетевой адрес для поиска сети-получателя, в которую следует пакет. В дополнение к сетевому адресу сетевой протокол также использует некую форму адреса узла. Для некоторых протоколов сетевого уровня сетевой администратор назначает адреса узлов на основе заранее заданных правил сетевой адресации. Для других протоколов сетевого уровня назначение сетевых адресов происходит частично или полностью динамически, либо автоматически. На рис. 10.19 показаны три устройства в сети 1 (две станции и один маршрутизатор), каждое из которых имеет свой уникальный адрес. (На рисунке также показано, что маршрутизатор подключен к двум другим сетям с номерами 2 и 3.)

Сеть	Узел
1	1 2 3
2	1
3	1

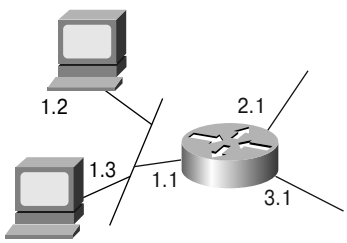


Рис. 10.19. Адреса сетей

Логическая адресация происходит на сетевом уровне. Вспомним аналогию между сетевыми адресами и телефонными номерами. Первая часть телефонного адреса представляет собой код региона, несколько первых цифр номера (в крупных городах — обычно три цифры) указывают на телефонную станцию. Последние цифры номера указывают оборудованию телефонной компании, на какой конкретный телефонный аппарат необходимо направить звонок. Последняя часть телефонного номера похожа на часть адреса, которая описывает узел. Часть целого адреса, содержащая адрес узла, дает маршрутизатору информацию о конкретном устройстве, которому необходимо доставить пакет.

Маршрутизация не может быть реализована без адресации сетевого уровня. Маршрутизаторам необходимо знать сетевые адреса, чтобы обеспечить надлежащую доставку пакетов.
Без иерархической структуры адресации пакеты было бы невозможно передавать между сетями.

Аналогично без определенной иерархии в схеме телефонных номеров, почтовых адресов и транспортных систем не существовало бы надежной доставки товаров и услуг.

MAC-адрес можно сравнить с именем получателя, а адрес сетевого уровня — с почтовым адресом (сетевой адрес и адрес узла). Так, например, если адресат переехал в другой город, имя его останется без изменений, но почтовый адрес должен отражать его новое местоположение. Сетевые устройства (отдельные компьютеры и маршрутизаторы) имеют как MAC-адрес, так и адрес сетевого уровня. Перемещение компьютера в другую сеть не изменит его MAC-адрес, но обязательно потребует назначения нового адреса сетевого уровня.

Коммуникационный путь

Задача сетевого уровня состоит в поиске наилучшего маршрута через сеть. Говоря практическим языком, устройства сети постоянно распространяют определенный набор доступных маршрутов между маршрутизаторами. На рис. 10.20 каждая линия, соединяющая маршрутизаторы, имеет номер, используемый маршрутизатором в качестве сетевого адреса. Эти адреса должны отражать информацию, использующуюся в процессе маршрутизации. Это означает, что адрес должен нести информацию о маршруте для данного физического соединения, которая необходима для передачи пакетов от отправителя получателю в процессе маршрутизации.

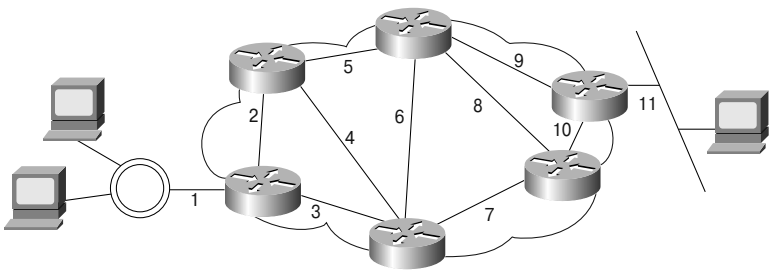


Рис. 10.20. Сетевые соединения

Благодаря использованию иерархических адресов на сетевом уровне создаются соединения, которые позволяют обеспечить взаимодействие между независимыми сетями. Логичность и связность адресов третьего уровня во всей сети улучшают эффективность использования пропускной способности, поскольку устраняют необходимость в ненужных широковещательных запросах. *Широковещательные рассылки* приводят к нежелательной загрузке и бесполезному расходу ресурсов устройств и каналов связи, которые не нуждаются в получении широковещательных пакетов. Использование сквозной схемы адресации для описания путей физических соединений дает возможность сетевому уровню находить путь к получателю, не прибегая к нежелательным перегрузкам устройств и каналов связи из-за использования широковещательных рассылок.

Таблицы маршрутизации

Чтобы найти маршрут, по которому следует передавать данные, протоколы маршрутизации создают и поддерживают таблицы маршрутизации (рис. 10.21). Информация о маршруте может отличаться в зависимости от используемого протокола маршрутизации. Таблица маршрутизации заполняется соответствующим протоколом различной информацией.

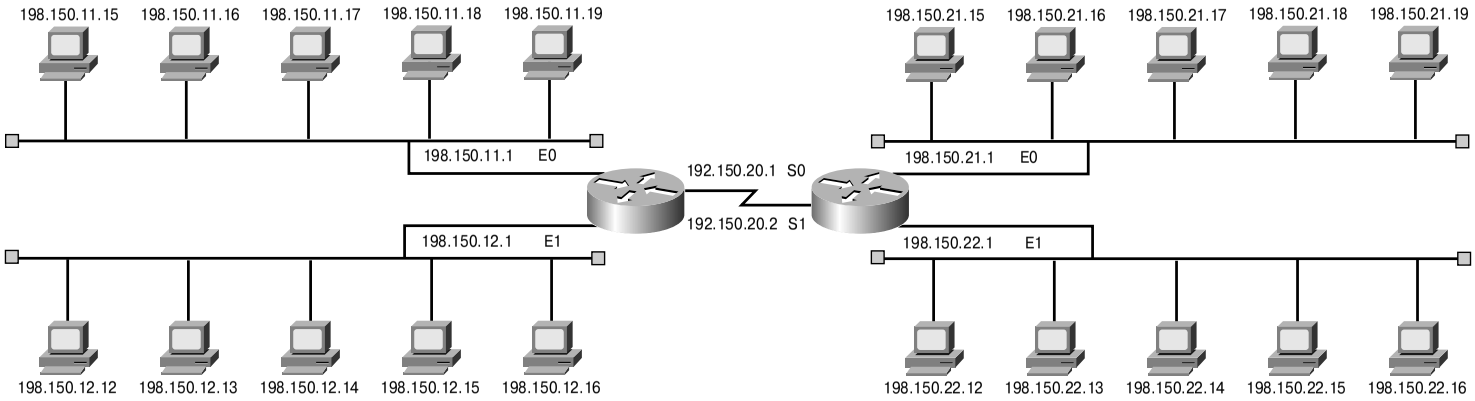


Таблица маршрутизации

Откуда получен	Сетевой адрес	Счетчик узлов	Интерфейс
C	-198.150.11.0	0	E0
C	-198.150.12.0	0	E1
C	-198.150.13.0	0	S0
R	-198.150.14.0	1	S0
R	-198.150.15.0	1	S0

Таблица маршрутизации

Откуда получен	Сетевой адрес	Счетчик узлов	Интерфейс
C	-198.150.21.0	0	E0
C	-198.150.22.0	0	E1
C	-198.150.23.0	0	S1
R	-198.150.24.0	1	S1
R	-198.150.25.0	1	S1

Рис. 10.21. Таблицы маршрутизации

Маршрутизаторы хранят и обновляют следующую важную информацию в таблицах маршрутизации:

- **тип протокола —** информацию о протоколе маршрутизации, создавшем запись в таблице маршрутизации;
- **связка получатель/следующий узел** сообщает маршрутизатору о том, что определенный получатель либо подключен непосредственно, либо может быть достигнут через другой маршрутизатор, называемый *следующим транзитным узлом (next hop)*, находящийся на пути к пункту назначения. Маршрутизатор анализирует адрес получателя во входящих пакетах и сравнивает его на соответствие с записями в таблице маршрутизации;
- **метрики маршрутизации**. Различные протоколы маршрутизации используют разные метрики, которые помогают определить предпочтительность маршрута. Например, протокол RIP использует *счетчик транзитных узлов (hop count)* в качестве метрики маршрутизации. Протокол IGRP использует пропускную способность, загрузку канала, суммарную задержку передачи и надежность для формирования комплексного значения метрики. Более подробно метрики и протоколы маршрутизации обсуждаются во второй части книги "Курс CCNA2: маршрутизаторы и основы маршрутизации";
- **выходной интерфейс —** интерфейс, через который должны быть отправлены данные, чтобы достичь пункта назначения.

Маршрутизаторы взаимодействуют друг с другом посредством передачи сообщений-анонсов для поддержки таблиц маршрутизации. В зависимости от протокола маршрутизации такие обновления маршрутных таблиц могут отправляться либо периодически, либо при изменении топологии сети. Протокол также определяет, нужно ли в анонсе отправить полную таблицу маршрутизации или только информацию об изменившемся маршруте. Используя анонсы, получаемые от соседей, маршрутизатор создает и поддерживает свою таблицу маршрутизации в актуальном состоянии.

Алгоритмы маршрутизации и метрики

Протоколы маршрутизации выбираются, исходя из характеристик, перечисленных ниже.

- **Оптимальность** описывает способности протокола и алгоритма по выбору наиболее оптимального маршрута на основании метрик и их весовых значений, используемых при расчетах. Например, некий протокол может использовать счетчик узлов и задержки для определения метрик; задержки имеют более высокий вес при учете окончательного значения, но зато их сложнее рассчитать.
- **Простота и низкие накладные расходы.** Идеальная эффективность работы алгоритма маршрутизации может быть достигнута, когда загрузка процессора и памяти маршрутизатора минимальны. Эта характеристика важна для масштабируемости сети, которая в предельном случае может быть расширена до размеров сети Internet.

- **Устойчивость и надежность.** Алгоритм маршрутизации должен корректно функционировать даже при наличии нестандартных и непредвиденных обстоятельств, таких, как сбой оборудования, высокая загрузка и ошибки эксплуатации.
- **Быстрая конвергенция.** Конвергенцией называется процесс установления договоренности между всеми маршрутизаторами об имеющихся маршрутах. Когда в сети происходят события, оказывающие влияние на доступность маршрутизатора, для установления повторного соединения требуются перерасчеты. Алгоритмы маршрутизации, не обладающие быстрой конвергенцией, могут вызвать сбой или значительную задержку при доставке информации.
- **Гибкость.** Алгоритм и протокол маршрутизации должны быстро адаптироваться к разнообразным изменениям в сети. Изменениями в сети считаются изменения в состоянии устройств, в частности, маршрутизаторов, изменение пропускной способности каналов, изменение размера очередей или сетевой задержки.
- **Масштабируемость.** Некоторые протоколы разработаны таким образом, что могут быть масштабируемы лучше других. Важно помнить, что если планируется расширение сети (или такая возможность в принципе предусматривается), следует отдать предпочтение протоколу EIGRP, нежели RIP.

Первоочередная задача *алгоритма маршрутизации* при обновлении таблицы маршрутизации состоит в определении наилучшей информации, которая должна быть внесена в таблицу. Алгоритмы маршрутизации используют различные метрики для определения наилучшего маршрута, но каждый алгоритм интерпретирует выбор лучшего варианта пути по-своему. Алгоритм маршрутизации рассчитывает число, называемое метрикой, для каждого сетевого маршрута. Сложные алгоритмы маршрутизации могут основывать выбор маршрута на основе нескольких параметров, объединяя их в одну общую метрику, как показано на рис. 10.22. Чем меньше метрика, тем лучше выбранный маршрут.

Метрики могут быть вычислены на основе одной или нескольких характеристик. Наиболее часто в алгоритмах маршрутизации используются параметры метрики, которые перечислены ниже.

- **Ширина полосы пропускания** представляет собой средство оценки объема информации, который может быть передан по каналу связи (канал Ethernet со скоростью 10 Мбит/с более предпочтителен, чем выделенная линия со скоростью 64 Кбит/с).
- **Задержка** — промежуток времени, необходимый для перемещения пакета по каждому из каналов связи от отправителя получателю. Задержка зависит от пропускной способности промежуточных каналов, размера очередей в портах маршрутизаторов, загрузки сети и физического расстояния.
- **Загрузка** — объем операций, выполняемых сетевым устройством, таким, как маршрутизатор, или средняя загруженность канала связи.

- **Надежность** обычно обозначает относительное значение количества ошибок для каждого из каналов связи.
- **Счетчик транзитных узлов —** количество маршрутизаторов, через которые должен пройти пакет, прежде чем достигнет пункта назначения. Когда пакет проходит через маршрутизатор, значение счетчика узлов увеличивается на единицу. Путь, для которого значение счетчика узлов равно четырем, означает, что данные, отправленные по этому маршруту, пройдут через четыре маршрутизатора, прежде чем будут получены адресатом. Если существует несколько путей, маршрутизатор выбирает тот, для которого значение счетчика узлов наименьшее.
- **Стоимость** — значение, обычно вычисляемое на основе пропускной способности, денежной стоимости или других единиц измерения, назначаемых администратором.

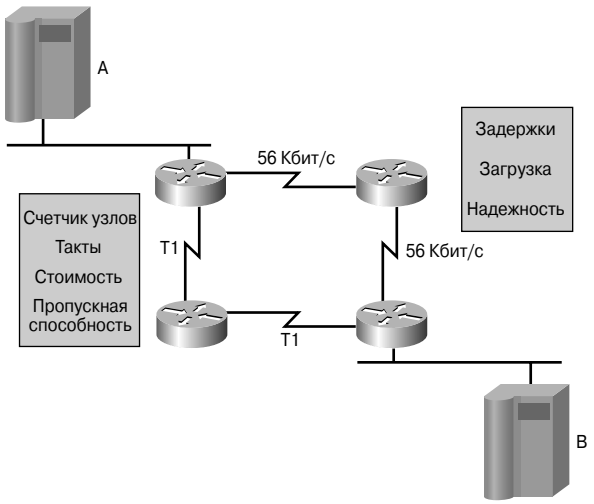


Рис. 10.22. Метрики маршрутизации

Внутренние и внешние протоколы маршрутизации

Маршрутизаторы используют протоколы маршрутизации для обмена маршрутной информацией. Иными словами, протоколы маршрутизации определяют, как маршрутизируются протоколы передачи данных (т.е. маршрутизируемые). Как показано на рис. 10.23, двумя семействами протоколов маршрутизации являются *протоколы внутренних шлюзов (Interior Gateway Protocol — IGP*) и *протоколы внешних шлюзов (Exterior Gateway Protocols — EGP*). Классификация всех протоколов по этим двум семействам основана на принципе их работы по отношению к автономным системам.

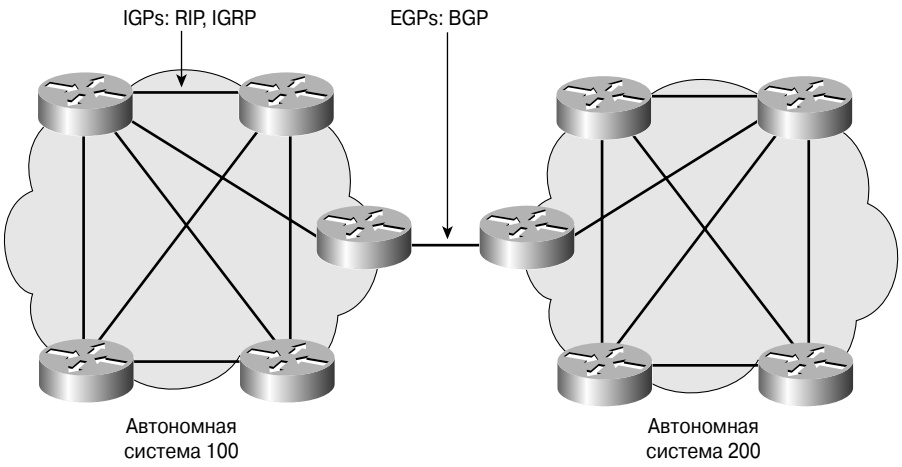


Рис. 10.23. Протоколы EGP и IGP

Автономной системой (Autonomous System — AS) называется сеть или группа сетей, находящихся под единым административным контролем, как, например, домен `Cisco.com`. Автономная система состоит из маршрутизаторов, которые для внешнего мира (т.е. для других сетей) выглядят как единая сеть. Агентство по выделению имен и уникальных параметров протоколов Internet (Internt Assigned Numbers Authority — IANA) выделяет номера автономных систем региональным регистраторам. Таким регистратором для Америки, стран Карибского бассейна и Африки является организация ARIN (American Registry for Internet Numbers — Американский регистратор номеров сети Internet, адрес — `hostmaster@arin.net`), для Европы — RIPE-NCC[2] (Reseaux IP Europeens Network Coordination Centre — сетевой координационный центр RIPE, адрес — `ncc@ripe.net`), для стран Азиатско-тихоокеанского региона — AP-NIC (Asia Pacific Network Information Centre — сетевой информационный центр азиатско-тихоокеанского региона, адрес — `admin@apnic.net`). Такие автономные системы описываются шестнадцатибитовым номером. При настройке таких протоколов маршрутизации, как BGP, требуется указать назначенный уникальный номер автономной системы.

Протоколы класса IGP маршрутизируют данные внутри автономных систем. К классу IGP относятся следующие протоколы маршрутизации:

- протоколы RIP и RIP V2;
- IGRP;
- EIGRP;
- OSPF;

[2] *Домены .ru официально регулируются Российским НИИ Развития Общественных Сетей (Russian Institute for Public Networks — RIPN),* `http://www.ripn.net.` *— Прим. ред.*

- протокол обмена данными между промежуточными системами (Intermediate system-to-Intermediate System — IS-IS).

Протоколы класса EGP маршрутизируют данные между автономными системами. Протокол BGP является наиболее широко известным представителем класса EGP.

Дистанционно-векторные и протоколы маршрутизации с учетом состояния каналов

Протоколы маршрутизации могут подразделяться по самым разным критериям, например, по сфере применения, т.е. по принадлежности к EGP- или IGP-типу. Другой классификацией, описывающей протоколы маршрутизации, может быть деление по используемым алгоритмам: протокол использует дистанционно-векторный (distanse-vector) алгоритм или работает с учетом состояния канала (link-state). Если принадлежность маршрутизаторов к EGP- или IGP-типу описывает их физическое взаимодействие, то использование алгоритмов маршрутизации по вектору расстояния или состоянию канала описывает характер взаимодействия маршрутизаторов между собой при рассылке маршрутных обновлений.

Дистанционно-векторные протоколы

Алгоритм дистанционно-векторной маршрутизации определяет направление (вектор) и расстояние (счетчик узлов) для каждого из каналов связи, образующих сеть. При использовании этого алгоритма маршрутизатор периодически (например, каждые 30 секунд) пересылает всю или часть своей таблицы маршрутизации своим соседям. Периодические обновления рассылаются маршрутизатором, использующим дистанционно-векторный алгоритм, даже если не произошли никакие изменения в сети. Получив таблицу маршрутизации от своего соседа, маршрутизатор может проверить уже известные маршруты и внести необходимые изменения на основе полученного обновления. Такой процесс иногда называют “маршрутизацией по слухам”, поскольку представление маршрутизатора о структуре сети базируется на данных его соседей. Дистанционно-векторные протоколы маршрутизации основаны на алгоритме Беллмана-Форда (Bellman-Ford) и используют его для поиска наилучшего маршрута.

Дистанционно-векторный алгоритм служит основой для следующих протоколов (рис. 10.25):

- для *протокола маршрутной информации* (Routing Information Protocol — RIP) — одного из наиболее широко распространенных протоколов IGP-типа, использующего в качестве метрики счетчик узлов;
- для *протокола маршрутизации внутреннего шлюза* (Interior Gateway Routing Protocol — IGRP); корпорация Cisco разработала этот протокол для маршрутизации в больших гетерогенных сетях;

- для *усовершенствованного протокола маршрутизации внутреннего шлюза* (Enhanced Interior Gateway Routing Protocol — EIGRP), представляющего собой улучшенную версию IGRP от корпорации Cisco; этот протокол имеет исключительно быструю конвергенцию, работает значительно более эффективно, чем его предшественник, и сочетает в себе все преимущества дистанционно-векторных алгоритмов и протоколов с учетом состояния каналов.

Протоколы маршрутизации по состоянию каналов

Протоколы маршрутизации, использующие *алгоритм с учетом состояния каналов*, были разработаны для преодоления ограничений, связанных с использованием дистанционно-векторных протоколов. Алгоритм с учетом состояния канала дает возможность протоколам быстро реагировать на изменения сети, рассылать обновления только в случае появления изменений и рассылать периодические обновления (называемые обновлениями состояния канала) через большие промежутки времени, примерно один раз каждые 30 минут.

Когда состояние канала изменяется, устройство, обнаружившее такое изменение, формирует извещение о состоянии канала (Link-State Andvertisement — LSA), относящееся к этому каналу (маршруту), и рассылает его всем соседствующим маршрутизаторам. Каждый маршрутизатор получает копию извещения о состоянии канала и на этом основании обновляет свою базу состояния каналов (топологическую базу), после чего пересылает копию извещения всем своим соседям. Такая массовая рассылка извещения нужна, чтобы гарантировать, что все маршрутизаторы обновят свои базы данных и создадут обновленную таблицу маршрутизации, которая отражает новую топологию (рис. 10.24).

База данных состояния канала используется для обнаружения наилучшего сетевого пути. Маршрутизация с учетом состояния канала основана на алгоритме первоочередного определения кратчайшего маршрута (Shortest Path First — SPF) Дейкстра (Dijkstra) для построения SPF-дерева, на основе которого принимается решение о том, какой маршрут является наилучшим. Наилучший (кратчайший) маршрут выбирается из дерева первоочередного определения кратчайшего маршрута и помещается в таблицу маршрутизации.

Примерами протоколов, использующих алгоритм с учетом состояния каналов, являются OSPF и IS-IS (рис. 10.25).

Интерактивная презентация: дистанционно-векторные протоколы и протоколы маршрутизации по состоянию каналов

Эта презентация позволит закрепить знания о протоколах маршрутизации, в частности, еще раз повторить отличия между двумя классами протоколов.

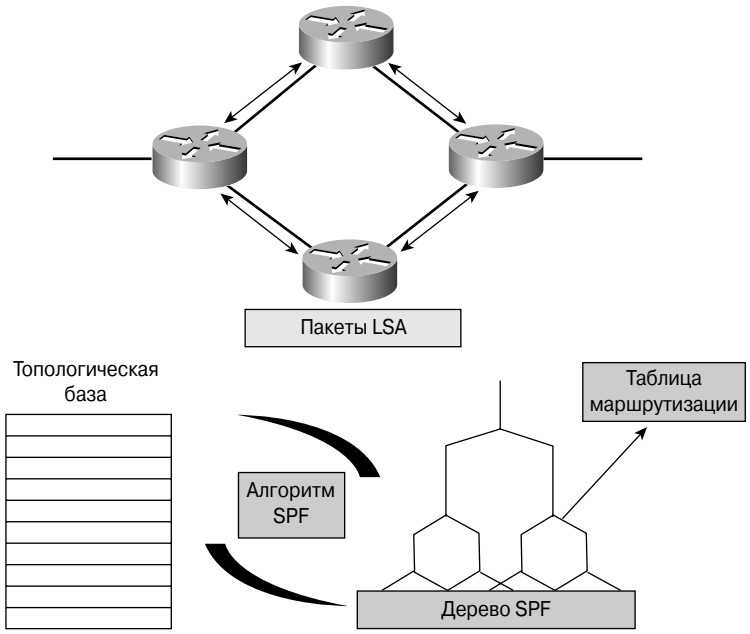


Рис. 10.24. Протоколы маршрутизации на основе состояния канала

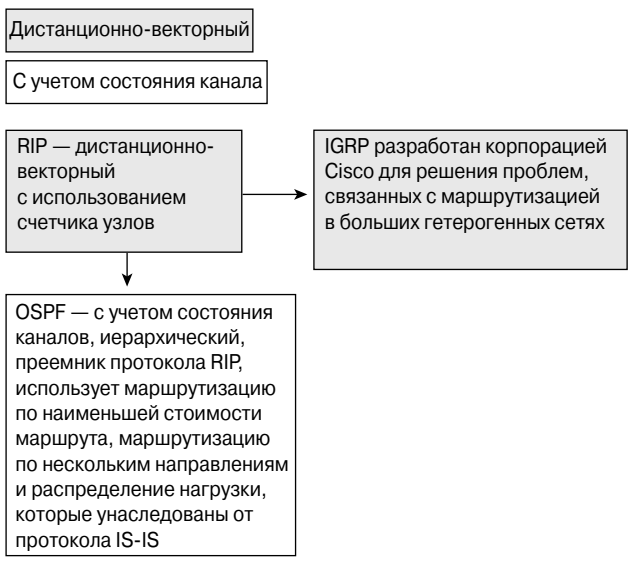


Рис. 10.25. Основные характеристики наиболее распространенных протоколов маршрутизации

Протоколы маршрутизации

В этом разделе описаны метрики, загрузка сети и другие важные характеристики наиболее широко используемых протоколов маршрутизации.

Протокол RIP

Протокол маршрутной информации (Routing Information Protocol — RIP) использует счетчик количества транзитных узлов для определения направления и расстояния для любого из каналов сети (рис. 10.26). Если существуют несколько маршрутов к получателю, протокол RIP выберет тот из них, который имеет наименьшее значение счетчика транзитных узлов. Поскольку счетчик является единственной метрикой, используемой протоколом RIP, выбранный маршрут далеко не всегда оказывается кратчайшим. Протокол RIP версии 1 позволяет использовать только классовую (classfull) маршрутизацию. Это означает, что все сетевые устройства должны иметь одинаковую маску сети, поскольку RIP версии 1 не включает в маршрутные обновления информацию о ней.

Протокол RIP версии 2 использует так называемую *префиксную маршрутизацию (prefix routing*) и пересылает маску сети вместе с анонсами таблиц маршрутизации: именно за счет этой функции обеспечивается поддержка бесклассовой маршрутизации. Благодаря протоколам бесклассовой маршрутизации можно использовать подсети с разной длины масками внутри одной и той же сети. Использование масок подсети разной длины внутри одной сети называется технологией масок переменной длины (Variable-Length Subnet Mask —VLSM).

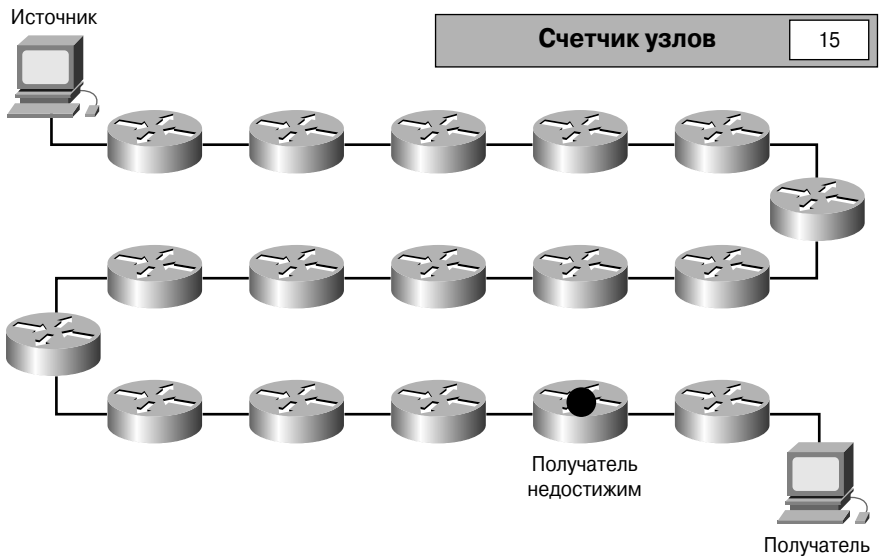


Рис. 10.26. Протокол RIP использует в качестве метрики счетчик транзитных узлов

Протокол IGRP

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP), разработанный корпорацией Cisco, использует дистанционно-векторный алгоритм и предназначен для решения проблем, возникающих при маршрутизации в больших сетях, где невозможно использовать такие протоколы, как RIP. Протокол IGRP способен выбирать самый быстрый путь на основе задержки, пропускной способности, загрузки и надежности канала. Стандартно протокол IGRP использует в качестве 24-битовых метрик только пропускную способность и задержку. Этот протокол имеет значительно большее максимальное значение счетчика узлов, чем протокол RIP, что дает возможность использовать его в более крупных сетях. Протокол IGRP позволяет использовать только классовую маршрутизацию.

Протокол EIGRP

Так же, как и IGRP, протокол EIGRP (Enhanced Interior Gateway Routing Protocol — расширенный протокол маршрутизации внутреннего шлюза) был разработан корпорацией Cisco и является ее фирменным продуктом. Этот протокол — усовершенствованная версия протокола IGRP, использует 32-битовые метрики. В частности, протокол EIGRP очень эффективен благодаря более быстрой конвергенции и низкому потреблению пропускной способности. Он является усовершенствованным вариантом протокола, работающего на основе дистанционно-векторного алгоритма. Протокол EIGRP также использует некоторые функции алгоритмов с учетом состояния канала. Вот почему использование термина *гибридный* тоже вполне законно при описании протокола IGRP.

Протокол OSPF

Открытый протокол поиска кратчайшего пути (Open Shortest Path First — OSPF) использует алгоритм маршрутизации по состоянию каналов. Проблемная группа проектирования Internet (IETF) разработала OSPF в 1988 году. Самая последняя версия этого протокола, OSPF версии 2, описана в спецификации RFC 2328. OSPF является протоколом IGP-типа, что означает, что он распространяет маршрутную информацию между маршрутизаторами, находящимися в единой автономной системе. Протокол OSPF был разработан для использования в больших сетях, в которых невозможно использование протокола RIP.

Протокол IS-IS

Протокол обмена маршрутной информацией между промежуточными системами (Intermediate System-to-Intermediate System — IS-IS) использует алгоритм маршрутизации по состоянию канала для *стека протоколов* модели OSI. Он распространяет маршрутную информацию для протокола сетевого обслуживания (Connectionless Network Protocol — CLNP), для соответствующих ISO-служб сетевого обслуживания без установления соединения (Connectionless Network Service — CLNS). Интегрированный протокол IS-IS является вариантом реализации протокола IS-IS для маршрутизации нескольких сетевых протоколов. Интегрированный протокол IS-IS объединяет CLNP-маршруты с информацией об IP-сетях и масках подсетей. Благодаря

соединению ISO CLNS и IP-маршрутизации в одном протоколе интегрированный протокол IS-IS предоставляет альтернативу протоколу OSPF при использовании в IP-сетях. Он может быть использован для IP-маршрутизации, ISO-маршрутизации и для комбинации этих двух вариантов.

ВНИМАНИЕ!

Протокол CLNP относится к сетевому уровню эталонной модели OSI и не требует установления виртуального канала перед тем, как будет начата передача данных.

Протокол BGP

Протокол граничного шлюза (Border Gateway Protocol — BGP) является примером протокола EGP-типа. Протокол BGP обеспечивает обмен маршрутной информацией между автономными системами и гарантирует выбор маршрутов без зацикливания. Он является базовым протоколом извещений маршрутизации, использующимся большинством крупных компаний и поставщиками услуг доступа к Internet (ISP). Протокол BGP-4 стал первой версией протокола BGP, в котором встроена *бесклассовая междоменная маршрутизация* (*Classless InterDomain Routing — CIDR*), и первым, использующим механизм агрегации маршрутов. В отличие от распространенных протоколов IGP-типа, таких, как RIP, OSPF и EIGRP, BGP не использует в качестве метрики счетчик узлов, пропускную способность или задержку в сети. Вместо этого протокол BGP принимает решение о выборе маршрута, руководствуясь указанными сетевыми правилами, используя различные маршрутные BGP-атрибуты.

Практическое задание 10.2.9. Покупка небольшого маршрутизатора
Цель этого задания — ознакомиться с существующим разнообразием и ценами на современные сетевые компоненты. В задании делается акцент на использование небольших маршрутизаторов, применяющихся в домашних офисах и для подключения к центральному офису телеработников.

Механизм создания подсетей

В изначальной двухуровневой[3] иерархии сети Internet предполагалось, что каждая подключенная к сети организация будет иметь только одну сеть. Следовательно, каждой организации требовалось бы только одно подключение к сети Internet. Поначалу такое предположение было вполне оправдано и не вызывало опасений. Однако по происшествии некоторого времени компьютерные сети достигли определенного уровня развития и широкого распространения. К 1985 году стало понятно, что предположение о том, что одна организация будет иметь только одну сеть и удовлетворится единственным подключением к глобальной сети Internet, больше не соответствует действительности.

[3] *Т.е. в такой иерархии, когда предполагается, что адрес состоит из двух частей и записывается в виде "сеть.узел". — Прим. ред.*

По мере того как организации начали создавать многочисленные сети, для проблемной группы проектирования Internet (Internet Engineering Task Force — IETF) стало очевидным, что требуется механизм разделения многочисленных логических сетей, появляющихся как подмножества второго уровня сети Internet. В противном случае стало бы невозможным организовать эффективную маршрутизацию данных до определенной конечной системы, принадлежащей организации с многочисленными сетями.

Классы сетевых IP-адресов

Как уже говорилось, сети разных классов могут содержать от 254 до 16,8 млн. адресов узлов. Чтобы наиболее эффективно использовать имеющийся ограниченный запас сетевых IP-адресов, каждая сеть может быть разделена на подсети меньшего размера. На рис. 10.27 показано разделение на сетевую и узловую части адресов сетей разных классов.

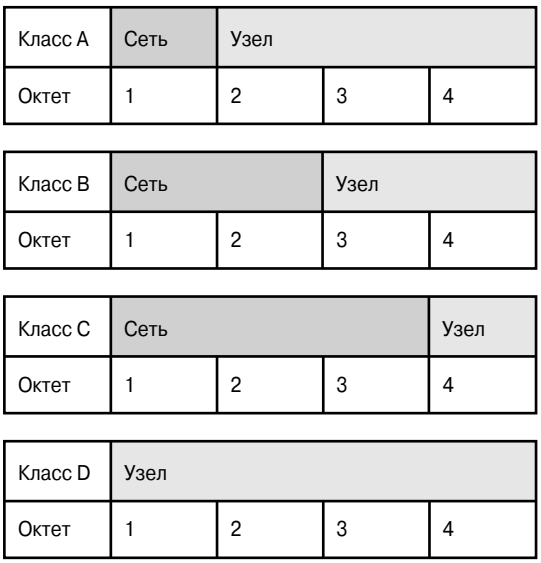


Рис. 10.27. Сети классов A-D: сетевая и узловая части

Введение в технологию подсетей и ее обоснование

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

Помимо повышения управляемости, создание подсетей позволяет сетевым администраторам ограничить широковещательные рассылки и реализовать механизм низкоуровневой безопасности в локальной сети. Безопасность при использовании подсетей в локальных сетях реализуется благодаря тому, что доступ в другие подсети организуется через маршрутизаторы. Маршрутизатор, как рассказывается в главе 22, "Списки управления доступом", может быть настроен таким образом, чтобы разрешить или запретить доступ к подсети на основе различных критериев, реализуя таким образом политику безопасности. Некоторые организации, обладатели сетей классов A и B, обнаружили также, что использование механизма выделения подсетей может принести дополнительные доходы за счет продажи или передачи в аренду ранее не использовавшихся IP-адресов.

На рис. 10.28 показано, как в среде с многочисленными сетями каждая из них подключена к сети Internet посредством единой точки доступа — общего маршрутизатора. Подробности и детали организации внутренней сети несущественны для сети Interenet. С использованием подсетей можно организовать частную сеть, в которой внутренние устройства будут заниматься доставкой данных пользователей. Таким образом, задача устройств сети Internet состоит только в том, как доставить данные сетевому маршрутизатору-шлюзу, посредством которого частная сеть подключена к глобальной. Внутри частной сети узловая часть IP-адреса может быть разделена на части для создания подсетей.

Поскольку *адрес подсети* формируется из узловой части адреса класса A, B или C, он назначается локально, обычно местным сетевым администратором. Кроме того, как и остальные части IP-адреса, каждый адрес подсети должен быть уникальным внутри области их использования (рис. 10.29).

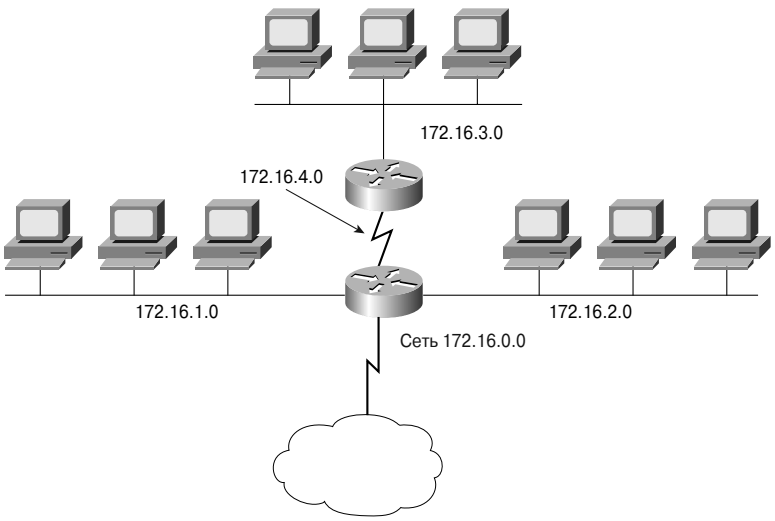


Рис. 10.28. Подсети

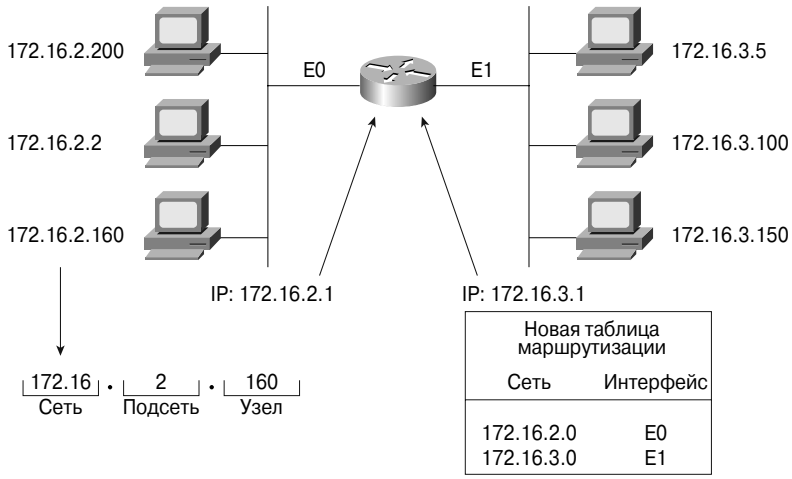


Рис. 10.29. Адреса подсетей

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

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

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

Адрес подсети включает сетевую часть адреса классов A, B и C плюс поле подсети и поле узла. Эти поля создаются на основе оригинального IP-адреса заимствованием битов из узловой части адреса и присоединением к исходной сетевой части адреса. Как показано на рис. 10.30-10.32, возможность деления оригинальной узловой части адреса на новые подсети и адреса узлов предоставляет гибкость в выборе схемы адресации для сетевых администраторов. Это означает, что у сетевого администратора

есть более широкий выбор при выборе схемы адресации как изначально, так и при расширении сети.

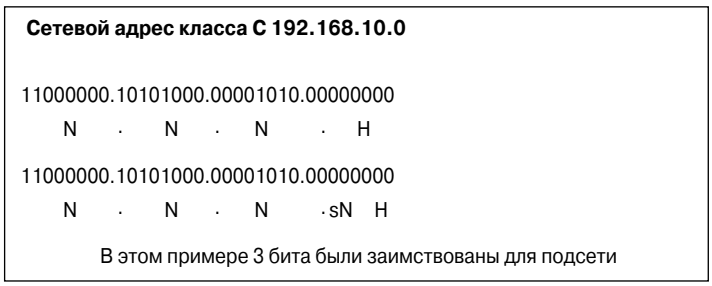


Рис. 10.30. Деление узлового октета адреса класса C

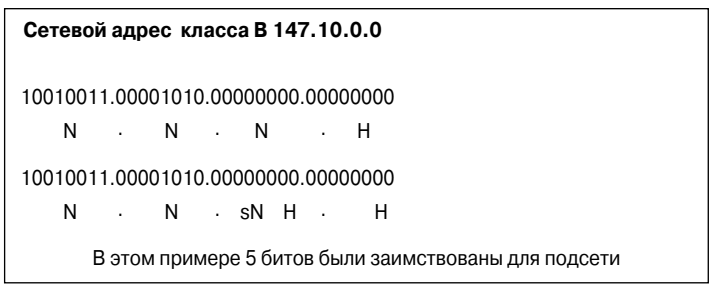


Рис. 10.31. Деление узлового октета адреса класса B

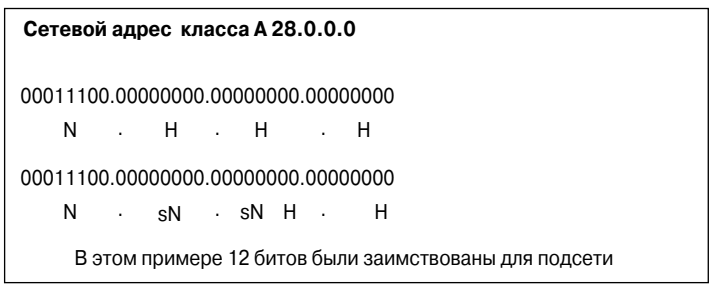


Рис. 10.32. Деление узлового октета адреса класса A

Назначение маски подсети

Выбор необходимого количества битов для создания подсети зависит от требуемого максимального количества узлов в подсети. Чтобы вычислить результат заимствования определенного количества узловых битов для создания подсети, необходимо иметь базовые знания из области двоичной математики и помнить битовые значения в каждой из позиций октета, как показано в табл. 10.2.

Таблица 10.2. Расчет подсети: позиция бита и соответствующее ему десятичное значение

Бит	1	2	3	4	5	6	7	8
Значение	128	64	32	16	8	4	2	1

Независимо от класса IP-адреса, последние 2 бита в последнем октете никогда не могут быть использованы для формирования подсети. Они называются *наименее значимыми битами*. Заимствование всех доступных битов, за исключением двух последних, позволяет создать подсеть, которая содержит только два узла. Такой способ используется на практике для экономии адресов при адресации последовательных связей между маршрутизаторами. Однако для работающих локальных сетей это вызвало бы недопустимые расходы на оборудование.

Чтобы создать *маску подсети*, дающую маршрутизатору информацию, необходимую для вычисления адреса подсети, которой принадлежит конкретный узел, необходимо выбрать столбец из таблицы с нужным количеством битов и в качестве значения маски воспользоваться числом строкой выше из того же столбца, как показано в табл. 10.3. Это значение получено в результате сложения двоичных значений для знакомест используемых битов. Как показано в табл. 10.3, если заимствованы 3 бита, маска подсети для сети класса C будет равна 255.255.255.224. При использовании формата записи маски с обратной косой чертой он может быть представлен как "/27". Число, указанное после символа обратной косой черты, представляет собой количество битов, составляющих адрес сети, плюс биты, использующиеся для маски подсети.

Таблица 10.3. Расчет подсети: два формата маски подсети

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

Чтобы определить требуемое количество битов, разработчик сети должен рассчитать, какое максимальное число узлов будет в подсети, и общее количество подсетей. В качестве примера предположим, что необходимо разместить по 30 узлов в 5-ти подсетях. Чтобы определить необходимое количество битов для переназначения, воспользуемся строкой "Количество используемых узлов" табл. 10.4. Так, для использования 30-ти узлов требуются 3 бита. Таким образом будет создано 6 подсетей, что также удовлетворяет указанным выше требованиям. Следует помнить, что разница в количестве доступных узлов и полном количестве возникает из-за того, что первый доступный адрес является идентификатором сети, а последний — ее широковещательным адресом. Классовая маршрутизация не предоставляет механизм

использования соответствующих подсетей, в то время как при бесклассовой маршрутизации множество таких "потерянных" адресов доступно для использования, как показано в табл. 10.4. Глядя на таблицу, можно также оценить, какое количество подсетей и узлов будет потеряно, если бесклассовая маршрутизация не используется.

Таблица 10.4. Расчет подсети: подсети и узлы

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

Еще одним способом вычислить маску подсети и количество доступных подсетей и узлов является использование формул, которые приведены и объяснены ниже.

Количество доступных подсетей равно 2 в степени, равной количеству используемых для формирования подсети битов, минус 2:

$(2^{\text{количество заимствованных битов}}) - 2 =$ количество используемых подсетей.

Например, при заимствовании трех битов из узловой части сети класса С $2^3 - 2 = 6$ — количество используемых подсетей.

Количество доступных узлов равно 2 в степени, равной количеству оставшихся от заимствования битов, минус 2:

$(2^{\text{оставшиеся биты}}) - 2 =$ количество используемых узлов.

Например, при заимствовании трех битов из узловой части сети класса С для адресации узлов будут использоваться 5 битов, следовательно, количество узлов в каждой подсети равно $2^5 - 2 = 30$.

Создание подсети

Для создания подсети необходимо расширить часть адреса, с которой оперируют маршрутизаторы. В сети Internet устройства оперируют с сетью как с единым целым, согласно классам адресов A, B или C, которые задаются восемью, шестнадцатью или

двадцатью четырьмя битами в маске (т.е. номером сети). Поле подсети описывает дополнительные биты, давая возможность локальным маршрутизаторам оперировать разными подсетями внутри единой, большой сети.

В маске подсети используется тот же формат, что и в IP-адресе. Иными словами, маска подсети состоит из четырех октетов, а длина ее составляет 32 бита. Сетевая часть маски подсети, как и часть, определяющая подсеть, состоит из всех единиц, а узловая ее часть заполнена нулем. Стандартно, если ни один бит не заимствован для разбиения сети на подсети, маска для сети класса B выглядит как 255.255.0.0. Если заимствованы 8 битов, соответствующая маска будет иметь вид 255.255.255.0, как показано на рис. 10.33 и 10.34. Поскольку в адресе класса B выделены два октета под адреса узлов, для задания маски подсети может быть заимствовано не более 14 битов. В сети класса C используются только 8 битов для поля узла. Следовательно, для задания маски подсети может быть заимствовано не более 6 битов.

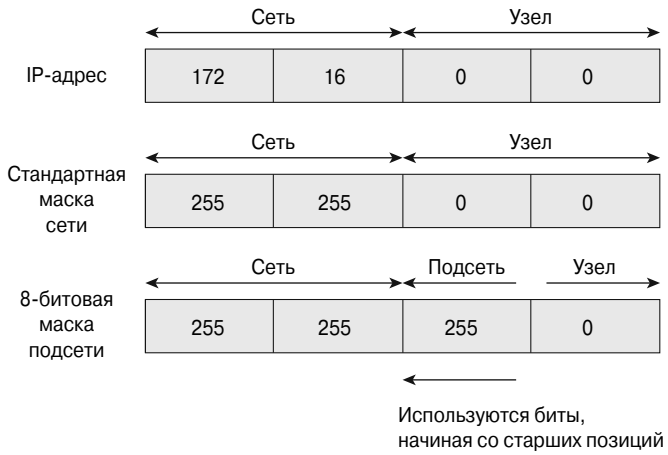


Рис. 10.33. Адреса сети и узла

Поле подсети всегда следует непосредственно за номером сети. Такое требование означает, что заимствовать можно первые *n* битов из стандартного поля узлов, где *n* — необходимая длина поля создаваемой подсети, как показано на рис. 10.35. Маска подсети является инструментом, который помогает маршрутизатору в определении сетевой (и используемой маршрутизатором) части адреса и его узловой части.

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

Рис. 10.34. Схема двоичных преобразований

Рис. 10.35. Создание подсети в адресе класса B

Дополнительная информация: определение размера маски подсети

Как уже говорилось, в маске подсети все биты в сетевой части (их количество определяется классом сети) и в части, которая описывает подсеть, равны 1, а все оставшиеся биты маски равны 0, поскольку они относятся к узловой части адреса.

Стандартно, если нет заимствования битов, маска подсети для сети класса B имеет значение 255.255.0.0; такая запись эквивалентна тому, что в первых 16 битах адреса, описывающих номер сети класса B, установлены единицы и нули в оставшихся 16 битах.

Если для задания поля подсети заимствованы 8 битов, маска подсети будет содержать дополнительные единицы еще в 8 битах и станет равна 255.255.255.0. Например, если маска подсети используется с адресом 130.5.2.144 для сети класса B (8 битов заимствованы для подсети), маршрутизатор будет знать, что такие пакеты следует направлять сети 130.5.2.0, а не сети с адресом 130.5.0.0, как это показано на рис. 10.36.

Рассмотрим другой пример: сеть класса C, адрес узла равен 197.15.22.131 и маска равна 255.255.255.224. Использование в последнем октете маски числа 224 (11100000 в двоичном виде) означает, что 24-битовый адрес сети класса C расширен на 3 бита, что в сумме дает 27 битов. Число 131 в последнем октете описывает третий, доступный для использования адрес узла в сети с адресом 197.15.22.128, как показано на рис. 10.37. Маршрутизаторы в сети Internet (которые не знают о маске подсети) отвечают только за доставку пакетов в сеть 197.15.22.0. Маршрутизаторы внутри этой сети, знающие о маске подсети, принимают решение об окончательной маршрутизации, используя 27 битов маски для вычисления адреса сети.

Рис. 10.36. Использование маски подсети для адреса класса B

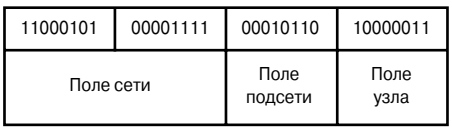


Рис. 10.37. Использование маски подсети: адрес класса C

Расчет маски подсети и IP-адреса

В процессе заимствования битов из поля узла важно уметь подсчитать количество дополнительных подсетей, создаваемых каждый раз при заимствовании каждого дополнительного бита. Мы уже говорили, что заимствование одного бита невозможно; наименьшее допустимое значение равно двум. Заимствуя два бита, можно создать четыре доступные подсети (2×2) (однако при этом следует помнить, что есть еще две зарезервированные не используемые подсети). При заимствовании каждого следующего бита из поля узла количество доступных подсетей увеличивается в 2 раза. Восемь подсетей создаются при заимствовании трех битов (2×2×2). Шестнадцать подсетей появятся в результате заимствования 4-х битов (2×2×2×2). Из перечисленных примеров, а также из схемы двоичных преобразований, показанной на рис. 10.34, можно сделать вывод, что каждый раз при заимствовании дополнительного бита количество доступных подсетей удваивается.

Расчет количества узлов в подсети

Каждый раз при заимствовании одного бита из поля узла количество битов, которые используются для указания номеров узлов, уменьшается. Строго говоря, каждый раз при заимствовании нового бита из поля узла количество адресов узлов, которые могут быть назначены, уменьшается вдвое.

Чтобы понять, как это происходит, рассмотрим для примера сетевой адрес класса C. Без маски подсети все 8 битов последнего октета используются в поле узла. Следовательно, могут быть использованы 256 (2^8) адресов для назначения узлам (254 за вычетом двух, которые, как известно, не могут быть использованы). Предположим теперь, что данная сеть класса C разделена на подсети. В случае, если заимствованы два бита из стандартных восьми, поле узла уменьшится до шести битов. Если воспользоваться всеми возможными комбинациями нулей и единиц в оставшихся шести битах, получится, что полное число доступных узлов, которые могут быть назначены узлам в каждой из подсетей, уменьшится до 64-х (2^6). Количество адресов узлов, которые могут быть использованы, равно 62.

Если в примере с адресом сети класса C заимствуются 3 бита, количество доступных битов в поле узла сократится до 5-ти и общее количество адресов узлов, которые могут быть назначены в каждой из подсетей, уменьшится до 32-х (2^5). Количество адресов узлов, которые могут быть использованы, равно 30-ти.

Количество возможных адресов узлов связано с количеством создаваемых подсетей. Например, для сети класса C и маски подсети 255.255.255.224 3 бита (224 в десятичной форме, что соответствует 11100000 в двоичной) заимствованы из поля узла. Подобным образом могут быть созданы 6 подсетей (8 - 2), в каждой из которых можно использовать 30 (32 - 2) адресов узлов.

Разбиение на подсети сетей класса A и B

Процесс разбиения на подсети сетей класса A и B полностью аналогичен процедуре, выполняемой для сетей класса C, но все же он немного сложнее, поскольку используется большее количество битов. Для использования в подсетях в сети класса A доступны 22 бита, в сети класса B — 24 бита, как показано на рис. 10.4139 и 10.3941.

Заимствование 12-ти битов из узловой части адреса сети класса B создает сетевую маску 255.255.255.240, или в другом обозначении — префикс /28. Все восемь битов третьего октета были использованы для создания маски, поэтому его значение равно 255-ти — максимальное значение восьми единичных битов. В четвертом октете были использованы только четыре бита, следовательно, его значение будет равно 240. Следует помнить, что маска подсети представляет собой сумму заимствованных битов и фиксированных битов сетевой части адреса.

Заимствование 20-ти битов в адресе класса A для создания подсети создает сетевую маску 255.255.255.240, или в другом обозначении — префикс /28. Все восемь битов второго и третьего октетов, а также 4 бита последнего октета в данном случае будут равны 1 и будут принадлежать маске подсети.

В рассмотренной ситуации на первый взгляд может показаться, что маски для сетей класса A и B будут абсолютно идентичными. Тем не менее, не зная, для какой сети или, точнее, для сети какого класса рассчитана маска, невозможно сказать, сколько в действительности битов было заимствовано для создания подсети.

Независимо от того, для сети какого класса необходимо рассчитать подсеть, правила расчета будут одинаковы:

общее количество подсетей = $2^{\text{количество заимствованных битов}}$;

общее количество узлов в подсети = $2^{\text{количество оставшихся от заимствования битов}}$;

общее количество используемых подсетей = $2^{\text{количество заимствованных битов}} - 2$;

общее количество используемых узлов в подсети = $2^{\text{количество оставшихся от заимствования битов}} - 2$.

Практическое задание 10.3.5a. Базовые принципы создания подсетей

В этом задании представлен краткий обзор механизма создания подсетей и использующейся в сетях операции логического умножения. По заданному адресу сети и с учетом дополнительных требований необходимо вычислить подходящую маску подсети, общее и доступное для использования количество подсетей и узлов в каждой из них. Кроме того, используя процедуру логического умножения, необходимо определить, является ли адрес получателя локальным или удаленным. И в конце на основании номера сети и маски подсети требуется определить, является ли действительным определенный IP-адрес узла.

Адрес сети класса B 147.10.0.0 (доступно 14 битов)
11001011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN . sN H В данном примере 12 битов было заимствовано для создания подсети

Рис. 10.38. Деление сети класса B на подсети

Адрес сети класса A 28.0.0.0 (доступно 22 бита)
00011100.00000000.00000000.00000000 N . H . H . H
00011100.00000000.00000000.00000000 N . sN . sN . sN H В данном примере 20 битов было заимствовано для создания подсети

Рис. 10.39. Деление сети класса A на подсети

Практическое задание 10.3.5b. Создание подсетей для сети класса A
В этом упражнении необходимо проанализировать сетевой адрес класса A для определения количества сетевых битов, выделяемых для создания маски подсети, количества подсетей, узлов в каждой подсети и информации об определенной подсети.

Практическое задание 10.3.5c. Создание подсетей для сети класса B
В этом упражнении необходимо проанализировать сетевой адрес класса B для определения количества сетевых битов, используемых для создания маски подсети, количества подсетей, узлов в каждой подсети и информации об определенной подсети.

Практическое задание 10.3.5d. Создание подсетей для сети класса C
В этом упражнении необходимо проанализировать сетевой адрес класса C для определения количества сетевых битов, которые могут быть использованы для создания маски подсети, количества подсетей, узлов в каждой подсети и информации об определенной подсети.

Вычисление адреса подсети посредством логической операции AND

Как уже говорилось, адрес сети или подсети содержит все нули в поле адреса узла. Для маршрутизации пакета маршрутизатор в первую очередь должен определить адрес сети или подсети получателя. Для этого маршрутизатор выполняет операцию логического умножения (операция AND или логическое “И”) с использованием IP-адреса узла получателя и соответствующей ему маски подсети.

Предположим, что для адресации используется сеть класса B с адресом 172.16.0.0. После оценки потребностей организации было заимствовано 8 битов для создания подсетей. Как было показано ранее, при заимствовании 8 битов маска подсети для сети класса B будет равна 255.255.255.0 (рис. 10.40).

	Сеть	Подсеть	Узел
IP-адрес узла 172.16.2.120	10101100 00010000	00000010	01111000
Маска подсети 255.255.255.0 или /24	11111111 11111111	11111111	00000000
Подсеть	10101100 00010000 172 16	00000010 2	00000000 0

Рис. 10.40. Использование 8-ми битов для задания подсети

Некто, находящийся вне данной сети, посылает пакет получателю с IP-адресом 172.16.2.120. Для определения направления, в котором следует отправить этот пакет, маршрутизатор производит логическое умножение (операция “И”) адреса с маской подсети.

В результате логического умножения двух чисел узловая часть адреса всегда получается равной нулю, и маршрутизатор вычисляет сетевой адрес, включающий подсеть. Таким образом, данные будут отправлены в подсеть с адресом 172.16.2.0, и только последний маршрутизатор, который рассчитывает маршрут, будет знать, что пакет необходимо доставить узлу с номером 120 в данной подсети.

Теперь предположим, что существует сеть с тем же адресом 172.16.0.0. Однако в этот раз заимствуются 7 битов для поля подсети. В двоичном виде маска выглядит для этого случая как 11111111.1111111.11111110.0000000. Как будет выглядеть данное значение в точечно-десятичном формате?

Как и в предыдущем примере, некто посылает пакет, адресованный узлу 172.16.2.120. Чтобы определить, куда следует отправить данные, маршрутизатор снова производит логическое умножение этого адреса и маски подсети. Как и ранее, при логическом умножении двух чисел узловая часть адреса будет равно нулю. В чем же разница между двумя приведенными выше примерами? Все выглядит идентично, по крайней мере, в десятичном виде. Разница состоит в количестве доступных подсетей и узлов в каждой из них. Отличие можно увидеть, только сравнив две разные маски подсети, как это показано на рис. 10.41.

При использовании семи битов в поле подсети можно выделить только 126 подсетей. Сколько узлов будет в таком случае доступно в каждой из подсетей? При 9 битах, используемых для узловой части, могут существовать до 510 узлов в каждой из этих 126-ти подсетей.

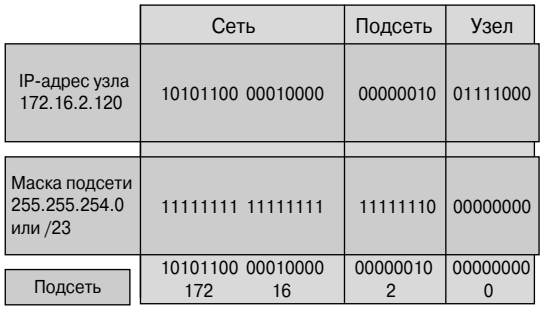


Рис. 10.41. Номер сети, расширенный дополнительными семью битами

Презентация: логическая операция "И"
В этой видеопрезентации проиллюстрирована логическая операция "И" (AND), которую выполняют маршрутизаторы над адресами и сетевыми масками.

Презентация: создание подсетей в сети класса C, часть 1
В этой видеопрезентации показан пример разбиения сети класса C на подсети.

Презентация: создание подсетей в сети класса C, часть 2
В этой видеопрезентации показан второй пример разбиения сети класса C на подсети.

Презентация: создание подсетей в сети класса C, часть 3
В этой видеопрезентации показан третий пример разбиения сети класса C на подсети.

Презентация: создание подсетей в сети класса B, часть 1
В этой видеопрезентации показан пример разбиения сети класса B на подсети.

Презентация: создание подсетей в сети класса B, часть 2
В этой видеопрезентации показан второй пример разбиения сети класса B на подсети.

Резюме

В главе была изложена информация по следующим ключевым вопросам:

- IP является протоколом без установления соединения, он не создает выделенный виртуальный канал между отправителем и получателем, перед тем как начать передачу информации;
- протокол IP также является ненадежным, поскольку в нем не содержатся механизмы, которые проверяют, достигли ли данные пункта назначения. Если требуется выполнить соответствующую проверку, то необходимо, чтобы протокол IP работал в связке с каким-либо транспортным протоколом с установлением соединения, например, протоколом TCP. Если же финальная проверка

и безошибочная доставка не требуются, протокол IP может быть использован в комбинации с каким-либо протоколом без установления соединения, например, протоколом UDP;

- службы без установления соединения зачастую называют процессами коммутации пакетов. Службы с установлением соединения зачастую называют процессами коммутации каналов;
- протоколы всех уровней эталонной модели взаимодействия открытых систем (OSI) добавляют контрольную и управляющую информацию в передаваемые данные по мере их продвижения по сети. Такая информация добавляется как в начало, так и в конец блока данных; сам процесс называется инкапсуляцией данных (т.е. упаковкой данных в информацию соответствующего уровня). На третьем уровне модели OSI добавляется сетевая, или логическая, адресная информация; на втором уровне модели добавляется локальная, или физическая, адресная информация;
- маршрутизация третьего уровня и коммутация второго представляют собой основные механизмы пересылки и доставки данных по сети. Изначально маршрутизатор принимает фрейм второго уровня, в котором инкапсулирован пакет третьего уровня, и обрабатывает его. Маршрутизатор должен отбросить информацию фрейма второго уровня, проверить и обработать пакет третьего уровня. Если пакет может быть доставлен локально, маршрутизатор должен инкапсулировать его в новый фрейм, который содержит правильный MAC-адрес в качестве идентификатора получателя. Если же данные должны быть доставлены в другой (удаленный) широковещательный домен, маршрутизатор должен инкапсулировать пакет третьего уровня в новый фрейм второго уровня, который в качестве адреса получателя содержит MAC-адрес следующего по маршруту межсетевого устройства. Таков процесс доставки данных по сети, от одного широковещательного домена другому; в итоге информация будет доставлена нужному конечному узлу;
- маршрутизируемые протоколы, например, IP, используются для транспортировки данных по сети. Протоколы маршрутизации позволяют маршрутизирующим устройствам выбрать оптимальный маршрут пересылки данных от отправителя получателю. Такие маршруты могут быть как статическими, т.е. такими, которые администратор сети вводит в конфигурацию устройства вручную, так и динамическими, т.е. такими, которые маршрутизатор получает посредством протоколов маршрутизации;
- если устройство использует динамический протокол или протоколы маршрутизации, оно обменивается информацией с другими маршрутизаторами посредством анонсов маршрутизации и таким образом поддерживает свои таблицы маршрутов в актуальном состоянии;
- алгоритмы маршрутизации используют метрики для обработки анонсов маршрутов и заполнения таблиц маршрутизации оптимальными (так называемыми наилучшими) маршрутами;

- время конвергенции протокола маршрутизации (или сети, если используются несколько протоколов) — это интервал после изменения в сети, по истечению которого все маршрутизаторы в сети обладают одинаковой информацией о ее структуре и маршрутах;
- протоколы внутреннего шлюза (IGP) используются внутри автономной системы (AS), протоколы же внешнего шлюза (EGP) предназначены для поиска оптимальных маршрутов между системами AS;
- протоколы IGP далее могут быть классифицированы по принципу работы: дистанционно-векторные и с учетом состояния каналов. В классических дистанционно-векторных протоколах маршрутизации периодически рассылаются анонсы маршрутизации, в которых содержится частичная либо полная таблица маршрутизации. В протоколах маршрутизации по состоянию каналов используется механизм LSA в качестве средства передачи анонсов, обновления информации о маршрутизации рассылаются только после изменения топологии сети, а не периодически; полная таблица маршрутизации рассылается значительно реже, чем в дистанционно-векторных протоколах;
- чтобы пакет мог быть передан по сети, устройствам необходимо наличие некоторого механизма, который позволит отличить часть IP-адреса от узловой. Маска адреса, 32-битовая величина, которую часто также называют маской подсети, указывает устройствам, какую часть IP-адреса следует трактовать как сетевую. Стандартная маска для сети класса A равна 255.0.0.0, для сети класса B — 255.255.0.0, а стандартная маска для сети класса C равна 255.255.255.0. С помощью маски подсети существующую стандартную классовую сеть можно разделить на подсети;
- чтобы предоставить сетевым администраторам дополнительную гибкость, сети, в особенности крупные, часто делятся на более мелкие, называемые подсетями. Механизм создания подсетей позволяет сетевым администраторам преодолеть ограничения, связанные с доступностью IP-адресов, с помощью деления целого сетевого адреса на множество подсетей, видимых только в пределах единой сети. Подсети позволяют уменьшить размеры широковещательных доменов, обеспечивают взаимодействие территориально удаленных сегментов локальных сетей посредством маршрутизаторов и повышение уровня безопасности за счет разделения участков локальных сетей;
- созданная администратором маска подсети использует больше битов, чем отведено для оригинальной классовой маски сети, поскольку биты заимствуются из узловой части адреса. Маска подсети состоит из трех частей:
  - оригинального номера сети;
  - адреса подсети, который создается за счет заимствования битов;
  - адреса узла, который формируется оставшимися незаимствованными битами;

- маршрутизаторы используют сетевые маски, чтобы определить адрес сети для входящего пакета. Это достигается с помощью логической операции "И" (AND);
- межсетевые функции сетевого уровня эталонной модели OSI включают в себя сетевую адресацию и выбор наилучшего пути для потока данных.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в настоящей главе.

Ключевые термины

IP-адрес — это 32-битовый адрес, назначаемый узлу при использовании протокола TCP/IP. IP-адрес принадлежит одному из пяти классов (A, B, C, D или E) и записывается в виде четырех октетов, разделенных точками (такой формат называется точечно-десятичным). Каждый адрес состоит из номера сети, необязательного номера подсети и номера узла. Адреса сети и подсети совместно используются для маршрутизации, а адрес узла необходим для доставки информации определенному сетевому узлу внутри сети или подсети. Маска подсети используется для извлечения из IP-адреса информации о сети и подсети. Механизм бесклассовой междоменной маршрутизации (Classless InterDomain Routing — CIDR) предоставляет новый способ представления IP-адресов и маски подсети. Этот тип адреса часто называют *Internet-адресом*.

MAC-адрес — это стандартизованный адрес канального уровня, необходимый каждому устройству, подключенному к локальной сети. Все устройства используют MAC-адреса, чтобы найти определенные устройства в сети, а также для создания и обновления таблиц коммутации и структур данных. Длина MAC-адресов составляет 6 байтов, контролируются они Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers — IEEE). Этот тип адреса также называют *аппаратным адресом* (hardware address), *адресом MAC-уровня* (MAC-layer address) и *физическим адресом* (physical address).

NetBEUI (расширенный пользовательский интерфейс NetBIOS — NetBIOS Extended User Interface) — это усовершенствованная версия протокола NetBIOS, используемого такими операционными системами, как LAN Manager, LAN Server, Windows for Workgroups и Windows NT. NetBEUI формализует транспортные фреймы и добавляет дополнительные функции. Механизм NetBEUI реализует протокол LLC2 модели OSI.

Автономная система — это отдельная сеть или набор сетей, находящихся под единым административным контролем, как, например, домен `Cisco.com`.

Адрес подсети — это часть IP-адреса, задающая подсеть с помощью маски подсети.

Алгоритм представляет собой четко заданные правила или процесс решения определенной проблемы. В области сетевых технологий алгоритмы в основном используются для определения наилучшего маршрута потока данных от конкретного отправителя к заданному получателю.

Бесклассовая междоменная маршрутизация (Classless InterDomain Routing — CIDR) — технология, поддерживаемая протоколом BGP (и многими другими) и основанная на агрегации маршрутов. Маршрутизация CIDR позволяет маршрутизаторам группировать маршруты, сокращая таким образом объем маршрутной информации, хранящейся в базовых маршрутизаторах. Благодаря использованию механизма CIDR несколько сетей могут быть сгруппированы и выступают в виде одного более крупного блока, который выглядит как единое целое для остальных сетей.

Дейтаграмма — логично связанный блок информации, передаваемой в сетевой среде в качестве модуля передачи сетевого уровня без предварительной установки виртуального соединения. IP-дейтаграммы являются основной единицей информации в сети Internet. Термины *ячейка*, *фрейм*, *сообщение*, *пакет* и *сегмент* также описывают способы логической группировки информации на разных уровнях модели OSI и разных технологических циклах.

Дистанционно-векторная маршрутизация представляет собой класс алгоритмов маршрутизации с последовательным подсчетом транзитных переходов пакета между маршрутизаторами на пути следования для расчета связующего дерева кратчайшего пути. Механизм обновления таблиц маршрутизации "дистанционно-векторный алгоритм" требует от каждого маршрутизатора из числа своих непосредственных соседей выслать свои полные таблицы маршрутизации. При использовании данного алгоритма маршрутизации возможно возникновение кольцевых маршрутов, однако механизм расчета маршрутов проще, чем у алгоритмов маршрутизации по состоянию канала. Этот тип маршрутизации основан на алгоритме Беллмана-Форда (Bellman-Ford).

Домен коллизий — область сети Ethernet, внутри которой распространяются сталкивающиеся фреймы. Концентраторы и повторители пропускают коллизии, коммутаторы локальных сетей, мосты и маршрутизаторы — нет.

Маршрутизатор — устройство сетевого уровня, использующее одну или несколько метрик для определения оптимального пути, по которому следует передавать поток данных. Маршрутизаторы передают пакеты между сетями на основе информации сетевого уровня, содержащейся в маршрутных обновлениях. Иногда такие устройства также называются *шлюзами (gateway)*, однако подобное определение шлюза на сегодняшний день является устаревшим.

Маршрутизируемый протокол — любой сетевой протокол, предоставляющий достаточно информации в адресе сетевого уровня, необходимой для передачи пакета от одного узла другому на основе принятой схемы маршрутизации.

Маска подсети — 32-битовые маски в протоколе IP, служат для указания битов IP-адреса, использующихся в адресе подсети. Иногда их называют просто *маской*.

Метрика маршрутизации представляет собой метод, с помощью которого алгоритм маршрутизации определяет, какой из маршрутов предпочтительнее. Информация о метрике хранится в таблицах маршрутизации и передается вместе с маршрутными обновлениями. В качестве параметров при расчете метрик могут использоваться пропускная способность, стоимость передачи данных, задержка, счетчик транзитных узлов, загрузка, параметр MTU, стоимость пути и надежность. Часто используют упрощенное понятие — *метрика*.

Октет — 8 битов. В области сетевых технологий термин октет часто используется (чаще, чем байт) по причине того, что в некоторых структурах используют байт, который не равен 8 битам.

Пакет — логически сгруппированная единица информации, включающая заголовок, который содержит контрольную информацию, и (зачастую) пользовательские данные. Чаще всего о пакете говорят как о модуле передачи информации сетевого уровня. Термины *дейтаграмма*, *фрейм* и *сегмент* также описывают различные логические единицы информации на разных уровнях модели OSI и на разных технологических стадиях.

Переход (hop) — прохождение пакетом данных расстояния от одного сетевого узла, обычно маршрутизатора, к другому.

Подсеть. 1. В IP-сетях — часть сети с общим адресом подсети. Сеть делится на подсети произвольно сетевым администратором; при этом обеспечивается многоуровневая, иерархическая структура маршрутизации, в то же время нет необходимости в сложной адресации присоединенных сетей. 2. В сетях OSI — набор систем ES и IS, находящихся под контролем одного административного домена и использующих один протокол сетевого доступа.

Протокол внешнего шлюза (Exterior Gateway Protocol — EGP) — Internet-протокол, использующийся для обмена маршрутной информацией между автономными системами. Протокол граничного шлюза (Border Gateway Protocol — BGP) является наиболее распространенным протоколом класса EGP.

Протокол внутреннего шлюза (Interior Gateway Protocol — IGP) — Internet-протокол, использующийся для обмена маршрутной информацией внутри автономных систем. Примерами широко используемых протоколов класса IGP являются IGRP, OSPF и RIP.

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP) — IGP-протокол, разработанный корпорацией Cisco для решения проблем маршрутизации в больших гетерогенных сетях.

Протокол маршрутизации — это протокол, реализующий маршрутизацию посредством использования определенного алгоритма поиска наилучшего пути. Примерами протоколов маршрутизации являются IGRP, OSPF и RIP.

Протокол маршрутной информации (Routing Information Protocol — RIP) — протокол IGP-типа, поставлявшийся с BSD UNIX-системами. Это наиболее широко распространенный протокол маршрутизации в локальных сетях. Протокол RIP использует в качестве метрики счетчик транзитных узлов.

Служба без установления соединения представляет собой механизм передачи данных без создания виртуального канала.

Служба с установлением соединения представляет собой механизм передачи данных, требующий установления виртуального канала.

Стек, или набор протоколов — это группа связанных, работающих совместно коммуникационных протоколов, обслуживающих взаимодействия на нескольких или всех семи уровнях модели OSI. Не все протоколы стека охватывают все уровни модели, и часто один протокол обслуживает одновременно несколько уровней. Типичным примером стека протоколов является набор TCP/IP.

Счетчик переходов (hop count) — это метрика маршрутизации, использующаяся для расчета расстояния между отправителем и получателем. Протокол RIP использует счетчик в качестве своей единственной метрики.

Таблица маршрутизации — таблица, хранящаяся в маршрутизаторах или некоторых других межсетевых устройствах и содержащая информацию о маршрутах до определенных сетей-получателей и, в некоторых случаях, связанные с ними метрики.

Широковещание — процесс, при котором информационный пакет рассылается всем узлам в сети. Получатель широковещательного пакета задается широковещательным адресом.

Широковещательный домен — это группа устройств, получающих широковещательные фреймы, отправленные одним из принадлежащих данной группе устройств. Обычно широковещательные домены ограничиваются маршрутизаторами (или в коммутируемых инфраструктурах посредством сетей VLAN), поскольку такие устройства не пересылают широковещательные фреймы.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Из скольких битов состоит IP-адрес?

а) 16.

б) 32.

в) 64.

г) Ни один из перечисленных выше ответов не является правильным.

2. Каково максимальное значение любого из октетов в IP-адресе?

а) 28.

б) 255.

в) 256.

г) Ни один из перечисленных выше ответов не является правильным.

3. Какую роль играет номер сети в IP-адресе?

а) Он задает сеть, которой принадлежит узел.

б) Он идентифицирует компьютер в сети.

в) Он определяет, какой узел в подсети адресуется.

г) Он определяет, с какими сетями может взаимодействовать устройство.

4. Какую роль играет номер узла в IP-адресе?

а) Он идентифицирует компьютер в сети.

б) Он определяет, какой узел в подсети адресуется.

в) Он задает сеть, которой принадлежит узел.

г) Он указывает, с какими узлами может взаимодействовать устройство.

5. Какое число является десятичным эквивалентом двоичного числа 101101?

а) 32.

б) 35.

в) 45.

г) 44.

6. Какому числу в двоичной форме будет соответствовать десятичное число 192.5.34.11?

а) 11000000.00000101.00100010.00001011.

б) 11000101.01010111.00011000.10111000.

в) 01001011.10010011.00111001.00110111.

г) 11000000.00001010.01000010.00001011.

7. Какой комбинации в десятичной форме соответствует двоичный IP-адрес 11000000.00000101.00100010.00001011 ?

а) 190.4.34.11.

б) 192.4.34.10.

в) 192.4.32.11.

г) Ни один из вышеперечисленных.

8. Какая часть IP-адреса класса B 154.19.2.7 является номером сети?

а) 154.

б) 154.19.

в) 154.19.2.

г) 154.19.2.7.

9. Какая часть адреса 129.219.51.18 описывает сеть?

а) 129.219.

б) 129.

в) 14.1.

г) 1.

10. Какой из перечисленных ниже адресов является широковещательным в сети 123.10.0.0 с сетевой маской 255.255.0.0?

а) 123.255.255.255.

б) 123.10.255.255.

в) 123.13.0.0.

г) 123.1.1.1.

11. Сколько адресов узлов может быть использовано в сети класса C?

а) 253.

б) 254.

в) 255.

г) 256.

12. Какое минимальное число битов может быть заимствовано для формирования подсети?

а) 1.

б) 2.

в) 4.

г) Ни один из перечисленных выше ответов не является правильным.

13. Что является основной причиной для использования подсетей?

а) Уменьшение размеров домена коллизий.

б) Увеличение количества адресов узлов.

в) Уменьшение размеров широковещательного домена.

г) Ни один из перечисленных выше ответов не является правильным.

14. Сколько битов содержится в маске подсети?

а) 16.

б) 32.

в) 64.

г) Ни один из перечисленных выше ответов не является правильным.

15. Выполнив логическую операцию, которую совершает маршрутизатор над IP-адресом 121.8.2.5 и маской 255.0.0.0, вычислите адрес сети/подсети.

а) 121.8.1.0.

б) 121.8.0.0.

в) 121.8.2.0.

г) Ни один из перечисленных выше ответов не является правильным.

16. Сколько битов было заимствовано для создания подсетей в адресе класса C 197.15.22.31 с маской 255.255.255.224?

а) 1.

б) 2.

в) 3.

г) Ни один из перечисленных выше ответов не является правильным.

17. Выполнив логическую операцию, которую совершает маршрутизатор над IP-адресом 172.16.2.10 и маской 255.255.255.0, вычислите адрес подсети.

а) 172.0.0.0.

б) 172.16.0.0.

в) 172.16.2.0.

г) Ни один из перечисленных выше ответов не является правильным.

18. Какое выражение из перечисленных ниже наиболее точно описывает одну из функций третьего уровня — сетевого уровня модели OSI?

а) Он отвечает за надежное сетевое взаимодействие между узлами.

б) Он связан с физической адресацией и топологией сети.

в) Он определяет наилучший путь для потока данных, следующего через сеть.

г) Он обслуживает обмен информацией между уровнями представления разных систем.

19. Какая функция позволяет маршрутизаторам обнаруживать доступные маршруты до пункта назначения и выбирать наилучший из них при пересылке пакета?

а) Информационная связь.

б) Определение маршрута.

в) Протокол SDLC-интерфейса.

г) Frame Relay.

20. Каким образом сетевой уровень передает пакеты от отправителя получателю?

а) Посредством использования таблицы маршрутизации.

б) При помощи ARP-ответов.

в) С помощью запросов к серверу имен.

г) С помощью запросов к мосту.

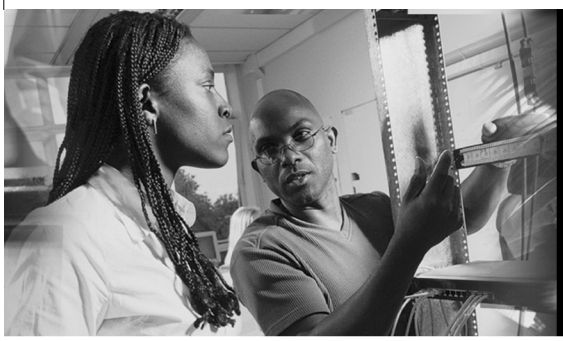
21. Какие две части адреса сетевого уровня используют маршрутизаторы для передачи данных через сеть?

а) Адрес сети и адрес узла.

б) Адрес сети и MAC-адрес.

в) Адрес узла и MAC-адрес.

г) MAC-адрес и маску подсети.



ГЛАВА 11
Уровень приложений и транспортный уровень стека протоколов TCP/IP

В этой главе...

- рассмотрены функции транспортного уровня стека протоколов TCP/IP;
- описан механизм управления потоком и его влияние на сетевой трафик;
- рассмотрены некоторые элементы процесса установления соединения между одноранговыми системами;
- описан механизм скользящего окна и его влияние на потоки данных в сети;
- описан процесс обмена уведомлениями;
- перечислены некоторые протоколы транспортного уровня и описано их назначение;
- описан формат заголовков и номера портов протоколов TCP и UDP;
- перечислены и описаны некоторые протоколы уровня приложений стека TCP/IP;
- рассмотрены некоторые широко известные приложения стека протоколов TCP/IP.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

порт, с. 548,
приложения, с. 549,
управление потоком, с. 550,
подтверждение, с. 551,
трехэтапное квитирование, с. 553,
механизм скользящего окна, с. 554,
протокол управления передачей, с. 558,
протокол передачи дейтаграмм пользователя, с. 559,
система доменных имен, с. 566,
протокол передачи файлов, с. 568,
простейший протокол передачи файлов, с. 569,
протокол передачи гипертекстовых файлов, с. 569,
гиперссылка, с. 570,
простой протокол передачи электронной почты, с. 571,
простой протокол управления сетью, с. 571,
telnet, с. 572.

Транспортный уровень использует службы, предоставляемые сетевым уровнем: службы выбора оптимального пути и логической адресации. Эти службы третьего уровня обеспечивают сквозное соединение между отправителем и получателем. В настоящей главе описано, как на транспортном уровне регулируются потоки информации, передаваемые от отправителя получателю. Транспортный уровень имеет следующие характеристики:

- поток данных транспортного уровня является логическим соединением между конечными точками сети;
- механизм скользящего окна обеспечивает сквозное управление и надежность соединения, позволяет отслеживать последовательность номеров пакетов и уведомлений;
- для управления различными сетевыми соединениями в протоколах четвертого уровня TCP и UDP и для передачи информации верхним уровням используются так называемые *порты* (port).

Основные характеристики уровня приложений (седьмого уровня) стека протоколов TCP/IP:

- на этом уровне выполняются приложения конечного пользователя;
- наиболее часто используемыми приложениями седьмого уровня являются NFS, DNS, ARP, rlogin, talk, FTP, NTP и traceroute.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Транспортный уровень стека TCP/IP

Согласно своему названию, транспортный уровень стека протоколов TCP/IP отвечает за транспортировку данных между приложениями устройства-получателя и устройства-отправителя. Знание принципов работы транспортного уровня является ключевым моментом, который необходим для глубокого понимания современных сетевых технологий. В последующих разделах подробно описаны функции и службы одного из самых важных уровней модели TCP/IP — транспортного.

Введение в транспортный уровень стека TCP/IP

Для описания четвертого, транспортного, уровня часто используется выражение *качество обслуживания*. Протокол UDP, который подробно рассматривается ниже, относится к транспортному уровню и обеспечивает работу транспортных служб без установления соединения. Однако основным протоколом, работающим на рассматриваемом уровне, является протокол TCP, который использует механизм установления соединения. Главными функциями этого протокола являются транспортировка

и надежное управление потоком информации от отправителя к получателю. К основным функциям транспортного уровня относятся обеспечение сквозного управления передачей, управление потоком посредством механизма скользящего окна (sliding window) и гарантирование надежности доставки за счет установки последовательных номеров и использования подтверждений.

Для того чтобы понять, для чего нужна надежность передачи данных и управление потоком, представьте себе иностранца, который очень быстро говорит. Его слушатель, скорее всего, будет вынужден иногда переспрашивать отдельные слова (аналог надежности передачи) и просить говорить медленнее (аналог потока). Таким образом, как показано на рис. 11.1, слушатель может воспринимать одну и ту же информацию по-разному и с разной скоростью в зависимости от своего уровня подготовки.

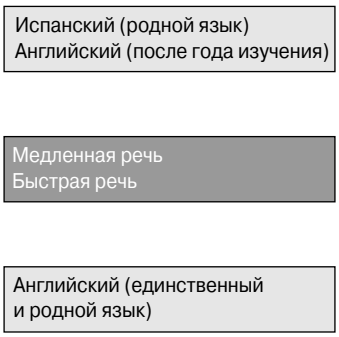


Рис. 11.1. Пример, поясняющий принципы работы транспортного уровня

Транспортный уровень предоставляет средства для надежной передачи данных от узла-отправителя узлу-получателю. На этом уровне создается логическое соединение между конечными точками сети; кроме того, к задачам транспортного уровня относятся сегментация и повторная сборка данных, передаваемых различными *приложениями* верхних уровней в один поток данных транспортного уровня. Этот поток обеспечивает сквозную передачу данных между конечными точками.

Поток данных транспортного уровня является логическим соединением между конечными точками в сети; на транспортном уровне также проверяется возможность установки соединения между приложениями. На рис. 11.2 проиллюстрирована работа транспортного уровня.

Транспортный уровень обеспечивает следующие функции:

- сегментацию данных приложений верхних уровней;
- управление сквозным взаимодействием;
- передачу сегментов от одного конечного узла другому;
- управление потоком посредством изменения размера окна;
- обеспечение надежности путем назначения номеров и использования подтверждений.

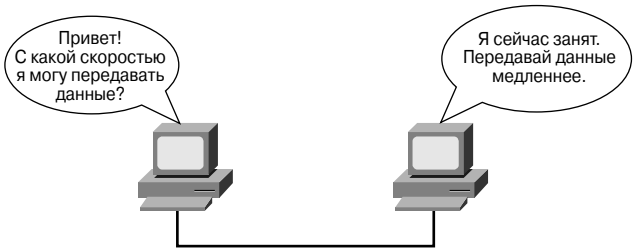


Рис. 11.2. Роль транспортного уровня во взаимодействии сетевых устройств

Для транспортного уровня внешнюю сеть можно представить в виде некоторой среды (изображаемой обычно в виде облака), по которой передаются пакеты данных от отправителя получателю. Такая среда отвечает за то, какой маршрут является оптимальным для конкретного получателя. Уже на этом этапе можно понять, какую важную роль играют маршрутизаторы в процессе передачи данных в сети.

Набор протоколов TCP/IP состоит из двух отдельных протоколов — TCP и IP. Протокол IP является протоколом третьего уровня без установления соединения, который обеспечивает эффективную передачу данных по сети. TCP является протоколом четвертого уровня, представляет собой службу с установлением соединения и обеспечивает управление потоком данных и, следовательно, высокую надежность передачи. Сочетание указанных двух протоколов позволяет решать широкий круг задач по передаче данных. Конечно же, стек протоколов TCP/IP состоит и из многих других протоколов, однако протоколы TCP и IP являются основными. К слову, вся сеть Internet основана именно на стеке протоколов TCP/IP.

Управление потоком

Когда протокол TCP транспортного уровня пересылает сегменты данных, он может гарантировать целостность данных. Одним из методов достижения этой цели является *управление потоком* (flow control), которое позволяет избежать проблем, связанных с ситуациями, когда узел на одном конце соединения переполняет буферы станции на другом конце. Переполнение вызывает серьезные проблемы, поскольку может привести к потере данных.

Службы транспортного уровня позволяют пользователям требовать надежного транспорта данных между узлами-отправителями и получателями. Чтобы обеспечить надежную передачу данных между коммуникационными партнерами-системами, используется механизм работы с установлением соединения. Надежная транспортировка обеспечивает следующие функции:

- гарантирует, что отправитель будет получать подтверждение о доставке каждого сегмента;
- обеспечивает повторную пересылку любых сегментов, подтверждение о доставке которых не было получено;

- позволяет сортировать сегменты в пункте назначения в правильном порядке;
- не допускает перегрузку сети и обеспечивает управление заторами в случае их возникновения.

Установка, управление и разрыв сеанса

В эталонной модели OSI несколько приложений могут одновременно использовать одно транспортное соединение. Функция транспортировки данных реализуются посегментно. Это означает, что различные приложения могут передавать данные по принципу "первым пришел, первым обслужен" (FIFO). Сегменты могут быть предназначены как одному получателю, так и разным. Это правило иногда называют механизмом мультиплексирования диалогов приложений верхнего уровня (рис. 11.3).

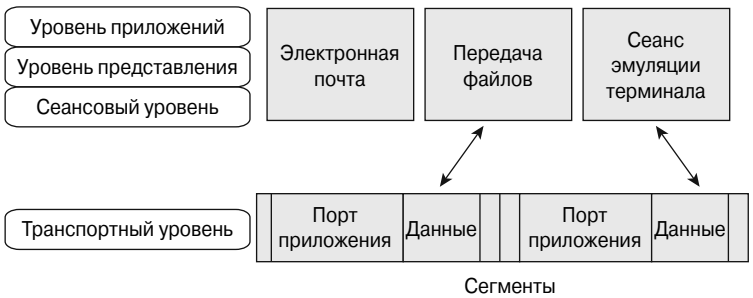


Рис. 11.3. Различные приложения самого верхнего уровня модели OSI используют транспортный уровень

Одна из основных функций транспортного уровня — это организация сеанса связи с установлением соединения с одноранговой системой. Чтобы начать передачу данных, приложения отправителя и получателя информируют свои операционные системы о инициализации соединения. Одна из станций инициализирует соединение, которое должно быть принято другой станцией. Модули операционных систем, отвечающие за работу протоколов, связываются между собой, отправляя специальное сообщение, и проверяют возможность передачи данных и готовность конечных узлов.

После завершения процесса синхронизации и установки соединения начинается передача данных. В процессе пересылки обе станции не перестают обмениваться сообщениями, которые позволяют убедиться, что принимаемые данные верны.

На рис. 11.4 проиллюстрировано типичное соединение между отправителем и получателем. Первое сообщение-запрос необходимо для синхронизации конечных узлов. Второе и третье необходимы для подтверждения начального запроса синхронизации; они также синхронизируют параметры соединения в обратном направлении. Последнее сообщение является *подтверждением* (acknowledgment), которое используется для информирования получателя о том, что обе стороны готовы установить соединение. После установления соединения начинается передача данных.

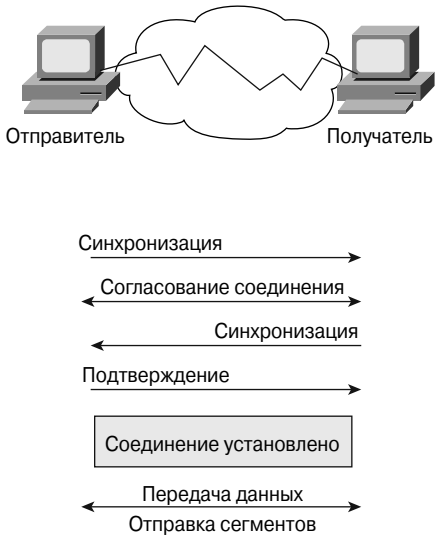


Рис. 11.4. Процесс установления соединения с одноранговой системой

В процессе передачи данных перегрузка может возникнуть по двум причинам. Первая состоит в том, что быстродействующий компьютер способен генерировать поток данных быстрее, чем сеть сможет его передать. Вторая возникает в ситуации, когда многим компьютерам одновременно необходимо отправить данные одному получателю. В таком случае получатель может испытывать перегрузку, хотя каждый отправитель в отдельности проблем не вызывает.

В тех случаях, когда дейтаграммы поступают слишком быстро и конечный узел или шлюз не успевают их обрабатывать, они временно сохраняются в памяти. Если интенсивность потока данных не уменьшается, то конечный узел или шлюз, исчерпав в конце концов свои ресурсы памяти, будут вынуждены отбрасывать все последующие дейтаграммы.

Чтобы предотвратить потери данных, транспортная функция может посылать отправителю информационное сообщение "устройство не готово к приему". Действуя как красный сигнал светофора, такое сообщение-индикатор сигнализирует отправителю о необходимости прекратить пересылку данных. После того как получатель снова сможет обрабатывать дополнительные данные, он посылает транспортное сообщение-индикатор "устройство готово к приему данных", который подобен зеленому сигналу светофора. Получая такой индикатор, отправитель может возобновить передачу сегментов.

После окончания передачи данных отправитель передает получателю сигнал, которой говорит о завершении передачи. Получатель подтверждает разрыв соединения, после чего соединение между машинами завершается.

Трехэтапное квитирование

Протокол TCP использует алгоритм работы с установлением соединения, поэтому перед передачей данных должно быть установлено логическое соединение. Для того чтобы установить сетевое соединение между двумя рабочими станциями, необходимо синхронизировать их начальные порядковые номера (ISN — Initial Sequence Number). Синхронизация достигается за счет обмена специализированными сегментами, которые содержат контрольный бит SYN (сокращение от synchronization) и номера ISN. Модули, которые несут в себе бит SYN, также иногда называют SYN-сообщениями. Для решения задачи установления нужно подобрать соответствующий механизм выбора ISN-номеров методом установки начального соединения для обмена ISN-номерами.

Для синхронизации необходимо, чтобы каждая сторона отправляла свой начальный порядковый номер ISN и принимала подтверждение в виде сообщения-уведомления ACK (сокращение от acknowledgment) от другого участника соединения. Кроме того, каждая сторона должна получать ISN-номер коммуникационного партнера и отправлять уведомление ACK об этом. Последовательность обмена сообщениями между двумя узлами сети, А и Б, описана ниже.

Такой обмен сообщениями называется *трехэтапным квитированием (three-way handshake)* (рис. 11.5).

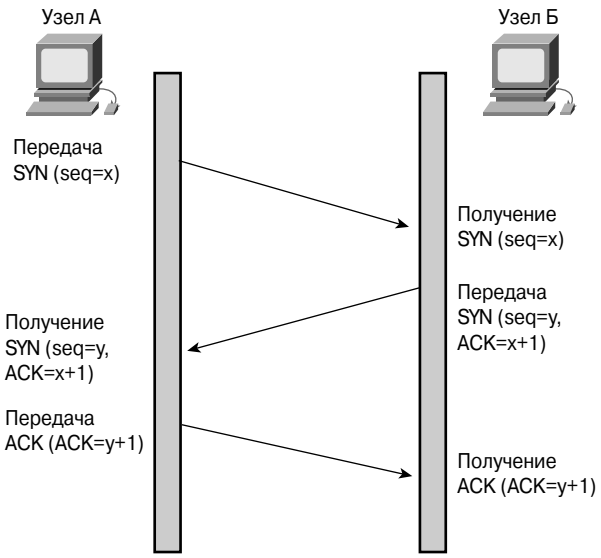


Рис. 11.5. Трехэтапное квитирование

1. **А → Б SYN.** Мой начальный порядковый номер ISN равен X, номер ACK — 0, бит SYN установлен, однако бит ACK не установлен.

2. **Б → А ACK.** Твой порядковый номер равен X+1, мой ISN-номер равен Y, биты SYN и ACK установлены.
3. **А → Б ACK.** Твой порядковый номер равен Y+1, мой порядковый номер — X+1, бит ACK установлен, а бит SYN не установлен.

Трехэтапное квитирование является асинхронным механизмом соединения, который необходим для синхронизации порядковых номеров, поскольку такие номера не зависят от некоторого виртуального глобального счетчика в сети. Поэтому в сети, работающей под управлением протокола TCP, используются различные механизмы назначения ISN-номеров. Одним из них является трехэтапное квитирование. Однако этот механизм предназначен не только для получения ISN-номера. При помощи него конечные устройства обмениваются информацией о размере окна передачи данных, параметре MTU и задержке передачи данных в сети. Получатель первого сигнала SYN не имеет в наличии средств, которые позволят определить, был ли полученный сегмент отложенным старым или новым сообщением, до тех пор пока не будет получено следующее сообщение; единственным исключением является случай, когда получатель хранит последний порядковый номер, используемый при соединении (что не всегда возможно). Таким образом, получатель должен запросить у отправителя проверку такого сообщения SYN.

Презентация: трехэтапное квитирование
Эта видеопрезентация посвящена методу установления соединения в протоколе TCP и механизму трехэтапного квитирования.

Механизм скользящего окна

В наиболее общей форме надежной пересылки данных с установлением соединения пакеты данных должны доставляться принимающей стороне в том же порядке, в котором они передавались. Протокол сигнализирует о сбое, если какие-либо пакеты данных теряются, повреждаются, дублируются или принимаются в другом порядке. Наиболее простым решением такой задачи является использование подтверждений получателя о приеме каждого сегмента данных.

Однако если отправитель вынужден ждать подтверждения после посылки каждого сегмента, как показано на рис. 11.6, то скорость передачи при таком способе значительно снижается. Поскольку с того момента, как отправитель заканчивает отсылку пакета данных, до момента завершения обработки какого-либо принятого подтверждения проходит определенный интервал времени, он может быть использован для передачи дополнительной порции данных. Количество пакетов данных, которое разрешается пересылать отправителю без получения подтверждения, называется *окном* (window).

В протоколе TCP используются так называемые ожидаемые подтверждения; они содержат номер, относящийся к октету, который ожидается следующим. Механизм скользящего окна заключается в том, что согласование размеров окна происходит динамически в течение TCP-сеанса. *Механизм скользящего окна* — это механизм управления потоком данных, который требует, чтобы получатель принимал подтверждение от отправителя после передачи некоторого количества данных.

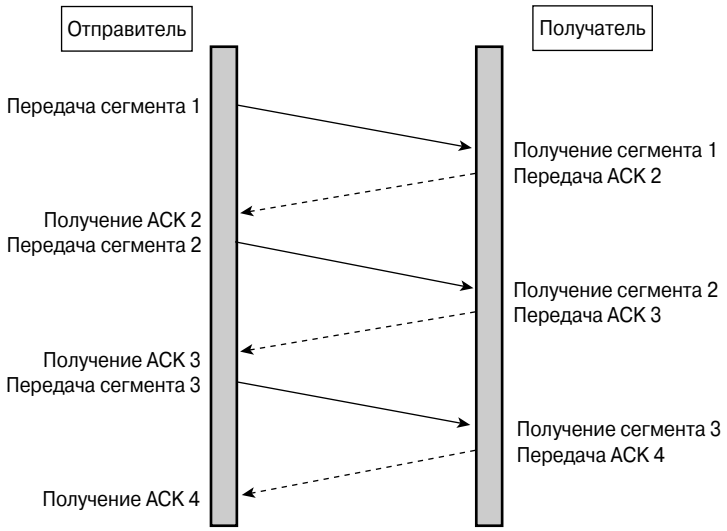


Рис. 11.6. Размер окна равен 1

Для управления потоком данных, передаваемых между двумя устройствами, в протоколе TCP используется *механизм управления потоком* (flow-control mechanism). Получатель докладывает отправителю о получении данных; получение такого уведомления позволяет установить размер окна. Окно определяет количество октетов, отсчитываемое от текущего номера подтверждения, которое TCP-устройство способно принять в заданный момент времени.

Например, при размере окна, равном 3, отправитель может передать получателю три октета. После этого он должен дождаться подтверждения от получателя. Если получатель получил три октета, он должен отправить подтверждение об этом отправителю октетов. После этого отправитель может передать следующие три октета. Если же получатель не получил три октета, например, при переполнении буфера, то он не отправит подтверждение. Если отправитель не получает подтверждение, это означает, что последние октеты нужно передать повторно и при этом снизить скорость передачи.

Размер окна TCP может изменяться в процессе передачи потока данных между двумя сетевыми устройствами. В каждом подтверждении, отправленном от получателя, содержится информация о количестве байтов, которые получатель способен принять. В протоколе TCP предусмотрено использование так называемого окна управления заторами, которое в нормальном состоянии равно окну устройства-получателя, но его размер уменьшается вдвое, если теряется какой-либо сегмент данных (например, при перегрузке в сети). Такой механизм позволяет уменьшать или увеличивать размер окна по мере необходимости в процессе управления буфером устройства и обработкой потока данных. Больший размер окна позволяет передать одновременно большее количество октетов.

Когда отправитель передает три октета, он переключается в режим ожидания сигнала ACK для четырех октетов. Если получатель способен обработать блок данных размером в два октета, то он отбрасывает третий октет и обозначает его как следующий ожидаемый блок данных. При этом указывается новый размер окна, который равен двум. Отправитель передает следующие два октета, однако размер окна все еще остается равным трем (предположим, устройство все же может обработать три октета одновременно). Получатель запрашивает октет с номером 5 и устанавливает новый размер окна, равный двум.

Презентация: механизм скользящего окна
В этой презентации описано, как маршрутизаторы управляют потоками данных с помощью механизма скользящего окна.

Подтверждения

Надежный механизм доставки гарантирует, что поток данных, пересланный одной станцией, будет доставлен по каналу передачи данных другой без дублирования или потери данных. Положительное подтверждение с повторной передачей является одной из методик, гарантирующих надежную доставку потоков данных. Положительное подтверждение требует, чтобы получатель общался с отправителем, посылая ему назад сообщение подтверждения после приема данных. Отправитель регистрирует каждый переданный им пакет и перед отправкой следующего пакета данных ждет подтверждения. В момент пересылки сегмента отправитель также запускает таймер и повторно передает блок данных, если установленное таймером время истекает до поступления подтверждения.

На рис. 11.7 показан отправитель, который передает пакеты 1, 2 и 3. Получатель подтверждает прием пакетов, запрашивая пакет 4. Отправитель, получив подтверждение, посылает пакеты 4, 5 и 6. Если пакет 5 не доставляется получателю, он посылает соответствующее подтверждение с запросом о повторной отправке пакета 5. Отправитель повторно отсылает пакет 5 и должен получить соответствующее подтверждение, чтобы продолжить передачу пакета с номером 7.

Протокол TCP обеспечивает соблюдение последовательности сегментов с последующим подтверждением. Каждой дейтаграмме перед передачей присваивается номер (рис. 11.8). После того как получатель принял все дейтаграммы, они собираются в завершенное сообщение. В обязанности протокола TCP входит восстановление поврежденных, утерянных, дублированных или пришедших в неверном порядке данных, которые передавались через сеть Internet. Механизм восстановления функционирует за счет назначения порядкового номера каждому переданному октету, после приема которого получатель должен отправить подтверждение (ACK). Если же в течение интервала времени ожидания подтверждение не было получено, данные передаются отправителем повторно. После доставки октетов получателю их порядковые номера используются для сборки сообщения из фрагментов и устранения дубликатов. Поврежденные данные восстанавливаются при помощи контрольной суммы, которая добавляется к каждому передаваемому сегменту. Контрольная сумма

проверяется получателем, и, если она не совпадает, поврежденные данные отбрасываются.

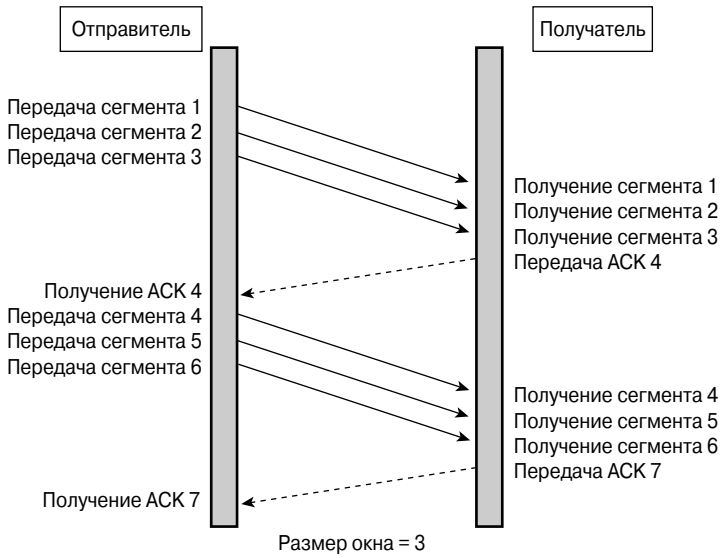


Рис. 11.7. Размер окна равен трем

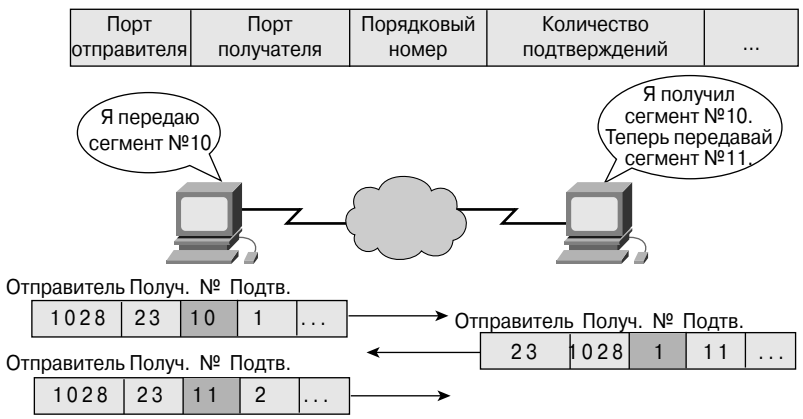


Рис. 11.8. Порядковые номера и подтверждения

Протокол TCP

TCP (*Transmission Control Protocol — протокол управления передачей*) является протоколом с установлением соединения транспортного уровня и обеспечивает надежную, дуплексную передачу данных. Протокол TCP является частью стека протоколов TCP/IP. В среде с установлением соединения для начала передачи данных между

двумя компьютерами должно быть установлено соединение. Протокол TCP отвечает за сегментацию сообщений в пакеты, повторную сборку их получателем и повторную передачу любых частей данных, если они не были приняты. Протокол также способен создавать виртуальные каналы между приложениями конечных пользователей.

Службы и протоколы верхнего уровня, которые используют механизмы TCP:

- FTP (File Transfer Protocol — протокол передачи файлов);
- HTTP (Hypertext Transfer Protocol — протокол передачи гипертекста);
- SMTP (Simple Mail Transfer Protocol — простой протокол электронной почты);
- DNS (Domain Name System — служба доменных имен).

На рис. 11.9 показан формат TCP-сегмента.

Рис. 11.9. Формат TCP-сегмента

Поля TCP-сегмента, показанные на рис. 11.9, описаны ниже.

- **Порт отправителя —** номер вызывающего порта.
- **Порт получателя —** номер вызываемого порта.
- **Порядковый номер —** номер, используемый для расположения поступающих данных в правильной последовательности.
- **Номер подтверждения** — номер следующего ожидаемого TCP-октета.
- **HLEN** — количество 32-разрядных слов в заголовке.
- **Зарезервированное поле** — все биты установлены в значение 0.
- **Биты кода** — служебные функции (например, установка и завершение сеанса).
- **Окно** — количество октетов, с которым отправитель готов согласиться.
- **Контрольная сумма** — расчетная контрольная сумма заголовка и полей данных.
- **Указатель срочных данных** — указывает конец срочных данных.
- **Параметры** — в настоящее время определен один параметр: максимальный размер TCP-сегмента.
- **Данные** — данные протокола более высокого уровня.

Протокол UDP

UDP (User Datagram Protocol — протокол передачи дейтаграмм пользователя), формат сегмента которого показан на рис. 11.10, является транспортным протоколом без установления соединения в стеке протоколов TCP/IP. UDP — это простой протокол, который осуществляет обмен дейтаграммами без подтверждения и без гарантии доставки. Простота протокола становится очевидной при сравнении форматов сегментов протоколов UDP и TCP. При использовании протокола UDP обработка ошибок и повторная передача данных должна осуществляться протоколом более высокого уровня. Например, если при пересылке данных по протоколу TFTP передача оборвалась, то только человек-оператор может повторно загрузить информацию.

В списке ниже перечислены поля UDP-сегмена, который показан на рис. 11.10.

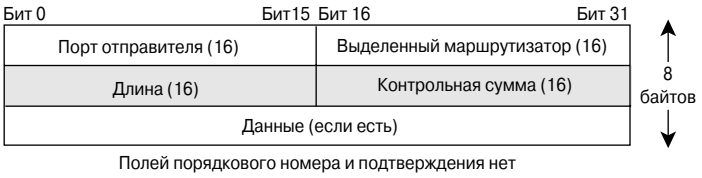


Рис. 11.10. Формат сегмента протокола UDP

- **Порт отправителя —** номер вызывающего порта.
- **Порт получателя —** номер вызываемого порта.
- **Длина** — количество байтов, включая заголовок и данные.
- **Контрольная сумма** — расчетная контрольная сумма заголовка и полей данных.
- **Данные** — данные протокола более высокого уровня.

В протоколе UDP не используется механизм скользящего окна, поэтому надежность передачи данных должна обеспечиваться *протоколами уровня приложений* (application layer protocol). Протокол UDP был разработан для приложений, у которых нет необходимости соединять вместе упорядоченные сегменты.

Протокол UDP используют такие службы и протоколы верхнего уровня:

- TFTP (Trivial File Transfer Protocol — простейший протокол передачи файлов);
- SNMP (Simple Network Management Protocol — простой протокол управления сетью);
- DHCP (Dynamic Host Configuration Protocol — протокол динамической конфигурации узла);
- DNS (Domain Name System — служба доменных имен).

Номера портов протоколов TCP и UDP

Для передачи информации на верхние уровни как протокол TCP, так и протокол UDP используют номер порта (port) или так называемого сокета (socket). Номера портов используются для отслеживания различных взаимодействий, одновременно ведущихся в сети.

Разработчики прикладного программного обеспечения договорились пользоваться зарезервированными номерами портов, назначением которых руководит агентство по выделению имен и уникальных параметров протоколов Internet (IANA — Internet Assigned Numbers Authority). Например, при любом обмене, связанном с передачей данных по протоколу FTP, должны использоваться стандартные порты 20 (для данных) и 21 (для управления), как показано на рис. 11.11. Сетевым взаимодействиям, не связанным с приложениями, имеющими общеизвестный номер порта, номера портов присваиваются произвольным образом, но при этом они выбираются из конкретного диапазона значений — выше 1023. Некоторые порты зарезервированы в протоколах TCP и UDP. Несмотря на то что некоторые порты зарезервированы в протоколах TCP и UDP, приложения могут быть не жестко привязаны к этим номерам. В табл. 11.1 перечислены наиболее часто используемые номера портов протоколов TCP и UDP.

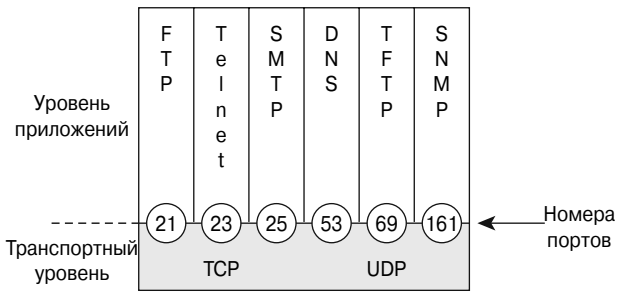


Рис. 11.11. Некоторые зарезервированные номера портов

Таблица 11.1. Зарезервированные номера портов протоколов TCP и UDP

Номер порта[1] (в десятичной системе)	Ключевое слово	Описание
0	—	Зарезервирован
1-4	—	Не назначены
5	`Rje`	Удаленное выполнение заданий
7	`Echo`	Эхо
9	`Discard`	Уничтожение сегментов
11	`Users`	Активные пользователи
13	`Daytime`	Время
15	`Netstat`	Активные соединения или сетевая статистика
17	`Quote`	Сообщение дня

[1] *Номера ниже 1024 считаются зарезервированными. Порты с номерами выше 1024 являются динамически назначаемыми. Зарегистрированные номера портов используются только для специализированных приложений. — Прим. ред.*

Окончание табл. 11.1

Номер порта (в десятичной системе)	Ключевое слово	Описание
19	`Chargen`	Генератор символов
20	`ftp-data`	Протокол FTP (данные)
21	`ftp`	Протокол FTP (управление)
23	`telnet`	Терминальное соединение
25	`Smtp`	Простой протокол передачи почтовых сообщений (SMTP)
37	`Time`	Время суток
39	`Rlp`	Протокол указания местонахождения ресурсов (RLP)
42	`Nameserver`	Сервер имен
43	`nickname`	Служба имен пользователей
53	`Domain`	Сервер доменных имен (DNS)
67	`Bootps`	Сервер протокола начальной загрузки
68	`Bootpc`	Клиент протокола начальной загрузки
69	`Tftp`	Протокол TFTP
75	—	Любая частная служба подключения к внешним системам по телефонной линии
77	—	Любая частная служба удаленного управления заданиями
79	`Finger`	Служба определения активных клиентов в сети
80	`HTTP`	Протокол передачи гипертекста
95	`SUPDUP`	Протокол SUPDUP
101	`HOSTNAME`	Сервер имен узлов
102	`ISO-TSAP`	Протокол ISO-TSAP
113	`AUTH`	Служба аутентификации
117	`UUCP-PATH`	Служба маршрутов UUCP
123	`Ntp`	Протокол синхронизации времени (NTP)
133-159	—	Не назначены
160-223	—	Зарезервированы
224-241	—	Не назначены
242-255	—	Не назначены

Как показано на рис. 11.12, для выбора соответствующего приложения конечная система использует номер порта. Номер порта отправителя — обычно какой-либо номер больше 1023, который присваивается динамически узлом-отправителем. Например, узел пытается соединиться с другим узлом по протоколу FTP, отправляя пакеты, в которых указан номер TCP-порта получателя 21 (FTP), и динамически генерирует номер порта отправителя 1028. Такая пара портов (отправителя и получателя)

определяет уникальность взаимодействия между двумя узлами. Если тот же узел инициирует FTP-соединение с третьим узлом, то порт получателя остается равным 21, но порт отправителя выбирается отличным от предыдущего (например, 1030), для того чтобы разделить два сеанса связи.

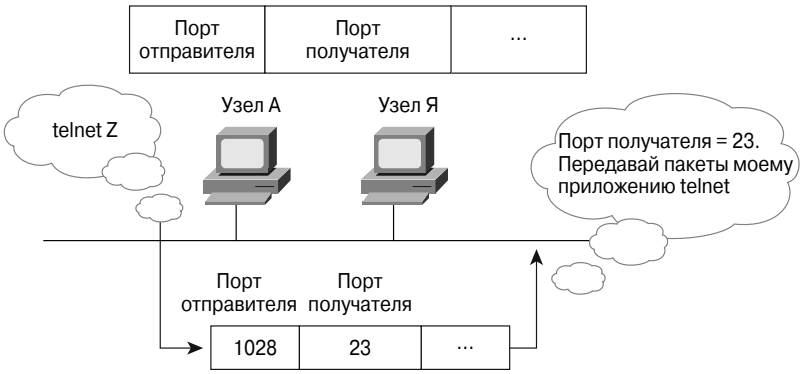


Рис. 11.12. Номера портов, определяемые используемым приложением

Уровень приложений

Последним уровнем (и самым верхним) моделей OSI и TCP/IP является *уровень приложений* (application layer). Уровень приложений наиболее близок к конечному пользователю при работе последнего с приложениями, такими, как приложения для пересылки и приема электронной почты через сеть. Принцип функционирования клиент-серверных приложений, службы доменных имен, различных сетевых приложений и многих других служб, список которых приведен ниже, зависит от уровня приложений.

- Клиент-серверные технологии.
- Перенаправление.
- Система доменных имен.
- Электронная почта.
- Служба Telnet.
- Серверы и клиенты протокола FTP.
- Протокол HTTP.

Введение в уровень приложений

В контексте эталонной модели OSI уровень приложений (седьмой) поддерживает коммуникационную составляющую приложения, как показано на рис. 11.13. Уровень приложений обеспечивает такие функции:

- идентификацию и определение доступности партнеров для связи;
- синхронизацию взаимодействующих приложений;
- установление соглашений по процедурам восстановления ошибок;
- управление целостностью данных.

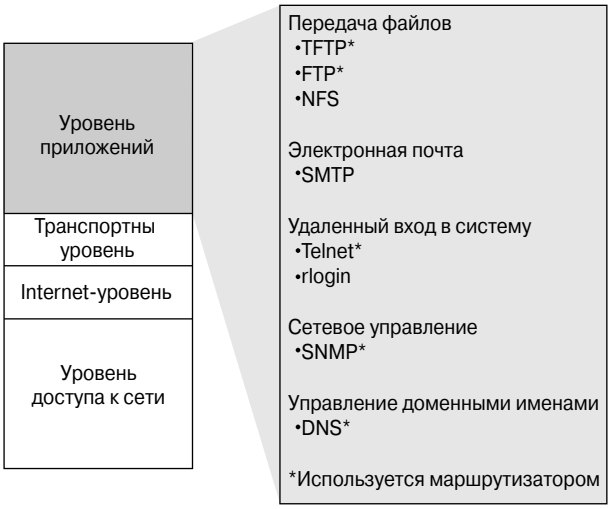


Рис. 11.13. Уровень приложений

Уровень приложений является наиболее близким к конечному пользователю при работе последнего с сетевыми приложениями. В функции уровня приложений входят задачи определения наличия доступных ресурсов для связи между системами. Без уровня приложений не было бы никакой сетевой поддержки в существующих пользовательских системах. Уровень приложений не обеспечивает никаких функций для других уровней, однако он обеспечивает некоторые функции процессам приложений, которые не может обеспечить модель TCP/IP, таким, как программы обработки электронных таблиц, текстовые процессоры и терминальные банковские программы. Кроме всего прочего, уровень приложений обеспечивает прямой интерфейс для взаимодействия с остальной частью модели сетевых приложений (например, браузеру или программе электронной почты) или косвенный интерфейс для локальных приложений (таких, как текстовые процессоры, электронные таблицы и программы создания презентаций).

Приложения, которые непосредственно взаимодействуют с сетью

Большинство приложений, которые работают в сетевой среде, взаимодействуют по технологии “клиент-сервер”. К ним относятся такие приложения, как FTP-клиенты, Web-браузеры, программы для чтения электронной почты. Эти приложения состоят из двух частей: клиентской части и серверной. Клиентская часть размещается на локальном компьютере и выполняет запросы к серверной части. Серверная

часть приложения размещена на удаленном узле и отвечает на запросы клиентской части.

Приложения типа "клиент-сервер" работают по следующей повторяющейся схеме: запрос клиента, ответ сервера; запрос клиента, ответ сервера. Например, Web-браузер получает доступ к Web-странице путем запроса URL-адреса, который перенаправляет браузер на соответствующий IP-адрес удаленного Web-сервера. После того как клиент определяет URL-адрес страницы, сервер отвечает на запрос, после чего, основываясь на информации, полученной от сервера, клиент может запрашивать другие порции информации от того же Web-сервера или же может получить доступ к другой Web-странице с другого Web-сервера.

Браузеры Netscape Navigator и Internet Explorer, скорее всего, являются самыми часто используемыми сетевыми приложениями. Web-браузер можно сравнить с пультом дистанционного управления телевизором. Пульт дистанционного управления дает вам возможность удаленно управлять функциями телевизора: громкостью, переключением каналов, яркостью и т.д. Для правильной работы пульта дистанционного управления вам совершенно не нужно знать его электрическую схему и принципы работы. То же можно сказать и о Web-браузерах. Браузеры дают возможность просматривать Web-страницы и переходить на новые, просто щелкнув по ссылке. Для нормальной его работы вовсе не нужно понимать принципы работы модели протоколов OSI, ее нижних уровней и механизмы их взаимодействия.

Приложения, которые косвенно взаимодействуют с сетью

В составе сетевой среды косвенно-сетевые приложения также поддерживают функции структуры "клиент-сервер". Если пользователь хочет сохранить файл из текстового процессора на сервере в сети, это осуществляется при помощи перенаправления. Стоит отметить, что прозрачность процедуры сохранения на сетевом сервере для пользователя поддерживается при помощи специализированной функции сеансового уровня — удаленного вызова процедур (Remote Procedure Call — RPC).

Перенаправление является функцией сеансового уровня модели OSI. Эта функция работает с операционными системами и сетевыми клиентами посредством специальных программ.

Примеры протоколов, в которых используется перенаправление, приведены ниже.

- AppleTalk Filing Protocol — протокол обмена файлами в среде AppleTalk.
- NetBIOS Extended User Interface (NetBEUI — расширенный пользовательский интерфейс NetBIOS[2]).

[2] *Network Basic Input Output System — сетевая базовая система ввода-вывода — стандартный сетевой интерфейс, предложенный для IBM PC и совместимых систем. — Прим. ред.*

- Протоколы IPX/SPX[3] компании Novell.
- Сетевая файловая система[4] (Network File System — NFS) стека протоколов TCP/IP.

Перенаправление позволяет администратору сети назначить удаленным ресурсам логические имена для локальных клиентов. Когда вы выбираете одно из логических имен для выполнения операции, такой, как сохранение файла или вывод его на печать, при помощи перенаправления этот файл передается для обработки удаленному ресурсу. Если же ресурс находится на локальном компьютере, то такой запрос игнорируется перенаправлением, что позволяет локальной операционной системе обработать его.

Причиной использования сетевого перенаправления для локального клиента является то, что приложения не могут распознать наличие или отсутствие сети. Кроме того, приложения, которые запрашивают службы, расположенные на локальном компьютере, при отсутствии перенаправления также не смогут получить доступ к ним.

Перенаправление позволяет расширить возможности несетевого программного обеспечения. Кроме того, оно позволяет пользователям предоставлять сетевой доступ к документам, шаблонам, базам данных, принтерам и многим другим типам ресурсов без использования специальных дополнительных программных средств.

Возможность объединения компьютеров в локальные сети оказала огромное влияние на разработчиков таких программ, как текстовые процессоры, программы обработки электронных таблиц, программы для создания презентаций, системы управления базами данных, графические пакеты и программы для разработки приложений. Подавляющее большинство перечисленного программного обеспечения в настоящее время имеет встроенную поддержку сети или средства для подключения таких возможностей. У этих программ есть возможность запуска интегрированных Web-браузеров или инструментов для работы в сети Internet и публикации результатов в виде HTML-отчетов, которые легко помещать в Internet.

Установка и разрыв соединения

Следует обратить внимание, что в каждом из примеров, упомянутых в предыдущих разделах, подключение к серверу было установлено только для выполнения одной задачи. В примере с Web-страницей подключение к серверу существовало только на время, необходимое для загрузки этой страницы. В примере с принтером подключение существовало только на время, необходимое для передачи на печать файла. После завершения операции соединение разрывается, и для последующих задач

---

[3] *Internetwork Packet Exchange — межсетевой пакетный обмен — протокол, используемый в качестве основного протокола в сетях Novell NetWare для обмена данными между узлами сети и приложениями, работающими на различных узлах. Sequenced Packet Exchange — упорядоченный пакетный обмен, или последовательный обмен пакетами, — протокол транспортного уровня сети; содержит расширенный по сравнению с IPX набор команд, позволяющий обеспечить более широкие возможности на транспортном уровне; обеспечивает гарантированную доставку пакетов — Прим. ред.*

[4] *Набор протоколов на основе транспортного протокола UDP, позволяющий Unix-машинам, PC и ПК Macintosh совместно использовать файлы в локальной сети. — Прим. ред.*

оно должно быть установлено заново. Описанный вариант — только один из двух путей сетевого взаимодействия.

Ниже в этой главе на примере протоколов telnet и FTP будет описан второй метод, при котором соединения после завершения сеанса не разрываются. При использовании этих протоколов соединение с сервером сохраняется на все время выполнения различных необходимых операций и разрывается по желанию пользователя. Все возможные соединения между компьютерами относятся к первой или второй категории. В следующем разделе описывается *система доменных имен* (Domain Name System — DNS), которая поддерживается процессами уровня приложений.

Служба DNS

Вся сеть Internet построена на иерархической системе адресации. Такой подход позволяет осуществлять маршрутизацию, основанную на классах адресов, а не на индивидуальных адресах. Однако использование IP-адресов не слишком удобно для пользователей. Так, различие между адресами 198.151.11.12 и 198.151.11.21 практически незаметно, хотя оба адреса принадлежат совершенно разным ресурсам в сети. Вероятность того, что пользователь ошибется и введет неправильный IP-адрес, очень высока, поскольку числовой IP-адрес никак не связан с тематикой ресурса.

ВНИМАНИЕ!

Подробная информация о доменных именах размещена на Web-сайте Агентства IANA (Internet Assigned Numbers Authority — Агентство по выделению имен и уникальных параметров протоколов сети Internet): `http://www.iana.org/domain-names.htm`.

Для привязки содержимого Web-страницы и ее адреса была разработана специальная система доменных имен (DNS). Служба DNS предназначена для трансляции IP-адресов узлов в имена и обратно. Домены — это группы узлов, расположенных в одной географической зоне, или же узлов, используемых для одних и тех же целей. Доменным именем называют строку символов и/или цифр, и обычно такое имя соответствует цифровому IP-адресу Web-узла в сети Internet. На сегодняшний день в сети Internet имеется более 200 доменов верхнего (зачастую называемых доменами первого) уровня. Домены первого уровня могут быть созданы по географическому признаку:

- `.us` — Соединенные Штаты;
- `.uk` — Объединенное Королевство;
- `.ru` — Россия;
- `.ua` — Украина.

Кроме того, существует много общих доменных имен:

- `.edu` — Web-страницы, посвященные образовательным учреждениям;
- `.com` — коммерческие Web-узлы;

- `.gov` — правительственные узлы;
- `.org` — некоммерческие Web-узлы;
- `.net` – сетевые службы;
- `.mil` – Web-узлы военных сил США;
- `.int` – Web-узлы интернациональных баз данных и соглашений.

Сервер доменных имен — это сетевое устройство, которое по запросу пользователей преобразовывает доменные имена в соответствующие IP-адреса и возвращает результат клиенту. Система доменных имен является строго иерархической, поэтому существуют несколько уровней имен и, соответственно, серверов DNS.

Если имя не может быть на месте транслировано в IP-адрес, то запрос передается вышестоящему DNS-серверу, который, в свою очередь, тоже пытается определить IP-адрес узла. Если на этом уровне DNS-сервер может преобразовать имя в IP-адрес, то результат запроса возвращается клиенту. Если же и этот сервер не может обнаружить необходимую запись, то запрос передается далее, вышестоящему серверу. Процесс повторяется до тех пор, пока не будет определен IP-адрес запрашиваемого узла или пока не будет достигнут DNS-сервер верхнего уровня. Если же для доменного имени не найден соответствующий IP-адрес и на этом уровне, то клиенту отправляется сообщение об ошибке. Все приложения, которые используют доменные имена для представления IP-адресов, обращаются к DNS-серверам, которые выполняют соответствующую трансляцию.

Службы FTP и TFTP

Протокол FTP (File Transfer Protocol — протокол передачи файлов) был разработан для загрузки файлов (получаемых от узла из сети Internet) или передачи файлов на удаленный компьютер (пересылка информации узлу в сети Internet). Возможность загружать и передавать на удаленный компьютер файлы является одной из самых востребованных функций в Internet. Протокол FTP является идеальным средством для людей, которые используют компьютер для многих целей и которым часто нужно обновлять драйверы и программное обеспечение. Подобно программам для работы с электронной почтой и терминальным соединением telnet, служба FTP является приложением типа “клиент-сервер”. Для работы клиентского программного обеспечения требуется наличие запущенного где-либо сервера.

FTP-соединение устанавливается так же, как и telnet-соединение. Аналогично, как и в случае с telnet-соединением, соединение завершается по желанию пользователя или же при наличии ошибок связи. Когда пользователь устанавливает новое FTP-соединение с FTP-процессом или служебной программой, ему необходимо ввести идентификатор пользовательского имени и пароль. Обычно используется имя `Anonymous` и адрес электронной почты пользователя в качестве пароля. Такой тип соединения называется *анонимным FTP-доступом*. После идентификации пользователя устанавливается соединение, подобное telnet-соединению, при котором команды, введенные клиентом, передаются серверу, а результат их выполнения возвращается клиенту. При помощи этой функции пользователь получает возможность

создавать и изменять каталоги, удалять и переименовывать файлы и выполнять многие другие функции.

Основным назначением протокола FTP является копирование файлов с одного компьютера на другой или передача файлов от сервера клиенту, а также от клиента серверу. При копировании файлов с сервера устанавливается дополнительное FTP-соединение, или канал связи, посредством которого и передаются данные. Передача данных может осуществляться в формате ASCII[5] или же в двоичном формате. Формат передачи данных определяет, как данные будут передаваться. При использовании ASCII-формата вся информация представлена в виде семи символов ASCII, удобных для восприятия человеком. Первым символом в этом случае является пробел или управляющий символ, после которого следуют три цифры, затем десятичная точка и еще две цифры. Если в числе стоит меньше трех цифр слева от десятичной точки, то дополнительный символ и цифры будут выравниваться по правому символу в поле из семи символов, и число будет записываться влево. Поскольку в двоичном формате для представления символа требуются только 4 байта в сравнении с 7 байтами в ASCII-формате, то передача данных в двоичном формате может осуществляться быстрее. Однако при использовании ASCII-формата есть свои преимущества. После завершения передачи данных подключение завершается автоматически. После того как программа завершит текущий сеанс копирования или перемещения файлов, достаточно просто выйти из системы и таким образом завершить сеанс.

Протокол TFTP (Trivial File Transfer Protocol — простейший протокол передачи файлов) является протоколом без установления соединения, который использует механизм UDP. Служба TFTP используется для передачи конфигурационных файлов и образов операционных систем Cisco IOS в маршрутизаторах и коммутаторах. Протокол разрабатывался маленьким и легким в использовании и установке, поэтому в нем отсутствует большинство функций протокола FTP. Единственное, что может выполнять данный протокол, — это читать и записывать файлы (или электронную почту) с или на удаленный сервер. Протокол TFTP не позволяет просмотреть список каталогов, и в настоящее время в нем не реализована аутентификация пользователей. Однако в некоторых локальных сетях этот протокол широко используется, поскольку он работает быстрее стандартного протокола FTP.

Другим протоколом, который позволяет загружать файлы, является протокол HTTP (Hypertext Transfer Protocol — протокол передачи гипертекста), который более подробно рассматривается в следующем разделе. Основным и самым существенным ограничением протокола HTTP является то, что пользователь может загружать файлы с сервера, но никак не может передавать файлы на сервер.

Служба HTTP

Протокол HTTP (Hypertext Transfer Protocol — протокол передачи гипертекстовых файлов) предназначен для работы с всемирной сетью World Wide Web, которая является самой быстроразвивающейся и наиболее используемой частью сети Internet.

[5] *American standard code for information interchange — Американский стандартный код обмена информацией. — Прим. ред.*

Главная цель существования служб WWW — это предоставление доступа к информации. Web-браузер, который используется для работы с интерактивной гипертекстовой информацией, является клиентским приложением, поэтому для его работы требуется сервер. Web-браузер позволяет представлять данные Web-страниц в мультимедийном формате совместно с текстом, графикой, аудио- и видеофрагментами. Статические Web-страницы создаются при помощи языка форматирования документов, который носит название HTML (HyperText Markup Language — язык гипертекстовой разметки). При помощи этого языка создаются правила форматирования страниц для Web-браузера. Кроме того, язык HTML позволяет указывать размещение текста, файлов и объектов, которые будут передаваться от Web-сервера Web-браузеру.

Гибкость и простота навигации по Web-сатйам обеспечивается за счет так называемых *гиперссылок* (hyperlink). Гиперссылка — это объект (слово, фраза или рисунок) на Web-странице, который после щелчка мыши по нему перенаправляет браузер на новую Web-страницу. Web-страница со ссылками содержит адреса размещения информации, которые называются URL (Uniform Resource Locator — унифицированный указатель информационного ресурса).

В табл. 11.2 показаны компоненты стандартного URL-адреса (в качестве примера рассмотрен `http://www.Cisco.com/edu/`).

Таблица 11.2. Компоненты URL-адреса

http://	**www.**	**Cisco.com**	**/edu/**
Указатель браузеру на используемый протокол	Указывает, что данная Web-страница должна быть обработана Web-браузером	Доменное имя Web-узла	Каталог, в котором размещена Web-страница. Если же имя не указано, то будет загружена стандартная страница, которая определяется на уровне сервера

Когда пользователь запускает Web-браузер, то первое, что он обычно видит, — это стартовая страница (или так называемая домашняя). URL-адрес стартовой страницы обычно хранится в конфигурации Web-браузера и может быть изменен в любой момент. Со стартовой страницы на нужную вам можно перейти по гиперссылке или же просто ввести URL-адрес в адресной строке браузера. После любого из указанных действий браузер проверяет протокол, чтобы определить, необходимо ли запускать другую программу для обработки страницы, и определяет IP-адрес Web-сервера. Далее создается сеанс связи с Web-сервером на транспортном уровне, сетевом уровне, уровне данных и физическом уровне. Данные, которые передаются на HTTP-сервер, содержат имя каталога, в котором размещена Web-страница (кроме всего прочего, такие данные содержат имя запрашиваемого HTML-файла). Если не было указано никакого имени, сервер использует стандартное имя (которое определяется конфигурацией сервера).

Отвечая на запрос клиента, сервер передает ему текстовые, аудио-, видео- и графические файлы в соответствии с HTML-инструкциями. Браузер клиента принимает эти данные и из них создает Web-страницу, которая отображается пользователю. Если пользователь выберет другую ссылку или введет другой адрес в адресной строке браузера, процесс повторится снова.

Практическое задание 11.2.4. Программное обеспечение Protocol Inspector, протокол TCP и HTTP

В этом задании описано, как пользоваться программным обеспечением Protocol Inspector компании Fluke Networks или любым другим эквивалентным продуктом, чтобы проследить процесс работы протокола TCP. Принцип работы этого протокола рассмотрен на примере работы службы передачи гипертекстовых файлов в процессе получения Web-страницы.

Протокол SMTP

Взаимодействие серверов при отправке и приеме электронной почты осуществляется посредством *протокола SMTP (Simple Mail Transfer Protocol — простого протокола передачи электронной почты)*. SMTP — это протокол, который используется для транспортировки электронных писем в ASCII-формате при помощи протокола TCP. Можно соединиться с SMTP-сервером, установив Telnet-сеанс на SMTP-порт (25). Такой тест — хороший способ проверки доступности почтового сервера.

Когда почтовый сервер принимает письмо, адресованное локальному клиенту, он сохраняет его и ожидает, когда пользователь проверит почту. Клиенты могут получать новые сообщения различными путями: они могут использовать специальную программу, которая соединяется непосредственно с почтовым сервером, или использовать один из многих других сетевых протоколов. Наиболее популярными являются протоколы POP3 (Post Office Protocol Version 3 — почтовый протокол версии 3) и IMAP4 (Internet Massaging Access Protocol Version 4 — протокол доступа к сообщениям в сети Internet версии 4). Оба протокола для передачи данных в качестве транспортного механизма используют протокол TCP. Чаще всего клиенты используют различные протоколы для получения почты, а для отправки писем в большинстве случаев служит протокол SMTP. Поскольку используются два различных протокола и возможно существование двух различных серверов для отправки и приема почтовых сообщений, почтовый клиент имеет возможность одновременно и отправлять, и принимать почту.

При проверке конфигурации почтового клиента необходимо отдельно настраивать свойства сервера-отправителя (SMTP) и сервера-получателя (POP или IMAP). Протокол SMTP не слишком хорош с точки зрения безопасности и не требует аутентификации пользователей. Для предотвращения неавторизированного доступа к серверу электронной почты и использования сервера в качестве посредника администратор сети должен запретить доступ к этому серверу из чужих сетей.

Протокол SNMP

Протокол SNMP (Simple Network Management Protocol — простой протокол управления сетью) является протоколом уровня приложений, который позволяет облегчить обмен управляющей информацией между сетевыми устройствами. Протокол SNMP помогает администраторам сети контролировать ее производительность, отыскивать и устранять проблемы в ее работе и планировать дальнейшее развитие сети.

Протокол SNMP состоит из следующих трех компонентов:

- **управляемого устройства** — сетевого узла, на котором установлен агент протокола SNMP и который расположен в управляемой сети. Управляемые устройства собирают и сохраняют информацию об управлении и предоставляют доступ к ней устройствам NMS при помощи протокола SNMP. Иногда управляемое устройство называют сетевым элементом. Сетевым элементом может быть маршрутизатор, сервер доступа, коммутатор, шлюз, компьютер или принтер;
- **агента** — модуля программного обеспечения, который размещен на управляемом устройстве. У агента имеется локальная база информации управления, он производит трансляцию этой информации в форму, совместимую с протоколом SNMP;
- **станции управления сетью (Network Management Station — NMS).** Она выполняет приложения, которые управляют сетевыми устройствами. Система NMS предоставляет процессорные ресурсы и выделяет память, необходимую для сетевого управления. В управляемой сети должны работать несколько систем NMS для повышения отказоустойчивости системы.

Служба telnet

Программа эмуляции терминала (telnet) обеспечивает удаленный доступ к другому компьютеру. Она позволяет подключиться к Internet-узлу и удаленно выполнять команды. Служба telnet часто используется для удаленного администрирования серверов и сетевого оборудования, например, маршрутизаторов и коммутаторов. Обычно клиентская часть сеанса telnet является *локальным узлом* (local host), а серверная часть, на которой используется специальное программное обеспечение, называется *удаленным узлом* (remote host) (рис. 11.14).

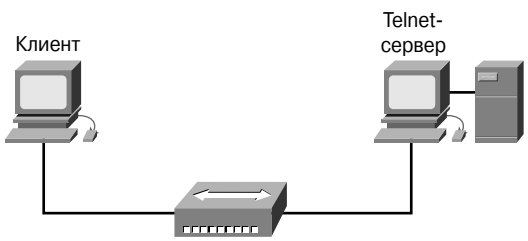


Рис. 11.14. Служба Telnet

Для создания соединения в режиме командной строки или в настройках telnet-клиента необходимо выбрать параметры соединения: прежде всего следует указать имя узла и тип терминала. В качестве имени узла нужно ввести IP-адрес удаленного сервера. Тип терминала определяет метод эмуляции выбранного терминала, посредством которого будет произведено соединение. Сеанс telnet не использует вычислительную мощность компьютера-клиента. Вместо этого программное обеспечение telnet передает нажатия клавиш удаленному компьютеру и принимает результаты их выполнения, которые выводятся на монитор клиента. Вся обработка и сохранение данных производятся на удаленном компьютере.

Когда в качестве имени узла в службе telnet вводится DNS-имя, оно должно быть транслировано в соответствующий IP-адрес. Приложение telnet работает основным образом поверх трех уровней модели OSI — уровня приложений (команды), уровня представления (формат, обычно ASCII) и сеансового уровня (передача информации). Вначале данные передаются транспортному уровню, где они сегментируются, затем дополнительно проверяется адрес, порт и наличие ошибок. После этого данные передаются сетевому уровню, где добавляется IP-заголовок (который содержит IP-адреса отправителя и получателя). Затем пакет передается канальному уровню, который инкапсулирует пакеты во фреймы данных, добавляет MAC-адреса отправителя и получателя. Если у узла-отправителя нет MAC-адреса, то выполняется ARP-запрос. После определения MAC-адреса фрейм посредством физического уровня (в двоичной форме) передается следующему устройству. Служба telnet является одним из самых лучших средств выявления неисправностей, поскольку с ее помощью можно проверить все семь уровней модели OSI, кроме того, telnet-соединение позволяет производить удаленную диагностику.

Когда данные достигают удаленного узла, он выполняет сборку исходной информации на основе полученных данных канального, сетевого и транспортного уровней. Удаленный компьютер, например, выполняет команду и передает результат обратно компьютеру клиента при помощи того же процесса инкапсуляции данных. Такой процесс отправки команд и получения результатов выполнения повторяется до тех пор, пока пользователь-клиент не завершит необходимые операции. После завершения коммуникации клиент разрывает сеанс связи.

Резюме

В этой главе были описаны функции уровня приложений стека протоколов TCP/IP и транспортного уровня. В ней также были рассмотрены различные процессы, происходящие при передаче пакета через оба уровня. Следует помнить о следующих функциях уровня приложений:

- идентификации, определении доступности сетевого партнера и готовности к взаимодействию;
- синхронизации взаимодействующих приложений;
- установлении соглашений по процедурам восстановления после сбоев;
- управлении целостностью данных.

Кроме указанных выше, уровень приложений поддерживает следующие функции:

- организует работу сетевых приложений, которые либо прямо, либо косвенно используют сеть;
- поддерживает работу системы доменных имен (DNS);
- обеспечивает работу служб Telnet, FTP и HTTP;
- работает совместно с протоколами TCP, UDP, SMTP и SNMP.

Дополнительную информацию по всем вопросам, рассмотренным в этой главе, можно найти на прилагающемся к книге компакт-диске, который содержит электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom).

Ключевые термины

DNS (Domain Name System) — система доменных имен. Система, используемая в сети Internet для трансляции имен узлов в сетевые адреса.

Американский стандартный код обмена информацией (American standard code for information interchange — ASCII) — наиболее распространенный код для представления буквенно-цифровых данных в компьютере, в котором используются двоичные числа для представления символов, набранных на клавиатуре.

Механизм скользящего окна (windowing) — механизм управления потоком, который требует, чтобы устройство-получатель получало подтверждение от устройства-отправителя после передачи определенной порции данных.

Порт (Port). В IP-терминологии представляет собой процесс верхнего уровня, который принимает данные от нижних уровней. Порты нумеруются и привязываются к конкретным процессам. Например, протокол SNMP приписан к порту с номером 25. Номер порта такого типа называется *зарезервированным портом, или адресом.*

Приложение (Application) — это программа, которая выполняет какую-либо функцию непосредственно для пользователя. Примерами сетевых приложений являются клиентские части протоколов FTP и telnet.

Протокол FTP (File Transfer Protocol) — протокол пересылки файлов. Прикладной протокол, являющийся частью группы протоколов TCP/IP и используемый для пересылки файлов между узлами сети. Протокол FTP описан в документе RFC 959.

Протокол HTTP — протокол передачи гипертекста (Hypertext Transfer Protocol). Протокол, используемый Web-браузерами и Web-серверами для передачи файлов, например, текстовых и графических.

Протокол TCP (Transmission Control Protocol) — протокол управления передачей. Протокол транспортного уровня с установлением соединения, обеспечивающий надежную полнодуплексную передачу данных. Входит в состав группы протоколов TCP/IP.

Протокол TFTP (Trivial File Transfer Protocol) — простейший протокол передачи файлов. Упрощенная версия протокола FTP, позволяющая передавать файлы от одного компьютера другому по сети.

Протокол UDP (User Datagram Protocol) — протокол передачи пользовательских дейтаграмм. Он является протоколом транспортного уровня без установления соединения из группы протоколов TCP/IP. UDP — это простой протокол, который обеспечивает обмен дейтаграммами без подтверждений или гарантий доставки, требуя, чтобы обработку ошибок и повторную передачу контролировал какой-либо другой протокол. Этот протокол описан в документе RFC 768.

Сигнал подтверждения (Acknowledgment) — извещение, посылаемое одним сетевым устройством другому, о том, что произошло некоторое событие (например, прием сообщения). Иногда он сокращенно обозначается как ACK.

Служба Telnet — стандартный протокол эмуляции терминала из группы протоколов TCP/IP. Протокол telnet используется для организации соединений с удаленного терминала и позволяет пользователям входить в удаленную систему и использовать ее ресурсы так, словно они подключены к локальной системе. Описан в RFC 854.

Трехэтапное квитирование (three-way handshake) — последовательность сообщений, которыми обмениваются два или более сетевых устройства для согласования и синхронизации параметров передачи данных перед началом передачи.

Управление потоком (Flow Control) представляет собой методику, благодаря которой не допускается ситуация, когда передающий объект переполняет данными принимающий объект. При полном заполнении буферов принимающего устройства посылающему устройству отправляется сообщение о необходимости отложить передачу данных до завершения обработки данных в буферах. В IBM-сетях этот метод называется *выравниванием скоростей.*

Уровень приложений (Application Layer) — это седьмой уровень эталонной модели OSI, обслуживающий прикладные процессы (такие, как электронная почта, пересылка файлов и эмуляция терминала), которые являются внешними по отношению к модели OSI. Уровень приложений идентифицирует и устанавливает доступность предполагаемых партнеров по коммуникации (и ресурсов, необходимых для их соединения), синхронизирует взаимодействующие приложения и устанавливает согласованный порядок выполнения процедур восстановления после сбоев и управления целостностью данных.

Язык HTML — язык гипертекстовой разметки документов (Hypertext Markup Language). Простой язык форматирования гипертекстовых документов, в котором для указания способа интерпретации заданной части документа прикладной программой визуализации, например, Web-браузером, используются дескрипторы (теги).

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. При разговоре с человеком, родной язык которого отличается от вашего, возможно, вам придется говорить медленнее и повторять некоторые слова. Повторение слов может быть сравнено с _____, а необходимость говорить медленнее подобна функции _____ транспортного уровня.

   а) Надежность; управление потоком.

   б) Управление потоком; надежность.

   в) Транспорт; подтверждение.

   г) Управление потоком; транспорт.

2. Какой протокол стека TCP/IP описывают следующие характеристики: с установлением соединения, повторная передача потерянных данных; деление исходящих сообщений на сегменты?

   а) IPX.

   б) TCP.

   в) UDP.

   г) SPS.

3. Что означает поле окна в сегменте TCP?

   а) Количество 32-битовых слов в заголовке.

   б) Номер вызываемого порта.

   в) Номер, используемый для обеспечения правильной последовательности получаемых данных.

   г) Количество октетов, которые устройство способно принять.

4. Какой транспортный протокол осуществляет обмен дейтаграммами без подтверждения и гарантированной доставки?

   а) UDP.

   б) TCP.

   в) IRQ.

   г) LLC.

5. Какое средство используют протоколы TCP и UDP для отслеживания сеансов связи, одновременно протекающих в сети?

   а) Номер порта.

   б) IP-адрес.

   в) MAC-адрес.

   г) Номер маршрута.

6. При помощи какого средства в протоколе TCP синхронизируется соединение между отправителем и получателем до передачи данных?
   а) Двухэтапное квитирование сеанса связи.
   б) Трехэтапное квитирование сеанса связи.
   в) Четырехэтапное квитирование сеанса связи.
   г) Функция Холтона.
7. Какой диапазон портов является нерегулируемым?
   а) Ниже 255.
   б) Между 256 и 512.
   в) Между 256 и 1023.
   г) Выше 1023.
8. Что случится с TCP-соединением, если сегмент данных не будет подтвержден в указанный период времени?
   а) В дальнейшем передача будет осуществляться при помощи протокола UDP.
   б) Виртуальный канал будет разорван.
   в) Ничего не случится.
   г) Будет выполнена повторная передача данных.
9. Какое выражение лучше всего описывает механизм управления потоком?
   а) Это метод управления ограниченной пропускной способностью.
   б) Это метод синхронного соединения двух узлов.
   в) Это метод предотвращения переполнения буфера.
   г) Это средство проверки данных на наличие вирусов перед отправкой.
10. Какое выражение лучше всего описывает цели использования стека протоколов TCP/IP?
    а) Набор протоколов, схожих с протоколами модели OSI верхнего уровня.
    б) Поддерживает все стандартные физические протоколы и протоколы передачи данных.
    в) Передает информацию от одного узла другому при помощи дейтаграмм.
    г) Осуществляет повторную сборку дейтаграмм в законченное сообщение на узле получателя.
11. Какой из протоколов используется на транспортном уровне?
    а) UCP.
    б) UDP.
    в) TDP.
    г) TDC.

12. Каково назначение номеров портов?

а) Они необходимы для отслеживания различных взаимодействий протоколов верхнего уровня, протекающих одновременно в одной сети.

б) Система отправителя использует их для организации сеанса.

в) Конечная система использует их для динамического назначения конечных пользователей отдельным сеансам в зависимости от используемого ими приложения.

г) Система отправителя генерирует их для предсказания адреса получателя.

13. Для чего используется трехэтапное квитирование в протоколе TCP? Выберите все подходящие ответы.

а) Для обеспечения возможности восстановления утерянных данных.

б) Для указания того, сколько данных может принять станция за один раз.

в) Для обеспечения рационального использования полосы пропускания.

г) Для преобразования двоичного ping-ответа в информацию верхних уровней.

14. Каково назначение динамического TCP-окна?

а) За счет увеличения размера окна больше данных может быть передано за один раз, что в результате повышает пропускную способность.

б) Размер окна изменяется для каждого блока дейтаграммы, что в результате повышает пропускную способность.

в) Этот механизм позволяет динамически устанавливать размер окна в TCP-сеансе, в результате более эффективно используется пропускная способность.

г) Этот механизм ограничивает входящие данные так, что все сегменты должны быть отправлены последовательно, в результате снижается пропускная способность.

15. Какие протоколы используются для надежной передачи UDP-сегментов?

а) Протоколы сетевого уровня.

б) Протоколы уровня приложений.

в) Internet-протоколы.

г) Протоколы управления передачей.

16. Сетевое перенаправление позволяет передавать данные _____.

а) Только сетевому серверу печати.

б) Только сетевому файловому серверу.

в) В одном направлении.

г) Ничего из указанного выше.

17. Примером приложения, которое основано на структуре "клиент-сервер", является _____.

а) Электронная почта.

б) Программа для работы с электронными таблицами.

в) NIC.

г) Утилиты для работы с жесткими дисками.

18. Клиентская сторона во взаимодействии "клиент-сервер" _____:

а) Расположена на удаленном компьютере.

б) Запрашивает обслуживание.

в) Более важная.

г) Постоянно размещена на сервере.

19. Какое утверждение лучше всего описывает доменное имя?

а) Оно соответствует цифровому адресу Internet-сайта.

б) Это то же, что и имя, которое дается первичному серверу.

в) Оно описывает месторасположение локальной сети.

г) Это IP-адрес, используемый для указания сервера печати.

20. `.com` — это домен, обычно назначаемый _____.

а) Машинам клиентов.

б) Заказчикам.

в) Компаниям, предоставляющим доступ к сети.

г) Корпорациям.

21. Во время telnet-соединения удаленный компьютер отвечает за _____.

а) Ни за что не отвечает.

б) Обработку.

в) telnet-приложение клиента.

г) Печать на стороне клиента.

22. В какой последовательности и какие три уровня модели OSI использует приложение telnet?

а) Уровень приложений, уровень сеансов, транспортный уровень.

б) Уровень представления, сеансовый уровень, транспортный уровень.

в) Канальный уровень, транспортный уровень, уровень представления.

г) Уровень приложений, уровень представления, уровень сеансов.

23. В типичном анонимном FTP-сеансе в качестве идентификатора пользователя используется _____ и _____ — в качестве пароля.

а) Anonymous; электронный адрес пользователя.

б) Электронный адрес пользователя; FTP.

в) FTP; FTP.

г) Guest; anonymous.

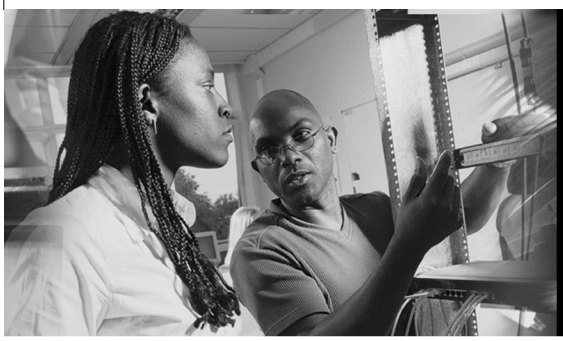
24. Вместо работы с определенным приложением механизм перенаправления работает с _____.

а) Операционной системой компьютера.

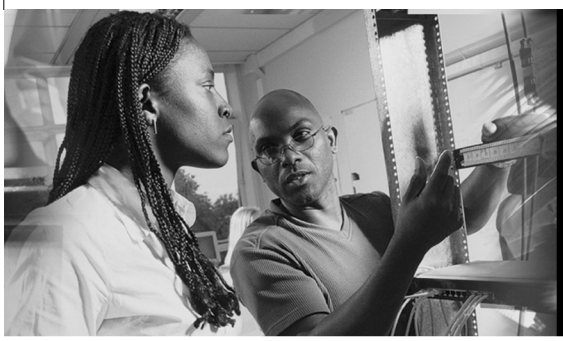
б) Электронной таблицей.

в) Электронной почтой.

г) Web-браузером.



ЧАСТЬ II
КУРС CCNA 2: МАРШРУТИЗАТОРЫ И ОСНОВЫ МАРШРУТИЗАЦИИ



ГЛАВА 12

Распределенные сети и маршрутизаторы

В этой главе...

- описаны различные типы WAN-соединений, инкапсуляции и протоколов;
- рассмотрены различия между сетями WAN и LAN и типы адресации, используемые в этих сетях, а также описаны используемые в разных типах сетей стандарты и протоколы;
- рассказывается о роли маршрутизаторов в распределенных сетях (WAN);
- описаны физические характеристики маршрутизаторов;
- перечислены основные типы портов, которые могут присутствовать на типичном маршрутизаторе;
- перечислены основные международные организации, которые отвечают за стандартизацию средств распределенных сетей;
- описаны внутренние компоненты маршрутизатора и рассмотрены их основные функции;
- описано, как правильно подключить последовательные, консольные и Ethernet-соединения к соответствующим портам.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

распределенная сеть, с. 584,
маршрутизатор, с. 584,
коммутатор, с. 584,
время безотказной работы, с. 585,
задержка распространения данных, с. 587,
модем, с. 587,
коммутация каналов, с. 596,
службы с коммутацией пакетов, с. 597,
службы с коммутацией ячеек, с. 598,
оборудование линии передачи данных, с. 604,
терминальное оборудование, с. 604.

В этой главе описаны WAN-устройства, технологии и стандарты. Кроме того, в ней рассказывается, как функционируют маршрутизаторы в распределенных сетях (WAN).

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в данной главе.

Распределенные сети

Распределенным сетям присущи несколько характерных особенностей, которые отличают их от локальных сетей (Local Area Network — LAN). В первой части главы представлен обзор технологий и протоколов распределенных сетей. В ней объясняются различия между локальными и распределенными сетями, а также указаны элементы, в которых эти сети очень похожи.

Введение в распределенные сети

Распределенная сеть (Wide-Area Network — WAN) — это сеть для передачи данных, которая охватывает большую географическую территорию. Распределенные сети часто используют в качестве средства передачи информации и данных крупные компании, например, телефонные.

Распределенная сеть (WAN) имеет несколько существенных отличий от локальной сети (Local Area Network — LAN). Например, в отличие от локальной сети, которая объединяет рабочие станции, периферийное оборудование, терминалы и другие устройства в одном здании или на небольшой географической площади, распределенная сеть соединят такие устройства на большой географической площади. Компании используют распределенные сети для объединения нескольких частей телекоммуникационной инфраструктуры в единую информационную структуру.

Распределенная сеть функционирует на физическом уровне (первый уровень) и на канальном уровне (второй уровень) эталонной модели OSI. Распределенная сеть объединяет локальные сети, которые обычно разделены большими географическими расстояниями, и обеспечивает обмен пакетами и фреймами данных между *маршрутизаторами и коммутаторами*.

В табл. 12.1 приведена классификация типов сетей.

Как показано на рис. 12.1, распределенные сети имеют такие основные характеристики:

- они соединяют устройства, разделенные большими географическими расстояниями;
- они используются крупными компаниями, в частности, телефонными, такими, как Bell, Sprint, MCI в США, British Telecom, German Telecom — в Европе, Укртелеком, Ростелеком и т.п.;

- в распределенной сети используются каналы с разной пропускной способностью на большой географической территории и на дальних расстояниях.

Таблица 12.1. Классификация сетей

Название	Размещение узлов сети	Расстояние между устройствами
Локальная сеть класса	Комната	10 м
Локальная сеть школы	Здание	100 м
Локальная сеть университета	Территория университета	1000 м = 1 км
Распределенная сеть корпорации Cisco Systems	Страна	100 000 м = 100 км
Распределенная сеть Африки	Континент	1 000 000 м = 1000 км
Распределенная сеть Internet	Планета	10 000 000 м = 10 000 км
Распределенная сеть Земли и искусственных спутников Земли	Системы Земли и Луны	100 000 000 м = 100 000 км

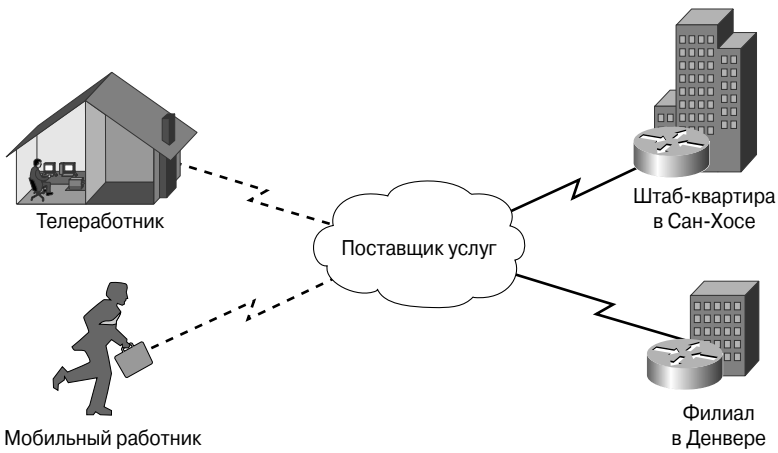


Рис. 12.1. Соединения распределенной сети

Дополнительная информация: критерии производительности распределенной сети

Время безотказной работы компонента

Каждый физический компонент распределенной сети может быть отслежен, может быть измерена его надежность на основании периода работоспособного состояния. *Время безотказной работы* (uptime) является параметром, противоположным *времени вынужденного бездействия* (downtime), и представляет собой промежуток времени, в течение которого сетевое устройство функционировало и обрабатывало запросы пользователей. Обычно статистическое время выше реального, поскольку часто запросы обрабатываются всего 5 дней в неделю, 12 часов в сутки, а в статистике учитывают работу 7 дней в неделю, по 24 часа в сутки.

Не следует забывать, что заявленные производителем параметры обычно выше реальных, и учитывать этот факт в своей профессиональной деятельности.

Поскольку сетевые устройства — очень сложные, то они периодически могут отказывать. Большинство производителей дает гарантию того, что их устройство может непрерывно проработать в течение определенного промежутка времени, называемого *средним временем безотказной работы (Mean Time Between Failures — MTBF*). Обычно показатель MTBF имеет значение около нескольких десятков тысяч часов. Такое время соответствует нескольким годам непрерывной работы. К сожалению, обычно эта оценка получается статистическим путем, а фактическое безотказное время работы устройства зависит от целого ряда факторов:

- диапазона колебаний температуры окружающей среды;
- отсутствия помех в питающем напряжении;
- качества обслуживания устройства до и во время работы.

Мониторинг и отслеживание времени работоспособного состояния отдельного сетевого элемента позволяет продемонстрировать пользователям качество сети и ее работоспособность. Кроме того, данные о времени непрерывной работы устройства могут использоваться для преждевременного выявления неполадок в сети и оценки риска отказа. Такие данные (или соответствующие им тенденции) могут быть использованы для оценки стабильности работы оборудования определенного типа или определенного производителя; впоследствии исследования устойчивости оборудования в целом могут быть расширены и использованы для оценки отказоустойчивости определенных компонентов.

Обратите внимание, что термин *доступность* используется в основном для описания периода непрерывной безотказной работы сети. Но, к сожалению, это не слишком хороший показатель для оценки инфраструктуры. Теоретически доступность сети указывает на ее надежность, однако на практике надежность и безотказность сети зависят от такого количества факторов, что этот показатель становится бессмысленным.

Для иллюстрации последнего утверждения рассмотрим пример: если в какой-либо точке сети выходит из строя маршрутизатор, то в такой точке всем пользователям сеть будет недоступна полностью. Однако в другой точке сеть будет доступна пользователям. Эти пользователи не смогут обращаться к узлам, расположенным в поврежденном участке сети, однако им ничего не будет мешать получить доступ к другим частям сети. Как видно из такого простого примера, доступность сети является очень размытым понятием, поэтому при оценке сети этот параметр может быть бесполезным.

Интенсивность потоков данных

Одной из наиболее важных характеристик любой распределенной сети является *интенсивность потоков данных* (traffic volume), поддерживаемых сетью. Интенсивность потоков данных непостоянна; она изменяется в зависимости от времени суток, рабочих и производственных циклов, сезонов и т.д. Иными словами, на постоянное значение интенсивности потока данных вы можете и не рассчитывать. Учитывая этот факт, производительность сети обычно оценивают на основании двух параметров: пиковой (максимальной) нагрузки и средней нагрузки.

- Максимальный объем, или максимальная интенсивность потока данных, которые способна передать сеть, известна под названием *пикового значения интенсивности потоков данных* (peak value). Как можно понять из названия, пиковое значение — это максимальный поток данных, который способна пропустить через себя сеть.
- *Среднее значение интенсивности потоков данных* (average value) — это разумная ожидаемая скорость поступления данных в сеть в течение дня.

Исходя из указанных выше двух параметров, обычно проектируется сеть и подбираются необходимые маршрутизаторы. Если ожидается в конкретном участке сети нагрузка до 100 Кбит/с, то пропускной способности в 56 Кбит/с будет явно недостаточно.

Задержка

Задержка является одним из наиболее часто используемых критериев оценки производительности сети. В общем случае *задержка* (delay) — это время между двумя событиями. В теории передачи данных такими двумя событиями обычно является передача и получение данных. Таким образом, задержка — это общее время, необходимое для передачи пакетов от отправителя получателю. Учитывая это определение, можно предположить, что задержка зависит от множества факторов. Покажем три самых распространенных типа задержки.

- *Задержка распространения данных (propagation delay)* — это суммарное время, необходимое для передачи или распространения данных от одного конца маршрута передачи к другому. Каждый элемент сети вносит свою лепту в такую задержку; кроме того, величина задержки зависит от объема данных, передаваемых через рассматриваемую сеть. Чем больший поток данных передается, тем меньше пропускной способности может быть отведено для передачи новых данных. Следует отметить, что задержка передачи данных присуща всем средствам коммуникации, независимо от того, ведется ли передача данных по медным проводам, оптоволокну или через воздух при помощи радиотехнических средств.
- *Задержки на восходящем или нисходящем спутниковом канале (satellite uplink/downlink delay)*. Для некоторых средств передачи, основанных на спутниковой связи, требуется, чтобы сигнал был передан на спутник, а затем получен обратно от спутника. Вследствие больших расстояний между наземными передающими станциями и спутниками такие задержки могут быть весьма значительными.
- *Задержка передачи данных (иногда называемая задержкой коммутации (forwarding delay).* Этот тип задержки обусловлен тем, что любому сетевому устройству необходимо затратить какое-то время на прием, буферизацию, обработку и передачу данных. Фактически задержка любого устройства непостоянна. Так, устройства, работающие на пределе своих возможностей, имеют гораздо большую задержку передачи данных, чем устройства, которые слабо задействованы. Кроме того, задержка передачи данных может быть увеличена слишком большим потоком данных в сети или наличием большого количества ошибок при передаче данных. Задержка передачи данных может быть просчитана для каждого отдельного сетевого устройства.

Устройства, используемые в распределенных сетях

Как показано на рис. 12.2, в распределенных сетях широко используются следующие устройства:

- **маршрутизаторы (routers)** выполняют множество функций, они отвечают за межсетевое взаимодействие и содержат интерфейсные порты распределенной сети;
- **коммутаторы (switches)** используются для голосовых и видео-коммуникаций посредством распределенной сети;
- **модемами (modem)** называют как устройства для подключения к каналам голосовых служб (аналоговые модемы для удаленного доступа по телефонной сети), так и модули обслуживания канала/модули обработки данных (Channel Service Unit/Data Service Unit — CSU/DSU), позволяющие взаимодействовать с цифровыми линиями, такими, как T1/E1 либо терминальные адаптеры или сетевые терминаторы 1 типа (TA/NT1), которые используются для подсоединения к службе ISDN;

- **шлюзы (communication server)** используется для коммутации входящих и исходящих коммутируемых соединений пользователей.

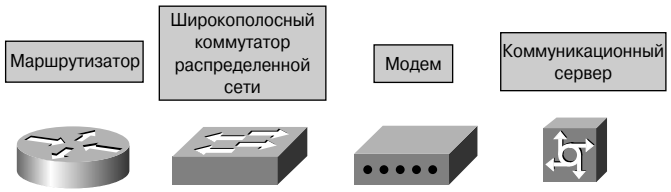


Рис. 12.2. Устройства, часто используемые в распределенных сетях

Стандарты распределенных сетей

Протоколы канального уровня описывают процесс передачи фреймов между системами в одном канале связи. Они включают в себя протоколы, разработанные для работы с выделенными двухточечными, многоточечными и разделяемыми коммутируемыми системами, такими, как, например, среда Frame Relay. WAN-стандарты определяются и управляются множеством организаций:

- **ITU-T (International Telecommunications Union — Международный телекоммуникационный союз)**, ранее называвшийся Consultative Committee for International Telephone and Telegraphy (Консультативный комитет по международной телефонной и телеграфной связи США);
- **ISO (International Organization for Standardization — Международная организация по стандартизации);**
- **IETF (Internet Engineering Task Force — Проблемная группа проектирования Internet)** — одна из групп IAB (Internet Activities Board — Координационный совет сети Internet), отвечающая за решение инженерных задач Internet. Выпускает большинство документов RFC (Requests for Comments — запросы на комментарии), используемых производителями для внедрения стандартов TCP/IP;
- **EIA (Electronics Industries Association — Ассоциация электронной промышленности)**, объединяет производителей электронного оборудования с целью разработки единых электрических и функциональных спецификаций интерфейсного оборудования;
- **IEEE (Institute of Electrical and Electronics Engineers — Институт инженеров по электротехнике и электронике) —** профессиональное объединение, выпускающее свои собственные стандарты; членами IEEE являются организации ANSI и ISO.

В синхронных последовательных линиях используются несколько типов инкапсуляции канального уровня, характеристики которых приведены в табл. 12.2.

Таблица 12.2. Инкапсуляции канального уровня синхронных последовательных линий

Инкапсуляция	Характеристики
High-level Data Link Control (HDLC — высокоуровневый протокол управления каналом)	Стандарт IEEE.
	Является стандартной инкапсуляцией, используемой для двухточечных выделенных соединений и коммутируемых соединений.
	Для связи между двумя Cisco-устройствами используется специальная *бит-ориентированная* (bit-oriented) версия протокола HDLC.
	Версия Cisco-HDLC может быть не совместима с версиями других производителей, в зависимости от выбранного производителем метода реализации.
	Обеспечивает поддержку двухточечной и многоточечной конфигураций с минимальными затратами
Frame Relay	Обеспечивает использование цифрового оборудования высокого класса.
	Позволяет использовать упрощенный алгоритм фреймирования без механизма коррекции ошибок, что означает более быструю передачу информации второму уровню по сравнению с другими протоколами распределенных сетей.
	Представляет собой промышленный стандарт коммутируемого протокола канального уровня, который управляет множеством виртуальных каналов.
	Являясь следующим поколением стандарта X.25, протокол Frame Relay обеспечивает такие возможности, которых не было в предыдущих версиях, например, коррекцию ошибок и управление потоком
Point-to-point protocol (PPP — протокол двухточечного соединения)	Описан в документе спецификации RFC 1661.
	Два стандарта этого протокола разработаны группой IETF.
	Содержит поле протокола (Protocol), которое идентифицирует используемый в соединении протокол сетевого уровня.
	Обеспечивает соединения маршрутизатор-маршрутизатор и узел-сеть через синхронные и асинхронные линии.
	Разработан для работы с несколькими протоколами сетевого уровня, такими, как Internet-протокол (Internet Protocol — IP) и протокол межсетевого пакетного обмена (Internetwork Packet Exchange — IPX).
	Содержит встроенный механизм обеспечения безопасности, как, например, протокол аутентификации с предварительным согласованием вызова (Challenge Password Authentification Protocol — CHAP)

Окончание табл. 12.2

Инкапсуляция	Характеристики
Synchronous Data Link Control (SDLC — синхронное управление каналом передачи данных)	Разработан компанией IBM. Протокол распределенных сетей канального уровня для среды System Network Architecture (SNA — системная сетевая архитектура). Впоследствии этот протокол был заменен более гибким протоколом HDLC
Serial Line Internet Protocol (SLIP — межсетевой протокол для последовательного канала)	Очень популярный протокол канального уровня распределенной сети, управляющий IP-пакетами. В большинстве приложений в настоящее время заменен более гибким протоколом PPP. Представляет собой стандартный протокол двухточечного соединения, использующий стек TCP/IP
Link Access Procedure Balanced (LAPB — сбалансированный протокол доступа к каналу связи)	Используется протоколом X.25. Имеет улучшенную защиту от ошибок
Link Access Procedure on the D channel (LAPD — протокол доступа к D-каналу)	Используется для сигнализации и установления вызова в канале ISDN
Link Access Procedure Frame (LAPF — протокол доступа к каналу связи Frame Relay)	Используется для служб, работающих в режиме передачи фреймов. Подобен протоколу LAPD с использованием Frame Relay
X.25/Link Access Procedure Balanced (LAPB)	Стандарт ITU-T, который определяет процедуру установления соединения между устройствами DTE и DCE для удаленного терминального доступа. Использует протокол LAPB в качестве механизма канального уровня. Является предшественником технологии Frame Relay

Технологии Frame Relay, HDLC, PPP, ISDN и синхронные последовательные соединения описаны подробнее во втором томе. Наиболее типичные применения различных инкапсуляций показаны на рис. 12.3.

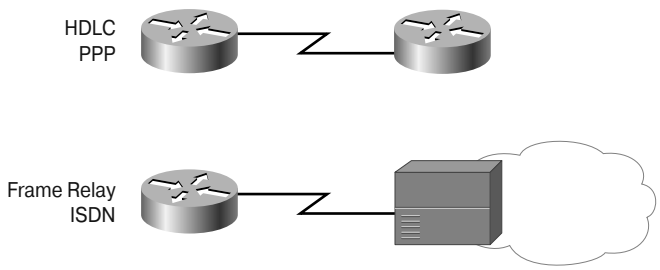


Рис. 12.3. Инкапсуляция на канальном уровне

Модель синхронной последовательной линии показана на рис. 12.4, доступ к службам телекоммуникационных линий для маршрутизатора обеспечивает модем или устройство CSU/DSU.

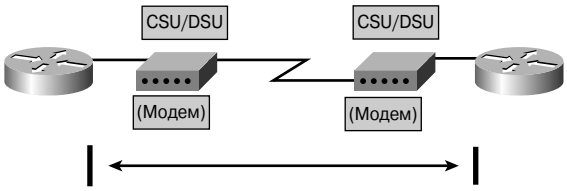


Рис. 12.4. Устройства CSU/DSU

Маршрутизаторы распределенных сетей

Так же, как для работы обычного компьютера требуется установленная на нем операционная система, так и для работы маршрутизатора необходима специальная операционная система Cisco IOS (Cisco Internetwork Operating System — межсетевая операционная система корпорации Cisco). Операционная система в маршрутизаторе используется для интерпретации конфигурационных файлов, в которых содержатся параметры и инструкции управления потоками исходящих и входящих данных. Используя специальные протоколы и таблицы маршрутизации, маршрутизаторы позволяют определить маршрут для передачи данных, по которому информация будет доставлена быстрее всего. Путь выбирается на основании действующих конфигурационных файлов и информации от протоколов маршрутизации. Файлы конфигурации содержат всю необходимую для работы устройства информацию. В маршрутизирующих устройствах корпорации Cisco, которые работают под управлением операционной системы Cisco IOS, существуют два конфигурационных файла: стартовый и рабочий, или текущий (startup-config и running-config). Оба файла подробно рассматриваются в последующих главах.

Маршрутизатор в самом простейшем приближении может рассматриваться как специализированный тип компьютера. Он содержит те же компоненты, что и обычный персональный настольный компьютер. В нем есть центральный процессор (CPU), память, системная шина и множество интерфейсов ввода/вывода. Тем не менее, любое маршрутизирующее устройство выполняет некоторые специфические функции, которые не присущи обычным настольным компьютерам. В качестве примера такой функции можно указать механизм объединения, например, двух сетей, и метод определения маршрутов для потоков данных между такими непосредственно подключенными к устройству сетями.

В нашей книге рассказывается о том, как создать из отдельных команд операционной системы Cisco IOS правильный конфигурационный файл и настроить устройство на выполнение жизненно важных сетевых функций. На первый взгляд файл конфигурации маршрутизатора может показаться исключительно сложным, тем не менее, к концу книги он будет выглядеть значительно проще и понятнее читателю, чем в самом ее начале.

К основным компонентам маршрутизатора, как показано на рис. 12.6, относятся: оперативная память (Random-Access Memory — RAM), энергонезависимая память (Non-Volatile Random-Access Memory — NVRAM), Flash-память, постоянное запоминающее устройство (Read-Only Memory — ROM) и интерфейсы.

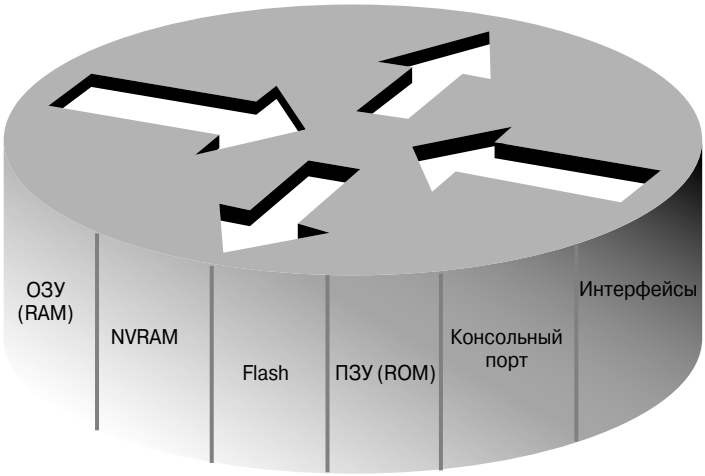


Рис. 12.5. Внутренние компоненты маршрутизатора

Маршрутизаторы в распределенных и локальных сетях

В маршрутизаторах имеются интерфейсы как для локальных, так и для распределенных сетей. Главным предназначением маршрутизаторов является объединение сетей в единую распределенную сеть посредством соединений Frame Relay или выделенных линий, например, T1. Их также можно использовать и просто для сегментации локальных сетей. Фактически для подключения других маршрутизаторов чаще всего используются интерфейсы распределенных сетей. Маршрутизаторы обмениваются информацией посредством распределенной сети. Эти устройства являются базовыми устройствами больших корпоративных сетей и сетей, которые входят в состав структуры Internet. Работают они на третьем уровне модели OSI, идентифицируя устройства по их сетевым адресам (в сети Internet — по IP-адресу). Фактически маршрутизаторы редко выступают в качестве основных устройств крупных распределенных сетей (а именно — телекоммуникационных и телефонных), чаще они используются для подключения к сети Internet в небольших инфраструктурах. В сетях среднего и крупного размера маршрутизаторы зачастую используются для разделения широковещательных доменов, маршрутизации и т.п.

Маршрутизаторы обеспечивают две основные функции:

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

Выполнение этих двух функций достигается путем создания маршрутизаторами таблиц маршрутизации и за счет обмена сетевой информацией с другими маршрутизаторами.

Администратор может изменять таблицы маршрутизации, формируя статические маршруты. Однако таблицы маршрутизации могут быть динамическими и создаваться при помощи какого-либо протокола маршрутизации в зависимости от текущей конфигурации сети на основании обмена информацией с другими маршрутизаторами.

Например, компьютеру А, который расположен в центральном офисе в штате Аризона, и его сотрудникам необходимо обмениваться информацией с компьютерами Б и В, которые размещены в Мехико и Лондоне. Компьютеры Б и В расположены на разных континентах. Соответственно, для связи с этими компьютерами потребуется маршрутизация, а также, для надежности, дополнительные резервные маршруты передачи данных. Нетрудно представить, что для связи этих компьютеров может использоваться множество маршрутов в распределенной сети.

Следует отметить, что межсетевое взаимодействие подразумевает следующие аспекты:

- непротиворечивая адресация;
- адресация отображает сетевую топологию;
- используется механизм выбора оптимального пути;
- используется динамическая или/и статическая маршрутизация;
- используется коммутация.

Дополнительная информация: роль маршрутизаторов в распределенных сетях

Очень часто в объединенных сетях используется большое количество маршрутизаторов, различных средств передачи данных и подсоединенных конечных систем. В большой распределенной сети, например, сети Internet, или даже в больших частных сетях практически невозможно обеспечить каждую машину информацией обо всех остальных компьютерах, работающих в этой сети. Поэтому для нормальной работы инфраструктуры и периферийных устройств требуется вводить некое подобие иерархии. Иерархическая организация компьютеров в объединенных сетях требует введения специализированных функций маршрутизации.

Маршрутизаторы могут выполнять функции изучения и распределения информации о маршрутизации в пределах определенного домена. Такие машрутизаторы называют *внутренними шлюзами (interior gateway)*. Соответственно, маршрутизаторы, занимающиеся сбором информации о маршрутизации в сетях, которые лежат вне локального домена (частно называемого доменом маршрутизации), называются *внешними шлюзами (exterior gateway)*.

Понятие *сетевых технологий* (networking, или объединение устройств в сеть) часто используется в широком смысле как универсальный термин, поскольку компьютеры, работающие в сети, могут быть связаны огромным количеством способов. Маршрутизаторы могут выполнять различные роли в объединенных сетях, например, использоваться как внешние, внутренние или граничные маршрутизаторы.

Как было описано выше, внутренние, внешние и граничные маршрутизаторы упоминались раньше как *внутренние шлюзы, внешние шлюзы* и *граничные шлюзы*. Термин *шлюз* (gateway) столь же стар, сколь и термин *маршрутизация* (routing). С течением времени оба понятия стали

обозначать одни и те же функции. Следовательно, оба термина правильны и могут употребляться абсолютно равноправно.

Существуют схожие понятия, упоминающиеся довольно часто, для понимания которых необходимо разобраться в тонкостях работы распределенной сети. Рассмотрим понятия *распределенная сеть*, *сеть* и *объединенная сеть*.

- **Распределенная сеть (Wide-Area Network — WAN**) — это совокупность взаимодействующих локальных сетей (LAN), связанных посредством маршрутизаторов и различных телекоммуникационных средств передачи данных, таких, как арендованные каналы или соединения Frame Relay. Неявно в этом определении подразумевается, что локальные сети в составе распределенной сети могут быть географически рассредоточены, однако управлять ими будет одна организация.
- **Сеть** — самый размытый термин, который не имеет точного определения. Обо всех видах локальных и распределенных сетей можно говорить как просто о сетях. Следовательно, понятие *сеть* (network) подразумевает некоторую объединенную совокупность сетевых устройств, поэтому сетью может быть как локальная, так и распределенная сеть, однако она должна принадлежать одной организации и иметь непротиворечивую структуру адресации. Иногда этот термин используется для обозначения международной сети или даже сети Internet.
- **Объединенная сеть (Internetwork**). Этот термин подразумевает под собой нечто большее, чем просто конкретная сеть. Объединенная сеть — это совокупность сетей, которые взаимодействуют между собой. Связанные сети могут принадлежать разным организациям. Например, две компании могут использовать сеть Internet для объединения своих распределенных сетей. Таким образом, объединенная сеть будет состоять из двух связанных между собой частных и одной открытой сетей. Самое общее определение объединенной сети — это набор сетей, связанных между собой маршрутизаторами. Такая объединенная сеть не обязательно должна быть набором связанных сетей, а может быть как одним доменом, так и единственной автономной системой (АС). Объединенная сеть может включать в себя несколько связанных автономных сетей.
- **Автономная система (Autonomous System — AS)** — это самодостаточная и независимая сеть или объединенная сеть (локальная или распределенная). Такая сеть управляется одним человеком, группой людей или организацией; в ней используется единый маршрутизируемый протокол и она имеет единую структуру адресов. Автономная система может поддерживать подключения к другим автономным системам, находящимся в собственности той же организации. Кроме того, автономные системы могут соединяться с другими сетями, такими, как сеть Internet, однако при этом не теряют автономности. Этот термин обычно используется в сочетании с протоколами маршрутизации, такими, как BGP (Border Gateway Protocol — протокол граничного шлюза), которые позволяют делить сети на связанные части. Обычно автономные системы связаны со структурами крупных поставщиков услуг или с большими сетями, например, со структурами провайдеров услуг сети Internet или с корпоративными сетями.

С учетом указанных выше терминов становится возможным определить функциональные классы маршрутизаторов. Внутренний маршрутизатор — это маршрутизатор, который может использоваться устройствами сети для обращения к устройствам в пределах этой же сети. Внутренние маршрутизаторы не поддерживают подключений к другим сетям. На рис. 12.7 показана небольшая сеть, в составе которой функционируют внутренние маршрутизаторы.

Внешние маршрутизаторы — это маршрутизаторы. которые находятся вне пределов любой сети. На рис. 12.7 показана примитивная модель сети Internet, цель которой — продемонстрировать методы размещения внешних маршрутизаторов.

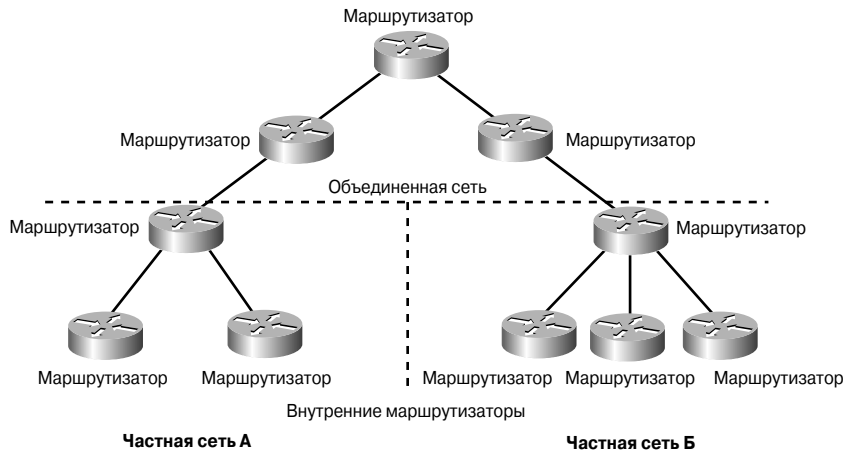


Рис. 12.6. Внутренние маршрутизаторы сети

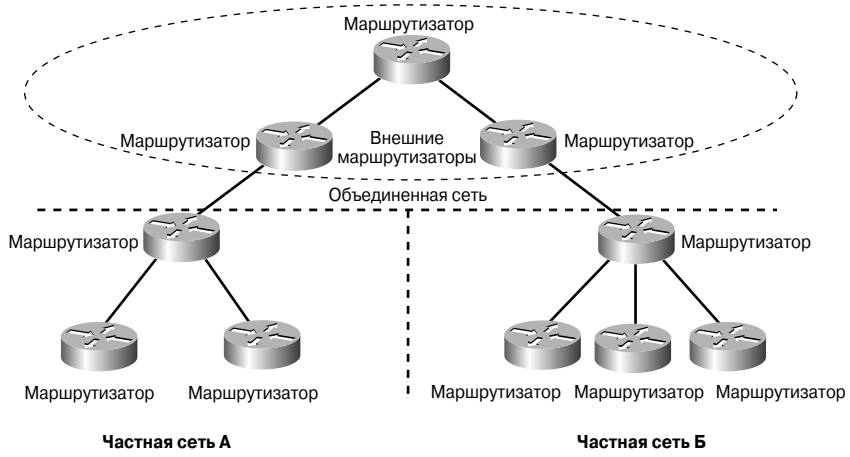


Рис. 12.7. Внешние маршрутизаторы

И последний тип маршрутизаторов — граничные маршрутизаторы. Как следует из их названия, эти маршрутизаторы предназначены для организации связи между сетями. Строго говоря, наиболее четкое определение понятия *граничный маршрутизатор* предполагает, что так называется устройство, которое подключено к маршрутизатору в другой автономной системе. В таком случае на двух маршрутизаторах будет запущен протокол BGP. Зачастую можно столкнуться с ситуацией, когда граничные маршрутизаторы называют внешними, по аналогии с протоколом BGP, под управлением которого они строят таблицы маршрутизации, поскольку такой протокол является протоколом внешней маршрутизации (т.е. маршрутизации вне автономной системы). Один граничный маршрутизатор может обрабатывать несколько автономных сетей, точно так же, как одна организация может владеть как одной, так и несколькими автономными системами. Следует помнить, что одно маршрутизирующее устройство может быть границей и между двумя автономными системами, и между частной и какой-либо другой сетью. На рис. 12.9 показан пример использования граничных маршрутизаторов, который основан на примерах сетей, проиллюстрированных на рис. 12.6 и 12.7.

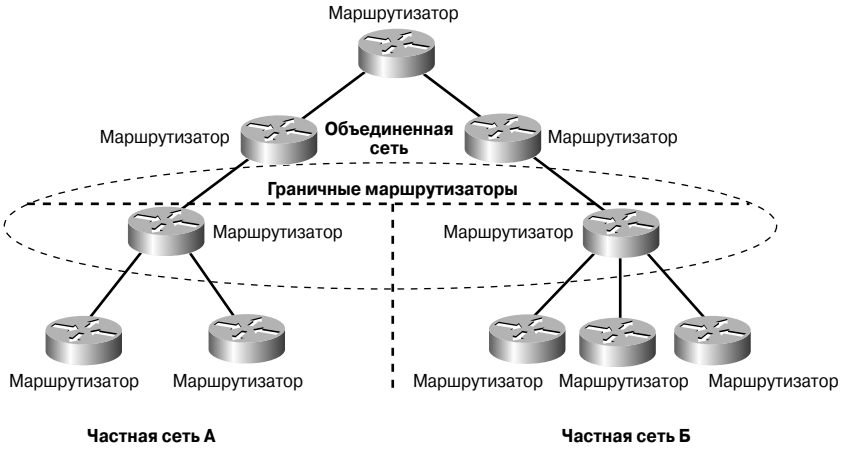


Рис. 12.8. Граничные маршрутизаторы

Соединения в распределенных сетях

Для соединения нескольких локальных сетей могут быть использованы разные типы распределенных сетей. Ниже подробно рассматриваются основные типы служб распределенных сетей:

- службы с коммутацией каналов;
- службы с коммутацией пакетов;
- службы с коммутацией ячеек;
- цифровые службы выделенных линий;
- коммутируемые, кабельные и беспроводные службы.

На рис. 12.9 проиллюстрирована схема, которая указывает различия между службами распределенных сетей.

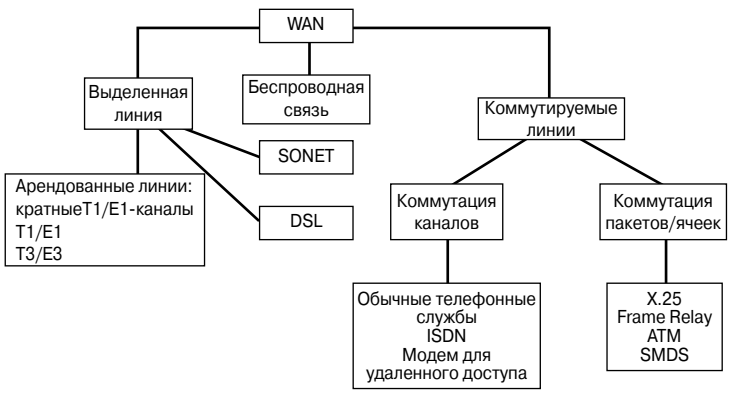


Рис. 12.9. Службы распределенных сетей

Службы с коммутацией каналов

Коммутация каналов (circuit switching) — это один из методов коммутации в распределенных сетях, в котором для установления, поддержания и завершения каждого сеанса связи предоставляется выделенный физический канал. Примером сети с коммутацией каналов является среда ISDN (Integrated Services Digital Network — цифровая сеть с комплексным обслуживанием). На рис. 12.10 показана топология сети, в которой используется коммутация каналов.

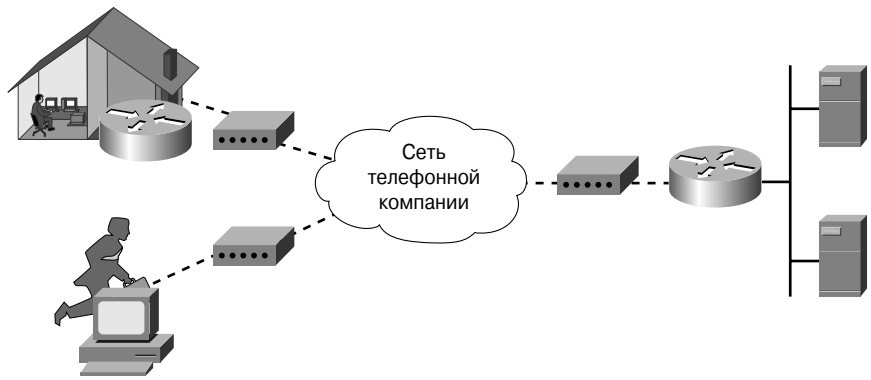


Рис. 12.10. Коммутация каналов

В табл. 12.3 приведены характеристики наиболее популярных служб с коммутацией каналов: обычные телефонные сети (Plain Old Telephone Service — POTS) и цифровые сети связи с комплексным обслуживанием (Integrated Services Digital Network — ISDN).

Таблица 12.3. Службы с коммутацией каналов

Служба с коммутируемым доступом	Характеристики
POTS	Некомпьютерная служба передачи данных, однако включает в себя множество технологий, которые являются частью инфраструктуры для передачи информации. Это очень надежная, удобная в работе распределенная система коммуникаций. Типичная для этой службы физическая среда передачи данных — медная витая пара
Узкополосная сеть ISDN	Гибкая, широко распространенная исторически важная технология. Эта сеть была первой полностью цифровой коммутируемой службой. Имеет умеренную стоимость. Максимальная пропускная способность составляет 128 Кбит/с при использовании интерфейса базового уровня (Basic Rate Interface — BRI) и достигает 3 Мбит/с при использовании интерфейса основного уровня (Primary Rate Interface — PRI). Технология является очень широко используемой службой, однако ее распространенность зависит от страны. Типичная для службы физическая среда передачи — медная витая пара

Службы POTS и ISDN являются коммутируемыми; это означает, что вызов может быть осуществлен только между двумя точками, и физическая передающая среда будет полностью задействована. И служба POTS, и ISDN используют *мультиплексную передачу с временным разделением* (Time-Division Multiplexing — TDM), которую иногда называют *синхронным режимом передачи* (Synchronous Transfer Mode — STM).

Службы с коммутацией пакетов

Службы с коммутацией пакетов (packet-switched services) используются для передачи и маршрутизации небольших блоков данных через сеть, называемых *пакетами* (packet). Пакеты передаются получателю, адрес которого содержится в заголовке пакета. На рис. 12.11 показана топология сети, в которой используется коммутация пакетов.

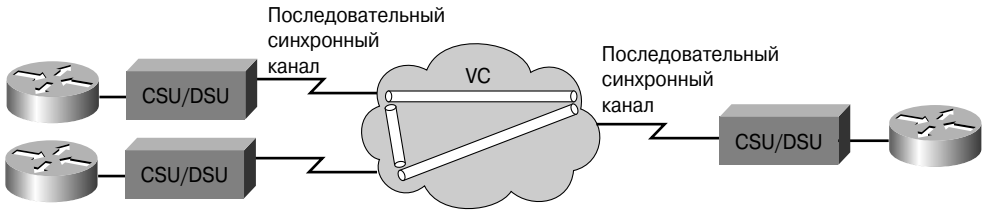


Рис. 12.11. Коммутация пакетов

В табл. 12.4 перечислены характеристики наиболее распространенных служб с коммутацией пакетов — X.25 и Frame Relay.

X.25 является надежным протоколом с установлением соединения на канальном и сетевом уровнях, и именно из-за этого он работает намного медленнее, чем протокол Frame Relay.

Технология Frame Relay и механизм пересылки фреймов обычно считается более быстродействующим механизмом, или более совершенной версией протокола X.25. Технология Frame Relay, как и ее предшественник, протокол X.25, является службой с установлением соединения.

Службы с коммутацией каналов используют мультиплексную передачу с временным разделением и, как обычно говорят, являются синхронными технологиями (используют механизм STM), тогда как службы с коммутацией пакетов используют *статистическую* мультиплексную передачу с временным разделением; их иногда называют асинхронными (подобно технологии ATM).

Службы коммутации ячеек

Службы с коммутацией ячеек (cell-switched services) обеспечивают коммутацию выделенных виртуальных каналов посредством группирования цифровых данных в некоторые блоки-ячейки и передают их по физической среде посредством цифровой технологии передачи.

В табл. 12.5 перечислены характеристики двух наиболее популярных служб коммутации ячеек — ATM (Asynchronous Transfer Mode — асинхронный режим передачи) и SMDS (Switched Multimegabit Data Service — коммутируемая многомегабитовая службы передачи данных[1]).

[1] *Высокоскоростная сетевая технология, предлагаемая телефонными компаниями США. — Прим. ред.*

Таблица 12.4. Службы с коммутацией пакетов

Служба	Характеристики
X.25	Довольно старая технология, которая, однако, довольно широко используется и по сегодняшний день. Имеет улучшенную систему проверки ошибок с тех времен, когда распределенные сети были подвержены большому количеству ошибок. Такой механизм повышает качество, однако уменьшает скорость передачи. Максимальная пропускная способность составляет 2 Мбит/с. Служба довольно широко распространена. Стоимость ее внедрения и сопровождения весьма умеренна. Типичная для службы физическая среда передачи — медная витая пара
Ретрансляция кадров (Frame Relay)	С определенной точки зрения представляет собой разновидность узкополосной службы ISDN с коммутацией пакетов. На сегодняшний день эта служба стала очень популярной технологией распределенной сети. Похожа на X.25, однако более эффективна. Максимальная пропускная способность составляет 44,736 Мбит/с. В Соединенных Штатах чрезвычайно популярны скорости передачи 56 Кбит/с и 384 Кбит/с. Служба довольно широко распространена. Стоимость ее внедрения и сопровождения весьма умеренна. Типичные для этой службы физические среды передачи — медная витая пара и оптическое волокно

Таблица 12.5. Службы сотовой коммутации

Служба	Характеристики
ATM	Тесно связана с широкополосной технологией ISDN. Является очень важной технологией распределенных сетей. Для передачи данных используются маленькие ячейки данных фиксированной длины (53 байта). Максимальная пропускная способность составляет 622 Мбит/с, хотя в настоящее время разрабатываются и более высокоскоростные варианты. Типичная для этой службы физическая среда передачи — медная витая пара и оптическое волокно. Технология широко распространена и обретает все большую популярность. Для нее характерна высокая стоимость
SMDS	Основана на службе ATM и обычно используется в региональных вычислительных сетях (сеть, промежуточная по масштабу между локальной и распределенной, MAN — Metropolitan Area Network). Максимальная пропускная способность составляет 44,736 Мбит/с. Не слишком распространена. Стоимость внедрения и сопровождения сравнительно высока. Типичные для этой службы физические среды передачи — медная витая пара и оптическое волокно

Цифровые службы выделенных линий

Выделенные цифровые службы также обеспечивают коммутацию каналов, однако при их использовании соединение никогда не разрывается.

В табл. 12.6 перечислены характеристики основных цифровых выделенных служб — T1, T3, E1, E3; *цифровых абонентских линий* (Digital Subscriber Line — xDSL); *синхронной оптической сети* (Synchronous Optical Network — SONET).

Таблица 12.6. Цифровые службы выделенных линий

Служба	Характеристики
Каналы T1, T3, E1, E3	Службы T-серии являются очень важными в технологиях распределенных сетей Соединенных Штатов и Европы. Для передачи данных в этих службах используется мультиплексная передача с разделением сигналов по времени (TDM), которая позволяет разделить данные и присвоить им канальные интервалы[2] (timeslot). Пропускная способность линий серий T и E составляет 1,544 Мбит/с для T1, 44,736 Мбит/с для линии T3, 2,048 Мбит/с для E1 и 34,368 Мбит/с — для линии E3. Эти линии могут быть использованы на других скоростях передачи, называемых кратными. Типичные для рассматриваемой службы физические среды передачи — медная витая пара и оптическое волокно. Служба очень широко распространена. Стоимость ее использования умеренна
xDSL	Новое, развивающееся семейство технологий распределенных сетей, которое предназначено преимущественно для домашнего использования. Аббревиатура xDSL подразумевает семейство DSL-технологий, включая высокоскоростную службу DSL (HDSL), технологию DSL с одной линией (SDSL), асимметричную технологию DSL (ADSL) и сверхвысокоскоростную технологию DSL (VDSL). При увеличении расстояния до телефонного оборудования компании-поставщика услуг скорость передачи данных снижается. Максимальная скорость передачи данных в 51,84 Мбит/с достижима только недалеко от офиса компании-поставщика услуг. Однако в большинстве случаев реальная скорость ниже и лежит в пределах от сотен Кбит/с до нескольких Мбит/с. Стоимость использования в настоящее время умеренная и постоянно снижается

[2] *Часть мультиплексируемого канала, выделенная для передачи информации одному подканалу; канальный интервал линий T1 и E1 обычно соответствует одному подканалу 64 Кбит/с. — Прим. ред.*

Окончание табл. 12.6

Служба	Характеристики
SONET	Семейство сверхвысокоскоростных технологий физического уровня. Разработана для передачи данных посредством оптического волокна, однако может работать и на медном кабеле. Имеет ряд скоростей передачи данных, которые обозначаются специальным образом. Позволяет осуществлять поддержку различных уровней *оптических носителей* (Optical Carrier — OC), которые поддерживают скорости передачи от 51,84 Мбит/с (OC-1) до 9 952 Мбит/с (OC-192). Использование механизма *спектрального уплотнения* (Wavelength Division Multiplexing — WDM) позволяет достичь высоких скоростей передачи данных. В случае использования технологии WDM цвета лазеров настроены на несколько различные цвета или работают с отличными длинами волн, и это позволяет передавать посредством оптического канала огромные объемы данных. Широко используется в главных магистралях сети Internet. Стоимость чрезвычайно высока. Поэтому технология и не рассматривается в качестве технологии для домашнего использования

Коммутируемые, кабельные и беспроводные службы

В табл. 12.7 приведены описания и характеристики других служб распределенных сетей, которые не вошли ни в одну из рассмотренных выше категорий: модемы для удаленного доступа по телефонной сети, кабельные модемы, а также наземные и спутниковые беспроводные службы.

На рис. 12.12 проиллюстрированы различные технологии распределенных сетей.

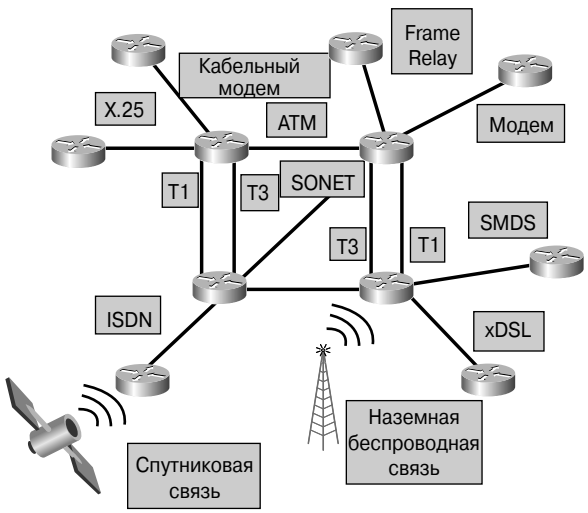


Рис. 12.12. Различные технологии распределенных сетей

Таблица 12.7. Коммутируемые, кабельные и беспроводные службы

Служба	Характеристики
Модем для удаленного доступа (аналоговый для коммутируемых служб)	Ограничен в скорости, но весьма универсален. Позволяет работать с существующими телефонными сетями без каких-либо дополнительных затрат или действий. Максимальная пропускная способность составляет приблизительно 56 Кбит/с. Дешевый в использовании. Очень распространен. В качестве физической среды передачи используется двухпроводная телефонная линия
Кабельный модем (аналоговый для разделяемых служб)	Помещает сигналы данных в один канал в виде телевизионного сигнала. Очень широко применяется в районах, где используется кабельное телевидение, транслируемое по коаксиальному кабелю. Максимальная скорость передачи данных может достигать 10 Мбит/с, однако она снижается по мере подключения пользователей к одному сегменту сети. Кабельный модем подобен некоммутируемой (разделяемой) локальной сети. Стоимость сравнительно невысока. В качестве физической среды передачи используется коаксиальный кабель
Беспроводные сети	Для работы беспроводных служб не требуется никакая передающая среда, поскольку данные переносятся посредством электромагнитных волн. Существует большое количество различных типов беспроводной связи, включая следующие: ■ **наземные,** обычно имеют скорость передачи в 11 Мбит/с (например, микроволновый канал передачи). Стоимость передачи данных относительно невысока; для связи обычно требуется прямая видимость между станциями (Line Of Sight — LOS); ■ **спутниковые** каналы передачи позволяют обслуживать мобильных пользователей, используются в сетях мобильной связи и для подключения удаленных пользователей, которые размещены слишком далеко от любых других беспроводных или кабельных сетей. Широко распространенный, но вместе с тем и дорогостоящий вид связи

Сравнение технологий распределенных сетей

В табл. 12.8 приведен сравнительный обзор всех рассмотренных выше технологий, которые используются для создания распределенных сетей.

Таблица 12.8. Сравнение технологий распределенных сетей

Аббревиатура	Название	Максимальная скорость передачи	Особенности
POTS	Обычная телефонная сеть	Аналоговая 4 кГц	Стандарт надежности
ISDN	Цифровая сеть связи с комплексным обслуживанием	128 Кбит/с	Одновременная передача данных и звука
X.25	X.25	2 Мбит/с	Старая, надежная технология
Frame Relay	Frame Relay	До 44,736 Мбит/с	Новая версия X.25
ATM	Асинхронный режим передачи	622 Мбит/с	Мощная, высокоскоростная сеть
SMDS	Коммутируемая многомегабитовая служба данных	1,544 Мбит/с и 44,736 Мбит/с	Городской вариант среды ATM
T1, T3	T1, T3	1,544 Мбит/с и 44,736 Мбит/с	Широко используемые телекоммуникации
xDSL	Цифровая абонентская линия	384 Кбит/с	Технология передачи данных посредством телефонной линии
SONET	Синхронная оптическая сеть	9 992 Мбит/с	Быстрая передача данных посредством оптического канала
Обычный аналоговый модем	Модем	56 Кбит/с	Устаревшая технология, использующая телефонные линии
Кабельный модем	Кабельный модем	10 Мбит/с	Технология, в которой используются линии кабельного телевидения
Наземная беспроводная служба	Беспроводная служба	11 Мбит/с	Соединения посредством микроволн (сверхвысоких частот — СВЧ) и лазера
Спутниковая беспроводная служба	Беспроводная служба	2 Мбит/с	Соединения посредством микроволн (СВЧ) и лазера

Стоимость распределенной сети

Одним из главных факторов, уменьшающих параметры производительности распределенной сети, является, как ни странно, ее стоимость. Затраты на обслуживание сети и выполнение работ в ней включают как стоимость начального запуска сети, так и ежемесячные расходы на ее обслуживание. Неудивительно, что большие и более мощные сетевые компоненты обходятся намного дороже меньших и менее надежных. Поэтому одной из главных целей при разработке распределенной сети является поиск оптимального баланса ее стоимости и надежности работы.

Именно в этом и заключается главная проблема сети. Ни один специалист не захочет спроектировать распределенную сеть, которой будут недовольны пользователи, однако также никто не захочет создавать слишком дорогостоящую сеть! К счастью, были разработаны некоторые принципы, которые помогут создать сеть, удовлетворяющую существующим требованиям, которую можно будет безболезненно расширить и которая к тому же будет соответствовать имеющемуся бюджету.

- Основные вложения производятся в маршрутизаторы и другое сетевое оборудование, которые являются основой сети, поэтому замена именно этого оборудования в случае необходимости будет самой дорогостоящей. В зависимости от срока амортизации, некоторое оборудование придется использовать пять и более лет. Поэтому имеет смысл приобретать маршрутизаторы с дополнительными портами, поскольку их расширение невозможно. Другие аппаратные средства (память, процессоры и интерфейсы) можно будет приобрести в будущем по мере необходимости. Такой метод позволяет создать сеть, которую легко можно будет расширить, и при этом у такой сети будет низкое *время бездействия* (downtime) после отказа.
- Средства передачи данных сравнительно несложно могут быть заменены. На них необходимо затратить какие-то средства, однако это будут небольшие вложения. Они могут заменяться так часто, как позволяет арендный договор. Таким образом, разработчик может подобрать необходимые средства передачи данных согласно имеющимся требованиям и используемым технологиям.

Степень использования ресурсов

Хорошим показателем эффективности используемой сети является степень использования ее физических ресурсов. Ее можно определить по нагрузке на такие компоненты:

- процессор и память маршрутизатора;
- физические средства передачи данных.

Степень использования физических средств маршрутизатора

Маршрутизаторы являются одним из самых главных компонентов любой распределенной сети. Любой современный маршрутизатор имеет собственный процессор и память. Эти аппаратные средства необходимы для вычисления маршрутов в распределенной сети и передачи пакетов данных, кроме того, они могут использоваться для мониторинга производительности маршрутизатора. Если степень загрузки центрального процессора маршрутизатора или его памяти достигает 100%, то процесс обработки и передачи данных замедляется. К стопроцентной загрузке ресурсов маршрутизатора могут привести различные факторы. Одним из них является увеличение потока передаваемых данных из локальной сети в распределенную. Локальная сеть может функционировать и передавать данные на скоростях до 1 Гбит/с, однако обычно используются скорости передачи данных в 10, 16 или 100 Мбит/с. В сравнении с любой из этих скоростей скорость передачи данных в распределенной сети выглядит до смешного малой — 1,544 Мбит/с. Такое несоответствие скоростей передачи данных должно быть сглажено в буферах памяти маршрутизатора. По истечении некоторого времени при передаче больших объемов данных из локальной сети в распределенную ресурсы маршрутизатора будут полностью задействованы, что приведет к замедлению его работы.

Если такие ситуации возникают достаточно редко, их можно рассматривать как отклонения от нормы. Конечно же, подобные отклонения должны быть учтены, но их наличие не должно сильно влиять на выбор модели или обновление маршрутизаторов. Если подобные отклонения

возникают часто, должны быть приняты соответствующие меры по их устранению. Обычно маршрутизатор обновляют путем закупки более мощного оборудования или же просто за счет расширения оперативной памяти имеющихся маршрутизаторов. Если в маршрутизаторе постоянно задействовано 100% оперативной памяти, то это означает, что пришло время подумать о приобретении дополнительных модулей памяти.

Решение проблемы постоянной полной загрузки центрального процессора маршрутизатора не столь однозначно, как решение проблемы нехватки памяти. Существуют всего три варианта решения проблемы высокого уровня загрузки процессора:

- по возможности — добавление другого процессора в маршрутизатор;
- замена устройства на более мощное;
- исследование потока данных, протекающего через маршрутизатор, и определение, может ли нагрузка быть оптимизирована.

Управление потоками данных является действительно жизнеспособным средством в больших распределенных сетях со сложной структурой, которое позволяет значительно уменьшить нагрузку на сетевое оборудование.

Степень использования физических средств передачи данных

Помимо маршрутизаторов и их компонентов, наблюдение может также вестись за загрузкой физических средств передачи данных. Обычно степень загруженности определяется в процентах от максимальной пропускной способности компонента передачи данных. В случае использования, например, службы T1, уровень загруженности может составлять около 30% от максимальной пропускной способности в 1,544 Мбит/с.

Указанные выше нормы могут ввести в заблуждение. Например, некоторые программы управления сетью могут обновлять статистические данные один раз в час, 5 минут или в любой другой конечный промежуток времени. Если установлен слишком большой промежуток между выборками, то подобные программы могут пропустить некоторые пиковые нагрузки на сеть. Если же выборка будет происходить слишком часто, администратору будет сложно разобраться в огромном массиве данных. Основной задачей менеджера по управлению сетью является поиск минимального промежутка времени между выборками.

Кроме выбора частоты дискретизации, определенную проблему составляет выбор оптимального размера времени выборки. Оно должно быть определено в соответствии с требованиями и режимом работы пользователей. Если оценка загруженности сети производится 24 часа в сутки и 7 дней в неделю, а пользователи активно используют сеть лишь только 10 часов в сутки и 5 дней в неделю, то очевидно, что такая оценка будет не слишком точной.

Для контроля и определения состояния средств передачи существует замечательный статистический показатель — *коэффициент использования* (utilization rate). Этот показатель не является единственным. Сеть реализована хорошо только в том случае, если она полностью отвечает нуждам пользователей, поэтому при оценке сети следует учитывать не только статистические данные, но также и другие показатели.

Роль маршрутизаторов в распределенных сетях

Обычно говорят, что распределенные сети работают на первом и втором уровнях эталонной модели OSI. Однако это не означает, что в сети WAN верхние уровни отсутствуют напрочь. Сети WAN и LAN по своим характеристикам имеют наибольшие отличия именно на первых двух уровнях эталонной модели взаимодействия открытых систем: физическом и канальном. Иными словами, стандарты и протоколы, которые используются на первом и втором уровнях в сетях WAN, существенно отличаются от технологий локальных сетей (LAN) на тех же уровнях.

Физический уровень распределенной сети описывает интерфейсы между *терминальным оборудованием* (Data Terminal Equipment — DTE) и *конечным оборудованием линии передачи данных* (Data Circuit-terminating Equipment — DCE). Как правило, оборудование линии передачи данных (DCE) обеспечивает синхронизацию и коммутацию в пределах сети, а терминальное оборудование (DTE) присоединено к устройствам пользователей. При использовании такой модели службы, доступные DTE-устройствам, становятся доступными через модем или устройство CSU/DSU, как показано на рис. 12.13.

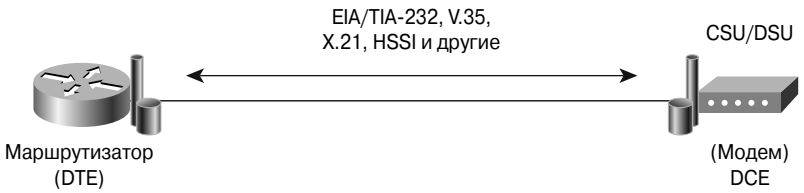


Рис. 12.13. Физическая структура служб сети WAN

Для того чтобы убедиться, что используется корректный протокол, администратору необходимо соответствующим образом настроить инкапсуляцию второго уровня в маршрутизаторе. Выбор протокола зависит от технологии построения распределенной сети и оборудования, используемого для связи.

Стандарты физического уровня распределенной сети описывают электрическое, механическое, операционное и функциональное соединения для служб сети WAN. Такие службы обычно предоставляются владельцами распределенных сетей, такими, как местные операторы связи (в США их называют Regional Bell Operating Company — RBOC, региональная телефонная компания) или национальные операторы связи (в США их называют агентствами PTT, Postal Telegraph and Telephone — почтово-телеграфная и телефонная связь).

В настоящее время широко используются следующие стандарты физического уровня:

- **EIA/TIA-232** — общий стандарт интерфейса физического уровня, который поддерживает несбалансированные схемы взаимодействия на скорости передачи данных до 64 Кбит/с. Этот стандарт наиболее близок к спецификации V.24;
- **EIA/TIA-449** — это версия стандарта EIA/TIA-232 с большей скоростью передачи, которая способна работать с более длинными кабельными системами;
- **V.24** — интерфейс физического уровня между устройствами DTE и DCE. Строго говоря, интерфейс V.24 — это практически то же, что и стандарт EIA/TIA-232;
- **V.35** — синхронный протокол физического уровня для связи между сетевыми устройствами и частями сети. Протокол V.35 чаще всего используется в Соединенных Штатах и Европе. Его рекомендованная скорость составляет до 48 Кбит/с;

- **X.21** — протокол для последовательного соединения цифровых линий. Протокол X.21 используется преимущественно в Европе в и Японии;
- **G.703** — спецификации Союза ITU-E электрического и механического соединения между оборудованием телефонной компании и устройством DTE при помощи BNC-соединителей, которые поддерживают работу каналов на скорости вплоть до E1 (Европейский стандарт цифровой передачи данных с полосой пропускания 2,048 Мбит/с);
- **EIA-530** представляет собой ссылку на две электротехнические реализации стандарта EIA/TIA-449: интерфейс RS-422 (для сбалансированной передачи) и интерфейс RS-423 (для несбалансированной передачи данных).

Моделирование распределенной сети в лабораторных условиях

Распределенная сеть может объединять маршрутизаторы из различных частей мира. В академических лабораториях все сети связаны при помощи последовательного или Ethernet-кабеля, и студенты могут видеть и напрямую подключать все сетевое оборудование. В реальной жизни один маршрутизатор может находиться в Нью-Йорке, а другой — в Сиднее. И администратор, который находится в Сиднее, вынужден работать с нью-йоркским маршрутизатором по распределенной сети.

В академической лаборатории распределенная сеть моделируется небольшим участком между конечными разъемами кабелей DTE-DCE. Соединение между интерфейсом `s0/0` одного маршрутизатора и интерфейсом `s0/1` другого маршрутизатора в некотором роде эмулирует распределенную сеть[3].

Следует отметить, что в этом случае должна быть правильно настроена синхронизация, в противном случае описанные методы не будут работать.

Дополнительная информация: сценарии объединения сетей

Исследовав основные понятия о маршрутизации и организации объединенных сетей, можно рассмотреть три основных варианта объединения сетей. В каждом из вариантов имеются свои сложности при разработке схемы адресации в любой сети или объединенной сети, которые связаны:

- с маршрутизацией в пределах сети;
- с маршрутизацией между смежными сетями;
- с маршрутизацией между удаленными сетями.

Эти три варианта сетевой маршрутизации фактически охватывают все возможные варианты, с которыми специалист может столкнуться в своей профессиональной деятельности. Для каждого варианта маршрутизации сетевому администратору следует учитывать различные аспекты, включая вычисление пути, конвергенцию и обеспечение безопасности работы. Ниже приведены краткие обзоры всех вариантов сетевой маршрутизации и даны рекомендации по их применению в конкретных ситуациях.

[3] *Такое подключение называется* лабораторным (back-to-back). — *Прим. ред.*

Маршрутизация в пределах сети

Самая простая форма маршрутизации подразумевает маршрутизацию в пределах одной сети. В такой сети имеются только внутренние маршрутизаторы. Теоретически в такой сети должны использоваться один протокол маршрутизации, единая структура адресации и небольшое количество получателей. Такая структура существенно уменьшает нагрузку на все маршрутизаторы и максимизирует потенциальную производительность сети, поэтому в случае реализации отдельной сети основное влияние на качество маршрутизации оказывает размер сети и ее топология и гораздо меньшее — структура адресации и протоколы маршрутизации. К выбору топологии сети нужно подходить с осторожностью, так, чтобы она соответствовала требованиям пользователей.

Если сеть невелика, администратору проще будет задать все маршруты статически, чем настраивать сложный протокол динамической маршрутизации. Однако при расширении сети статическая маршрутизация может доставить определенные хлопоты. Каждый раз при добавлении новых сетевых устройств администратору придется на каждом маршрутизаторе обновлять таблицы маршрутизации.

Маршрутизация между смежными сетями

Немного сложнее осуществляется маршрутизация между смежными сетями. Физическая смежность сетей означает, что эти сети непосредственно связаны друг с другом. Сети могли быть разъединены для улучшения конвергенции протоколов маршрутизации, повышения уровня безопасности или по каким-либо другим причинам.

Логическое разделение сетей подразумевает, что граничные маршрутизаторы должны собирать и распределять между этими сетями информацию о маршрутизации. Вследствие такой ситуации сетевые устройства одной сети могут непосредственно обращаться к сетевым устройствам другой сети.

Если же необходимо обеспечить доступ из локальной в распределенную сеть, то в таком случае в маршрутизации имеются отличия. Должны быть заранее определены некоторые принципиальные аспекты:

- принадлежат ли сети одной организации? Если нет, то для обеспечения безопасности внутренней сети должны использоваться граничные маршрутизаторы;
- используется ли в сетях один протокол маршрутизации? Если нет, то должен быть использован какой-либо компромиссный вариант;
- используется ли в сетях один маршрутизируемый протокол? Если нет, то вполне возможно, что администраторам и пользователям придется мириться с задержками в сети.

Кроме всего прочего, на маршрутизацию между смежными сетями может повлиять их топология. Использование одной точки взаимосвязи, например, упрощает процесс вычисления маршрутов и обмен информацией между сетями. Однако в случае неполадок в такой точке будет полностью блокирована связь между сетями, что неприемлемо для пользователей. Добавление второй точки связи (или нескольких) поможет решить эту проблему, однако в таком случае возникает риск образования циклических маршрутов и зацикливания потоков данных. Эта проблема должна учитываться администраторами сети и, рассмотрев все “за” и “против”, администратор должен принимать решение об использовании конкретного метода связи.

Маршрутизация между удаленными (несмежными) сетями

Маршрутизация между удаленными сетями является одновременно самым сложным и самым полезным типом маршрутизации. Для объединения двух сетей в качестве посредника может использоваться третья сеть. Вполне вероятно, что в трех различных сетях будут использоваться различные протоколы маршрутизации, различные маршрутизируемые протоколы и различные структуры адресации. Поэтому основной задачей граничного маршрутизатора является согласование таких сетей, а также обеспечение безопасности.

Граничные маршрутизаторы каждой сети должны защищать свои сети от несанкционированного доступа. Поскольку маршрутизируемые сети не являются смежными, и сеть-посредник лежит вне зоны их контроля, то возможность несанкционированного доступа значительно повышается.

Поэтому при настройке маршрутизаторов администратор должен разработать набор критериев, согласно которым доступ к сети могут получить только пользователи второй маршрутизируемой сети, а все попытки доступа из сети-посредника должны быть немедленно отвергнуты. Такая настройка маршрутизаторов возможна благодаря использованию так называемых *списков управления доступом* (Access Control List — ACL).

Вторая наиболее важная задача пограничного маршрутизатора заключается в суммировании внутренних маршрутов и передаче этой информации внешним сетям. Такой механизм дает возможность пользователям из внешних сетей обращаться к сетевым устройствам внутренних сетей. Если маршрутная информация не будет передана внешним маршрутизаторам, то ни одна внешняя система не сможет обратиться к сетевым устройствам, находящимся во внутренней сети.

И в заключение следует заметить, что велика вероятность того, что граничные маршрутизаторы должны быть сконфигурированы для использования нескольких протоколов маршрутизации. Протокол внутреннего шлюза, вероятнее всего, будет использован для маршрутизации во внутренней сети. Для маршрутизации в распределенной сети, скорее всего, будет использоваться более мощный и сложный протокол маршрутизации с возможностью суммирования маршрутов. Суммирование маршрутов позволяет уменьшить размер таблиц маршрутизации, объединяя маршруты к нескольким сетям в одно или два правила маршрутизации.

Маршрутизаторы

Сетевой администратор должен знать физические компоненты маршрутизатора и представлять себе их принцип работы. Такие знания понадобятся администратору как в процессе конфигурирования устройств, так и при поиске и устранении неисправностей, а также для поддержки маршрутизируемых сетей. Ниже подробно описаны внутренние и внешние физические компоненты маршрутизатора, а также методы организации физического подключения между портами устройств.

Внутренние компоненты маршрутизаторов

В табл. 12.9 перечислены основные внутренние компоненты маршрутизатора.

Таблица 12.9. Основные компоненты маршрутизатора

Компонент	Функции
Оперативная память (RAM/DRAM)	Используется для хранения таблиц маршрутизации.
	Хранит кэш протокола ARP.
	Содержит быстродействующий кэш.
	Отвечает за буферизацию пакетов (разделяемая оперативная память).
	Обеспечивает хранение пакетов.
	Обеспечивает временную и рабочую память для файлов конфигурации маршрутизатора при включенном питании.
	Содержимое RAM-памяти теряется после выключения питания или перезагрузки устройства

Окончание табл. 12.9

Компонент	Функции
Энергонезависимая память (NVRAM)	Содержит резервную, или стартовую, копию файла конфигурации.
	При перезагрузке или после выключения данные в этой памяти не стираются
Flash-память	Стираемая, перепрограммируемая память, которая обычно работает только в режиме чтения (EPROM).
	Содержит образ операционной системы и микрокод.
	Позволяет обновлять программное обеспечение без извлечения и перемещения чипа на процессоре.
	Содержит данные, которые при перезагрузке или завершении работы маршрутизатора не уничтожаются.
	Несколько версий операционной системы Cisco IOS могут быть сохранены во Flash-памяти
Постоянное запоминающее устройство (ROM)	Содержит код команд самотестирования при включении питания (Power-On Self Test — POST).
	Содержит программы начальной загрузки и основное программное обеспечение операционной системы.
	Для обновления программного обеспечения в ПЗУ требуется замена подключаемого чипа на системной плате устройства
Интерфейс	Сетевое соединение, через которое пакеты данных передаются из маршрутизатора и поступают в устройство.
	Размещается на системной плате или в отдельном модуле интерфейса

Интерактивная презентация: внутренние компоненты маршрутизатора
Эта презентация поможет идентифицировать и запомнить основные физические компоненты маршрутизатора.

Дополнительная информация: подробнее о маршрутизаторах

Маршрутизаторы предназначены для обеспечения связи между большим количеством сетей. Такая связь дает возможность компьютерам из разных сетей обмениваться между собой информацией. Связанные сети могут принадлежать одной компании или же быть географически рассредоточены и принадлежать кому угодно. Обычно сети, разделенные большими расстояниями, связываются посредством распределенных сетей. Распределенные сети основаны на большом количестве различных технологий, включая маршрутизаторы, средства передачи и различные типы линий. Маршрутизаторы создавались только для одной цели — для объединения разделенных сетей в единую глобальную сеть.

Маршрутизатор является интеллектуальным устройством, которое работает преимущественно на первых трех уровнях эталонной модели OSI. Однако, подобно любому другому узлу сети, маршрутизатор способен к взаимодействию на любом из семи уровней модели OSI. Необходимость использования первых трех уровней существует практически всегда. Для связи с локальной сетью маршрутизатор использует первые два уровня эталонной модели (конструкции канального уровня). Наиболее важной функцией является способность маршрутизаторов

идентифицировать сетевые маршруты на основе адресов третьего уровня. Этот механизм позволяет маршрутизаторам взаимодействовать с множественными сетями, используя адресацию сетевого уровня вне зависимости от месторасположения и технологии работы сетей.

Для того чтобы понять принципы маршрутизации и разобраться в работе маршрутизаторов, необходимо понимать два аспекта их работы: физический и логический. С физической точки зрения маршрутизатор состоит из огромного количества компонентов, каждый из которых выполняет строго заданную функцию. С логической точки зрения маршрутизатор выполняет определенные действия, включая обнаружение других маршрутизаторов, получение информации о потенциально достижимых сетях и узлах, определение и отслеживание потенциальных маршрутов и передачу дейтаграмм получателям. Это позволяет формировать и использовать международные сети, включая распределенные.

Физические компоненты маршрутизатора

Маршрутизаторы — это чрезвычайно сложные устройства. Сложность их структуры заключается в определенной логике механизма маршрутизации, который дает возможность физическому устройству выполнять функции маршрутизации. Сложность маршрутизации частично скрадывается простой физической формой маршрутизатора. В общем случае маршрутизатор является обыкновенным специализированным компьютером и, соответственно, состоит из схожих компонентов:

- центрального процессора (Central Processing Unit — CPU);
- оперативной памяти (Random-Access Memory — RAM);
- базовой системы ввода-вывода (Basic Input/Output System — BIOS);
- операционной системы (ОС);
- системной платы;
- портов ввода-вывода;
- источника питания, каркаса, металлического кожуха.

Большая часть компонентов маршрутизатора закрыта кожухом и недоступна для системных администраторов. Эти компоненты чрезвычайно надежны и в нормальных условиях не должны выйти из строя. Исключением из правила является установка дополнительных модулей в маршрутизатор. В любое время можно добавить дополнительные ресурсы маршрутизатору, однако при этом придется снимать внешний кожух. Чаще всего специалисту приходится устанавливать дополнительные порты ввода-вывода или дополнительную память.

При работе с маршрутизаторами системный администратор наиболее часто будет иметь дело с его операционной системой — программным обеспечением, которое обеспечивает совместную работу аппаратных компонентов (в случае использования маршутизаторов корпорации Cisco, несомненно, это будет операционная система Internetwork Operation System, сокращенно IOS), и портами ввода-вывода. Для изменения и создания конфигурации маршрутизатора системные администраторы обычно используют интерфейс командной строки. Конфигурация системы определяет число, месторасположение, типы портов ввода-вывода, параметры адресации и формацию о пропускной способности интерфейсов и устройства. Кроме того, конфигурация маршрутизатора может включать информацию о правах и типе доступа пользователей к отдельным портам ввода-вывода.

Порты ввода-вывода маршрутизатора — это единственный физический компонент, который может увидеть администратор. Порты предоставляют уникальную возможность создания, по-видимому, бесконечного количества комбинаций локальных и распределенных сетей, реализованных на основе разных технологий передачи данных. Каждый из портов в локальной или распределенной сети должен иметь собственный порт ввода-вывода на маршрутизаторе. Эти порты выполняют функции, подобные функциям сетевых интерфейсных плат (NIC) в компьютере, подключенном к сети; они связаны с механизмами фреймирования и обеспечивают поддержку соответствующих интерфейсов. Многие физические интерфейсы внешне кажутся одинаковыми. Однако на более высоком уровне они совершенно различны. Поэтому перед использованием тех или иных интерфейсов полезно изучить соответствующие технологии передачи.

Функции маршрутизатора

Логические функции маршрутизатора так же важны, как и обеспечение физической взаимосвязи множества сетей. Например, для объединенной сети требуется, чтобы между отправителем и получателем имелся хотя бы один физический канал передачи данных. Однако существование и использование физического канала — это две разные вещи. Естественно, что для нормальной работы отправитель и получатель должны "разговаривать" на одном языке (*использовать единый протокол маршрутизации*). Кроме того, такой язык (протокол маршрутизации) дает возможность путем общения с промежуточными маршрутизаторами находить кратчайший маршрут для передачи данных.

Таким образом, маршрутизатор должен обеспечивать следующие функции:

- физическое взаимодействие;
- логическое взаимодействие;
- безопасность;
- определять маршрут передачи данных.

Физическое взаимодействие

Маршрутизатор имеет как минимум два (обычно намного больше) физических порта ввода-вывода. Порты ввода-вывода или, как их часто называют, *интерфейсы* используются для физического присоединения передающей среды к маршрутизатору. Каждый порт подсоединен к плате расширения, которая в свою очередь подключается к системной плате маршрутизатора. Таким образом, системная плата маршрутизатора обеспечивает взаимодействие нескольких сетей.

Системный администратор должен настроить каждый интерфейс маршрутизатора посредством консоли. Конфигурация включает в себя определение номеров портов в маршрутизаторе, указание технологии передачи данных и доступной полосы пропускания для сетей, подключенных к интерфейсу, указание типов протоколов, которые будут использоваться с этим интерфейсом. Параметры конкретного порта должны зависеть от типа сетевого интерфейса.

Следует отметить, что в платформах верхнего уровня (7500 и 12000) интерфейсы (VIP2 или линейная плата) способны передавать пакеты без прерывания работы основного процессора.

Логическое взаимодействие

После настройки маршрутизатора его необходимо активизировать. Конфигурация интерфейсов определяет тип среды передачи данных, IP-адреса интерфейсов и адрес или адреса сети, которая подсоединена к интерфейсу. После активизации порта маршрутизатор немедленно начинает контролировать все пакеты, которые передаются в сеть, подключенную к этому порту. Мониторинг пакетов позволяет получить данные об IP-адресах узлов, расположенных в заданной сети, доступ к которым может быть получен через сконфигурированный порт. Все адреса сохраняются в специальных таблицах, которые называются *таблицами маршрутизации* (routing table). Таблицы маршрутизации сопоставляют номер порта каждого интерфейса маршрутизатора с адресами сетевого уровня, которые могут быть доступны посредством этого порта (в прямом и обратном направлениях).

Кроме всего прочего, в маршрутизаторе может быть также указан *стандартный маршрут* (default route). Этот маршрут связывает интерфейс маршрутизатора со всеми неизвестными адресами получателей. Такая связь позволяет маршрутизатору перенаправлять дейтаграммы получателям, IP-адрес которых ему не известен. Стандартные маршруты служат и для других целей. Они могут быть использованы, например, для уменьшения таблиц маршрутизации или потока данных при обмене информацией о маршрутизации между маршрутизаторами.

К конфигурированию стандартного маршрута следует подходить с осторожностью, поскольку его неправильное указание может вызвать проблемы в работе сети.

Обнаружение маршрута для передачи данных

Маршрутизаторы взаимодействуют друг с другом, используя специальный протокол, называемый *протоколом маршрутизации* (routing protocol). Использование протокола маршрутизации дает возможность маршрутизаторам выполнять следующие функции:

- находить потенциальные маршруты для определения сетей получателя;
- вычислять маршрут с помощью математических средств, основываясь на алгоритмах протокола маршрутизации, для определения наилучшего пути к каждому получателю;
- производить непрерывный мониторинг сети для определения любых изменений топологии, которые могут привести к ошибкам маршрутизации.

Существует большое количество различных протоколов маршрутизации. Некоторые, такие, как протокол RIP (Routing Information Protocol — протокол маршрутной информации), довольно просты. Другие, такие, как OSPF (Open Shortest Path First — первоочередное открытие кратчайших маршрутов), очень мощные, предоставляют много удобных функций, однако довольно сложны. В общем случае протокол маршрутизации для решения своей непосредственной задачи — маршрутизации — может использовать два подхода: маршрутизацию по вектору расстояния и по состоянию каналов. Протокол маршрутизации, использующий векторы расстояния, определяет маршрут на основании расстояния между отправителем и получателем.

Протокол, в котором используется механизм обнаружения состояния канала, определяет маршрут на основании различных состояний связей или механизмов, которые соединяют отправителя и получателя. Оба метода дают одинаковые результаты, хотя и достигаются они различными путями. Каждому методу также присуща различная производительность и разное время конвергенции.

Протоколы маршрутизации могут быть оценены по многим критериям. Наиболее значимые из них:

- **оптимальность** — этот критерий служит для оценки способности протокола маршрутизации выбрать наилучший из доступных маршрутов от отправителя к получателю. К сожалению, слово *наилучший* не всегда столь однозначно. Может существовать множество различных маршрутов в сети. И каждый из таких путей, в зависимости от остальных критериев оценки, может стать *наилучшим*. Критерии, используемые для оценки протоколов маршрутизации, называются *метрикой маршрутизации* (routing metric). Существует большое количество метрик маршрутизации, и они широко используются для оценки протоколов маршрутизации. Самой простой метрикой является *количество транзитных переходов* (hop count); она определяет количество переходов через промежуточные машрутизаторы между отправителем и получателем;
- **эффективность** является другим критерием оценки протоколов маршрутизации. Эффективность маршрутизатора может быть оценена по степени использования его ресурсов, включая оперативную память, процессор и пропускную способность, которая необходима для конкретного протокола. При приобретении маршрутизатора стоит посоветоваться с продавцом и выбрать наиболее подходящую для используемых протоколов модель;
- **отказоустойчивость**. Протокол маршрутизации должен выполнять свои функции вне зависимости от стабильности работы сети. Ошибки в работе сети включают в себя отказы аппаратных средств и средств передачи, ошибки конфигурации маршрутизатора, кроме того, чрезмерные нагрузки неблагоприятно сказываются на стабильности работы сети. Поэтому возможность функционирования протокола маршрутизации в неблагоприятных условиях является его важной характеристикой;
- **конвергенция**. Маршрутизаторы — это интеллектуальные устройства. и поэтому они могут автоматически определять изменения в распределенной сети. Когда изменяется топология сети, все маршрутизаторы должны согласованно изменить конфигурацию и заново вычислить все маршруты. Такой процесс называют *конвергенцией* (convergence). Для обнаружения и передачи другим маршрутизаторам информации об изменениях в сети в каждом протоколе маршрутизации используются индивидуальные механизмы. Поэтому каждому протоколу маршрутизации присуще свое время конвергенции. В общем случае, чем медленнее

происходит конвергенция протокола, тем больше вероятность неполадок при передаче данных в распределенной сети;

- **масштабируемость** — это возможность дальнейшего расширения сети. И хотя расширение сети потребуется далеко не в каждой организации, протокол маршрутизации должен обладать возможностью масштабируемости в случае, если расширение сети все-таки понадобится.

Компоненты маршрутизатора

Чтобы уметь правильно настраивать маршрутизатор и знать, как его использовать, необязательно знать местоположение различных компонентов маршрутизатора на его материнской плате и внутри корпуса. Тем не менее, в некоторых ситуациях, например, когда необходимо расширить объем оперативной памяти, такие знания могут значительно облегчить работу сетевого или системного администратора.

Местоположение и тип используемых компонентов устройства могут отличаться в разных моделях маршрутизаторов. На рис. 12.14 показано внутреннее устройство маршрутизатора серии 2600.

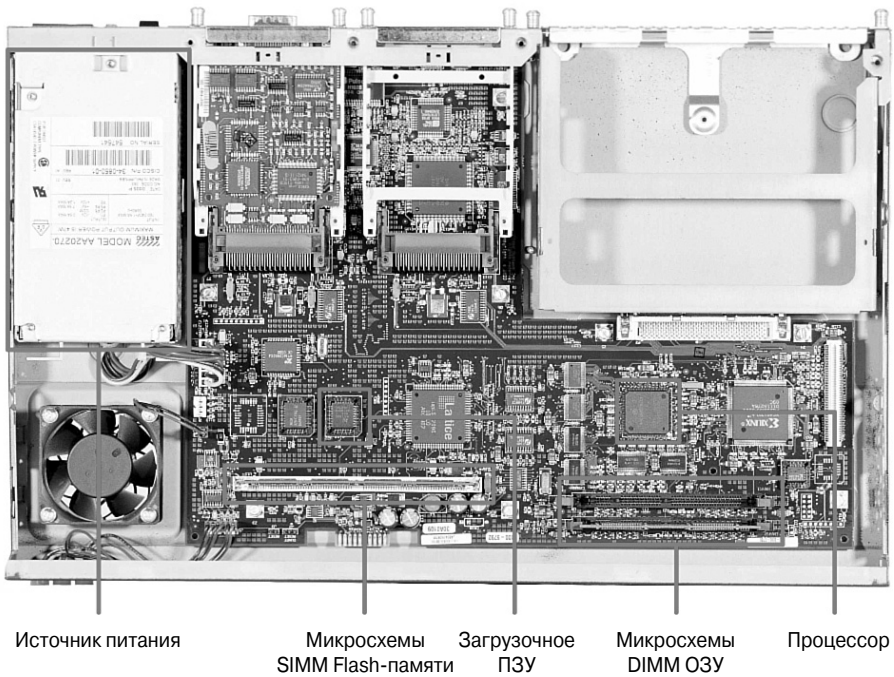


Рис. 12.14. Внутреннее устройство маршрутизатора серии 2600

На рис. 12.15 показаны внешние компоненты маршрутизатора серии 2600: внешние порты, которые используются для подключения линий.

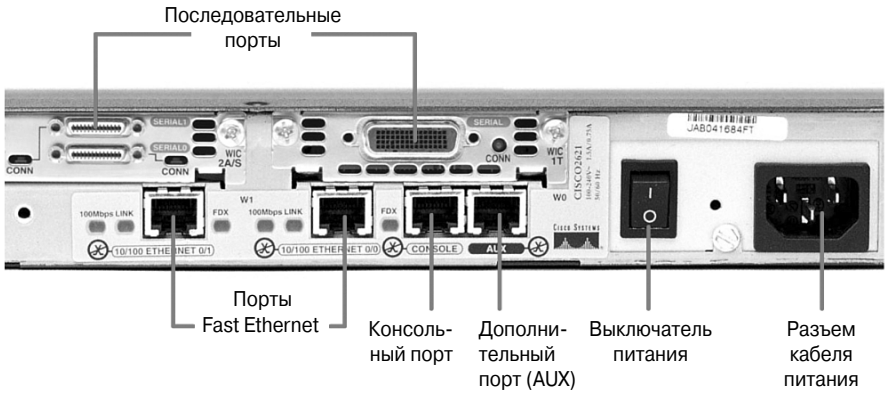


Рис. 12.15. Внешние порты маршрутизатора серии 2600

Презентация: маршрутизатор Cisco 1721
В этой презентации показан маршрутизатор модели 1721.

Презентация: маршрутизатор Cisco 2621
В этой презентации показан маршрутизатор модели 2621.

Внешние разъемы маршрутизаторов

Существуют три типа разъемов в маршрутизаторах: интерфейсы локальных сетей, интерфейсы распределенных сетей и порты управления. Все перечисленные интерфейсы показаны на рис. 12.16. Интерфейсы локальных сетей позволяют маршрутизатору соединяться со средой локальной сети, обычно в таких случаях используется одна из форм среды Ethernet, однако это не означает, что технологии Token Ring и ATM или любая другая не могут использоваться.

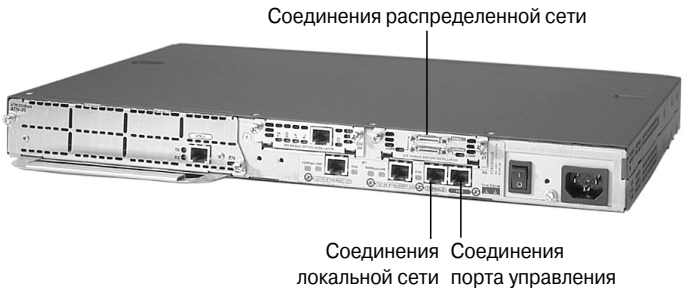


Рис. 12.16. Внешние разъемы маршрутизаторов

Интерфейсы распределенных сетей (WAN) обеспечивают подключение к удаленным узлам или к сети Internet через сеть провайдера. В качестве портов распределенной сети могут выступать как простые последовательные соединения, так и любой

другой тип интерфейса из множества существующих технологий распределенных сетей. При использовании некоторых типов интерфейсов распределенных сетей внешние устройства, такие, как CSU/DSU, необходимы для подключения маршрутизатора к местной службе провайдера услуг. Некоторые разновидности соединений распределенных сетей позволяют подключить маршрутизатор непосредственно к оборудованию поставщика услуг.

Функции портов управления отличаются от функций других интерфейсов. Интерфейсы локальных и распределенных сетей обеспечивают сетевое взаимодействие, посредством которого передаются пакеты данных. Порт управления обеспечивает соединение, передающее текстовую информацию, которая используется для конфигурирования и исправления ошибок в работе устройства. Наиболее часто используемые интерфейсы управления — это консоль и вспомогательные порты. Они представляют собой последовательные асинхронные порты EIA-232, которые подсоединяются к коммуникационным портам персонального компьютера. На компьютере должна быть запущена программа эмуляции терминала, которая должна обеспечивать сеанс обмена текстовой информацией с маршрутизатором. Такой сеанс дает возможность системному администратору управлять устройством.

Соединения портов управления устройством

Управляющими портами в маршрутизаторе являются порт консоли и вспомогательный порт (AUX). Эти асинхронные последовательные порты не предназначены для использования в качестве сетевых. Для начальной конфигурации маршрутизатора требуется использовать один из этих двух портов. Специалисты корпорации Cisco рекомендуют использовать для этого порт консоли; следует отметить, что не во всех маршрутизаторах есть вспомогательный порт.

При первом включении маршрутизатора в нем не настроены никакие сетевые параметры. Таким образом, устройство не способно взаимодействовать ни с какими сетями. Для подготовки маршрутизатора к запуску и настройке следует подсоединить ASCII-терминал к порту RS-232[4] или же компьютер, эмулирующий ASCII-терминал, к системному порту консоли. Таким образом администратор сможет передавать команды конфигурации маршрутизатору.

После того как маршрутизатор будет настроен, его можно подключать к сети для устранения неполадок или мониторинга.

Кроме того, маршрутизатор может быть настроен таким образом, что появится возможность удаленно управлять устройством, если подсоединить модем к порту консоли или AUX-порту.

Для поиска и устранения неисправностей предпочтительнее использовать порт консоли, чем AUX-порт, поскольку порт консоли стандартно настроен на отображение параметров запуска маршрутизатора, его отладки и сообщений об ошибках. Если сетевые службы по какой-либо причине не запустились или в их работе произошла ошибка, то для устранения проблем можно использовать порт консоли.

[4] *Теперь этот стандарт называется EIA-232 или TIA/EIA-232. — Прим. ред.*

Кроме того, порт консоли может быть использован для выполнения процедуры восстановления паролей. Дополнительный порт (AUX) может быть использован для подключения модема, который соединен с коммутируемой телефонной линией: администратор может удаленно соединиться с устройством через телефонную сеть для устранения каких-либо неполадок.

Подключение через консольный порт

Консольный порт, который показан на рис. 12.17, является портом управления устройством, который используется для так называемого "внеполосного" управления (out-of-band management). Внеполосный доступ представляет собой некоторое средство подключения к устройству, которое зарезервировано исключительно для управленческих целей. Он позволяет сетевому администратору подключиться к маршрутизатору независимо от того, в каком состоянии находятся его интерфейсы, работают или нет подключенные к нему сети. Консольное соединение используется для начальной конфигурации маршрутизатора, мониторинга устройства и восстановления после сбоев или утери паролей.

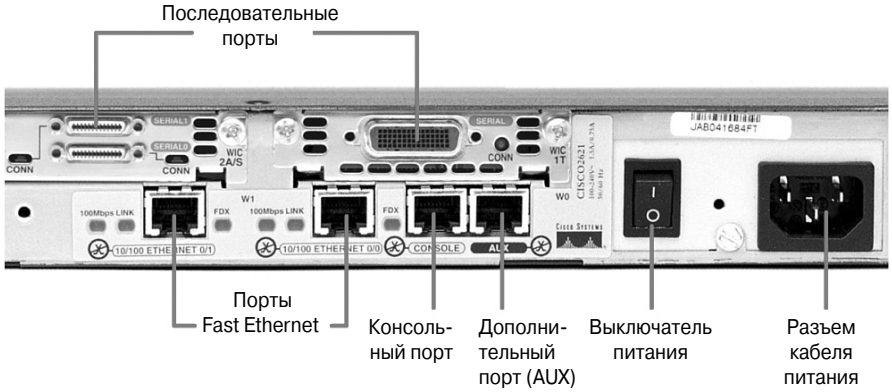


Рис. 12.17. Консольный порт маршрутизатора

Чтобы подключиться к консольному порту, необходимо использовать консольный кабель и адаптер для разъема RJ-45 на разъем DB-9[5] для подключения к персональному компьютеру, как показано на рис. 12.18. В стандартной поставке любое устройство комплектуется необходимыми средствами для подключения к персональному компьютеру: кабелем и адаптером-переходником.

Программное обеспечение персонального компьютера или алфавитно-цифровой терминал должны поддерживать режим работы или эмуляцию режима vt100. Программное обеспечение эмуляции терминала, программный пакет HyperTerminal, который входит в стандартную поставку операционной системы Windows корпорации Microsoft, используется наиболее часто (см. рис. 12.19).

[5] *В зависимости от типа COM-порта может использоваться и разъем DB-25. — Прим. ред.*

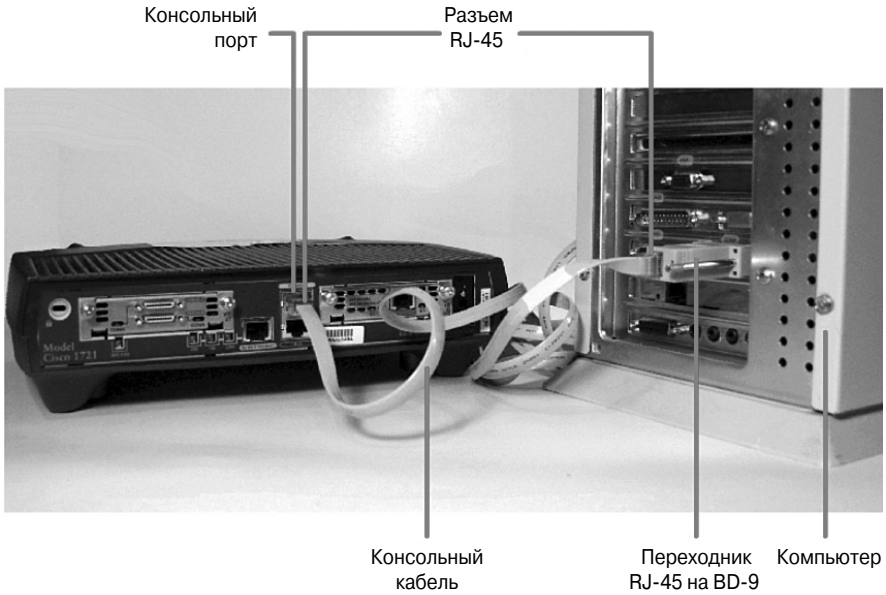


Рис. 12.18. Подключение к консольному порту маршрутизатора

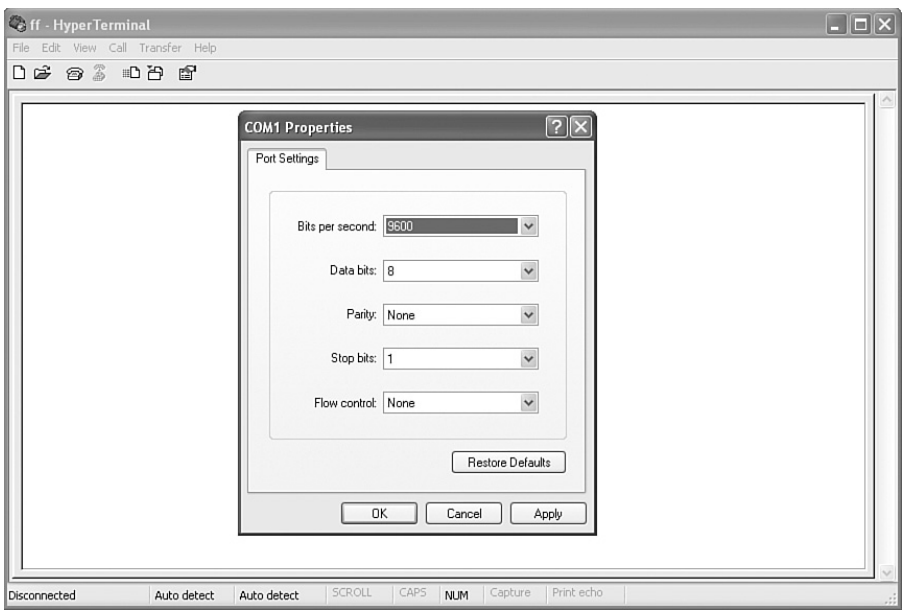


Рис. 12.19. Программа эмуляции терминала HyperTerminal

Для подключения персонального компьютера к консольному порту следует выполнить действия, описанные ниже.

Этап 1. Осуществить для программы эмуляции терминала персонального компьютера следующие настройки:
- указать соответствующий COM-порт;
- установить скорость 9600 бод;
- установить 8 битов данных;
- указать отсутствие проверки четности (no parity);
- установить использование одного стопового бита;
- указать отсутствие механизма управления потоком.

Этап 2. Подключить разъем RJ-45 консольного кабеля к консольному порту.

Этап 3. Подключить второй разъем RJ-45 консольного кабеля к переходнику DB-9.

Этап 4. Подключить переходник DB-9 к COM-порту персонального или портативного компьютера.

Практическое задание 12.2.5. Подсоединение интерфейса консоли
В этом задании необходимо идентифицировать интерфейс консоли маршрутизатора. Затем необходимо определить и подключить соответствующий кабель к коммуникационному порту компьютера и к порту консоли маршрутизатора.

Подключение через интерфейсы локальных сетей

К большинству сред локальных сетей маршрутизаторы подключаются посредством соединений Ethernet или Fast Ethernet. В данном случае маршрутизатор является узлом, который подключен к сети LAN посредством коммутатора или концентратора; для такого подключения используется кабель с прямой распайкой контактов. Интерфейс 10/100BASE-TX маршрутизатора должен быть подключен как минимум неэкранированной витой парой категории 5 (UTP) к любому другому устройству независимо от типа мрашрутизатора, как показано на рис. 12.20.

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

В любом соединении необходимо обращать внимание на тип интерфейса. Если для подключения будет использован “неправильный” интерфейс, то может пострадать как сам маршрутизатор, так и любое другое сетевое оборудование. Во многих портах или различных типах соединений используются одинаковые разъемы, например, для Ethernet-, ISDN-BRI-, консольных, AUX-портов интегрированных CSU/DSU и Token-Ring-портов используется один и тот же восьмиконтактный разъем RJ-45, RJ-48 или RJ-49. Чтобы администратор мог быстро и легко отличить

один порт от другого, в устройствах корпорации Cisco принято использовать специальные разноцветные метки для разных типов интерфейсов.

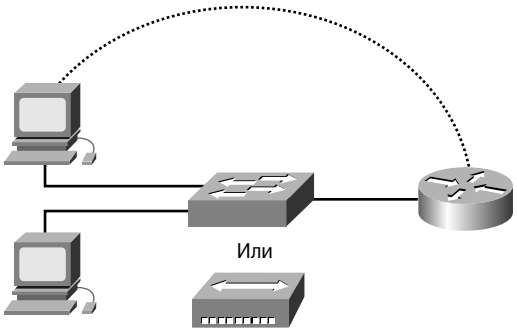


Рис. 12.20. Подключение маршрутизатора посредством неэкранированной витой пары

Практическое задание 1.2.6. Подсоединение интерфейса локальной сети
В этом задании необходимо идентифицировать интерфейс Fast Ethernet на маршрутизаторе. Затем нужно определить и подключить соответствующие кабели к маршрутизатору. После этого требуется подключить маршрутизатор и компьютер к концентратору.

Соединение WAN-интерфейсов

Соединений распределенных сетей существует великое множество, поскольку сами WAN-сети служат для объединения телекоммуникационных структур на большой географической площади посредством разнообразных технологий. Обычно WAN-службы арендуют у провайдеров услуг. К различным типам соединений распределенных сетей относят выделенные линии, соединения с коммутацией каналов и соединения с коммутацией пакетов (рис. 12.21).

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

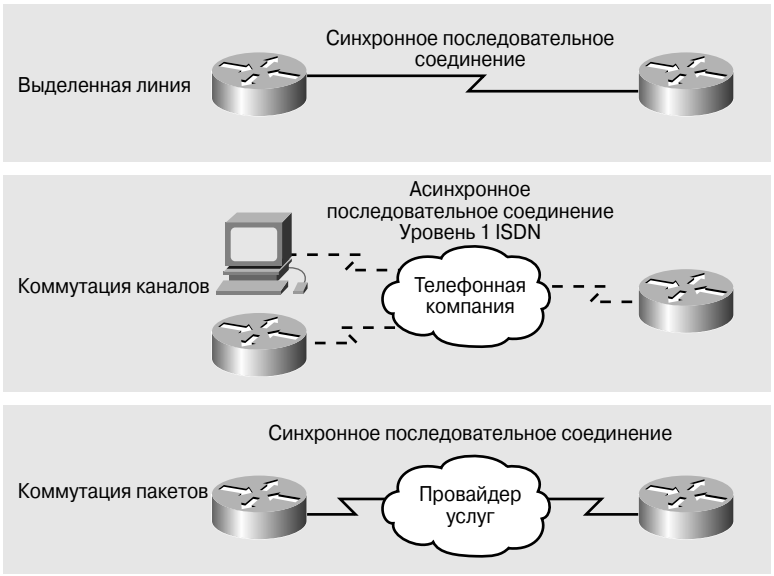


Рис. 12.21. Различные типы соединений распределенных сетей

Наиболее часто в качестве WAN-интерфейсов используются последовательные порты маршрутизатора. Чтобы упростить процесс выбора правильного последовательного кабеля для порта и правильно соединить два устройства, следует выяснить следующее:

- какой тип соединения используется на данном устройстве корпорации Cisco? В устройстве могут быть установлены разные разъемы для последовательных интерфейсов, как показано на рис. 12.22. Слева на рисунке показан так называемый *интеллектуальный* интерфейс (smart serial), справа — разъем интерфейса DB-60. Даже при беглом осмотре видно, что разъемы существенно отличаются один от другого, и поэтому необходимо выбрать и купить подходящий кабель в зависимости от типа интерфейса;
- к какому устройству подключен маршрутизатор: к DTE или DCE? DTE и DCE представляют собой разные типы взаимодействующих последовательных интерфейсов. Ключевое отличие двух интерфейсов состоит в том, что DCE-интерфейс обеспечивает сигнал синхронизации, который используется для осуществления коммуникации по шине. В документации к устройству обычно указано, к какому типу относится порт — DTE или DCE[6];

[6] *Практически все последовательные порты могут выступать как в качестве DTE-, так и в качестве DCE-порта; режим его работы, в частности, в непосредственном соединении двух устройств, зависит от типа кабеля: DTE или DCE. — Прим. ред.*

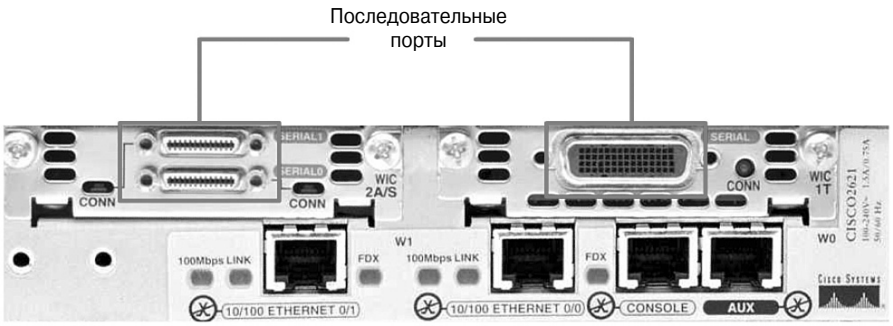


Рис. 12.22. Последовательные порты маршрутизатора

- какой стандарт сигнализации может использовать устройство? Для разных устройств и разных соединений могут использоваться различные стандарты последовательных соединений, как показано на рис. 12.23. В каждом стандарте указаны сигналы, передаваемые по кабелю, а также какой именно разъем используется на конце линии. Подробнее об используемом для интерфейса стандарте сигнализации написано в документации к устройству;

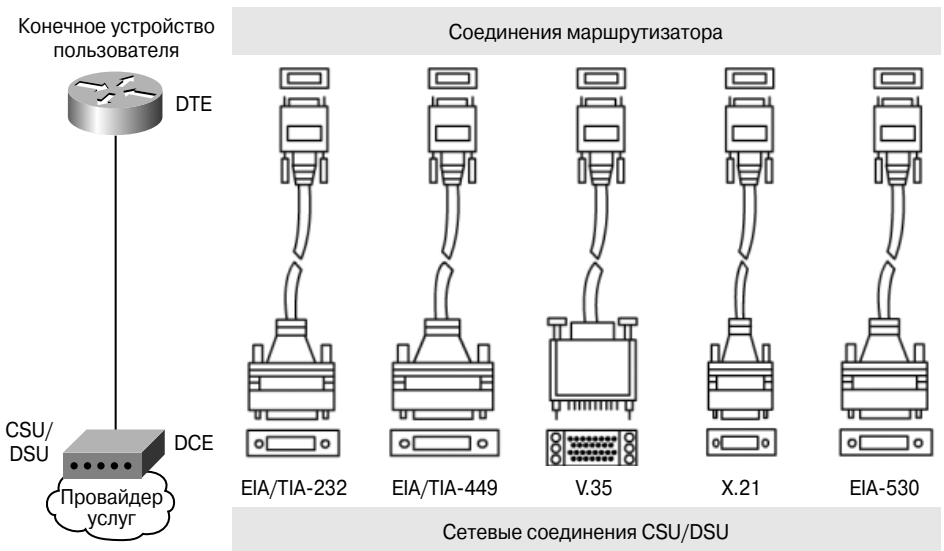


Рис. 12.23. Кабели и разъемы WAN-соединений

- какой тип разъема размещен на конце кабеля: вилка или розетка? Если у разъема есть штыри-контакты, то он является вилкой, если же отверстия для штырей, то это — розетка (рис. 12.24).

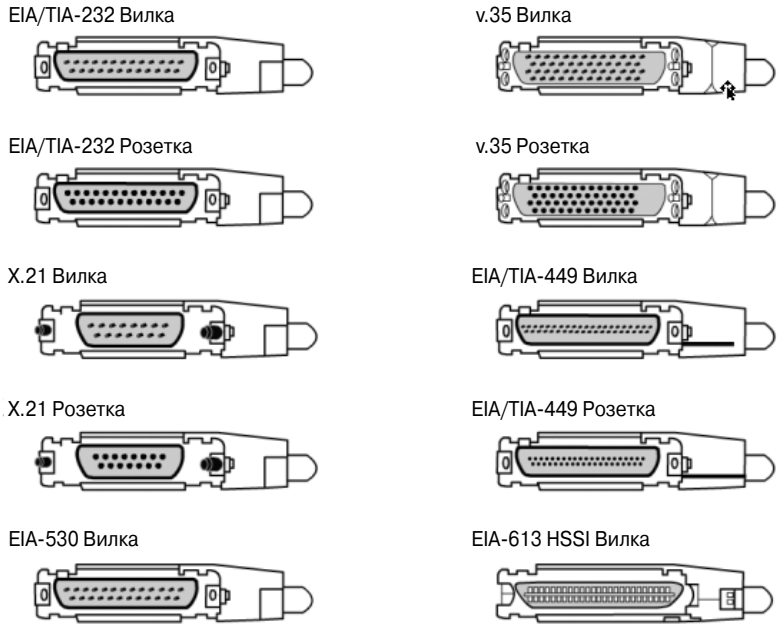


Рис. 12.24. Последовательные порты DCE-устройств

Практическое задание 12.2.7. Подсоединение интерфейса распределенной сети
В этом задании нужно идентифицировать последовательный интерфейс маршрутизатора. Далее необходимо определить и подключить соответствующие кабели к найденному порту распределенной сети маршрутизатора.

Резюме

В настоящей главе были изложены следующие ключевые темы, касающиеся маршрутизаторов:

- распределенная сеть Internet объединяет сотни больших и малых сетей по всему миру;
- распределенные сети используются для объединения локальных сетей, которые разделены большими географическими расстояниями;
- основными типами соединений в распределенных сетях являются выделенные линии, коммутируемые каналы, соединения с коммутацией пакетов и технологии с использованием коммутации ячеек;
- провайдеры служб сетей WAN предоставляют множество различных услуг потребителям; клиент должен уметь идентифицировать и выбрать необходимый кабель для подключения к службе;

- сетевыми устройствами распределенных сетей являются маршрутизаторы, коммутаторы распределенных сетей, модемы, устройства CSU/DSU и серверы доступа;
- протокол физического уровня распределенной сети описывает электрическое, механическое, операционное и функциональное взаимодействие служб распределенных сетей;
- протокол канального уровня распределенной сети описывает метод передачи фреймов между системами по одному каналу.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Ключевые термины

Время безотказной работы (uptime) — это промежуток времени, в течение которого сетевое устройство исправно функционировало и обрабатывало запросы пользователей.

Задержка распространения (propagation delay) — это время, которое требуется данным, чтобы пройти по сети от отправителя до конечного получателя. Часто этот термин заменяют радиотехническим термином *запаздывание (latency)*, который описывает процесс передачи сигнала.

Коммутатор (switch) — это сетевое устройство, которое фильтрует, перенаправляет и рассылает фреймы на основе адресов канального уровня получателя. Коммутаторы работают на канальном уровне эталонной модели OSI.

Коммутация каналов (circuit switching) представляет собой технологию, в которой во время сеанса связи должен существовать физический канал между отправителем и получателем. Широко используется в сетях телефонных компаний. С технологической точки зрения коммутацию каналов можно рассматривать как противоположность коммутации пакетов и сообщений, а с точки зрения методов доступа — как противоположность методу конкуренции и передачи маркеров. Примером сетевой технологии с коммутацией каналов является ISDN.

Коммутация пакетов (packet switching) представляет собой сетевую технологию, в которой разные узлы обмениваются друг с другом пакетами данных по одному разделяемому каналу связи.

Маршрутизатор (router) — это устройство сетевого уровня, которое использует одну или несколько метрик для определения оптимального пути доставки потока данных. Маршрутизаторы перенаправляют пакеты из одной сети в другую, основываясь на информации сетевого уровня. Иногда их называют *шлюзами (gateway)*, хотя это название уже устаревает.

Модем (модулятор-демодулятор — Modulator-demodulator, modem) — это устройство, преобразующее цифровые сигналы в аналоговые и наоборот. На станции-отправителе модем преобразует цифровые сигналы в форму, соответствующую каналам аналоговой связи. В пункте назначения аналоговые сигналы преобразуются в цифровую форму. Модемы позволяют передавать информацию по обычным телефонным линиям.

Конечное оборудование линии передачи данных (Data Circuit-terminating Equipment — DCE) — это устройство, используемое для конвертирования данных пользователя из цифрового формата DTE в форму, приемлемую для оборудования служб распределенной сети.

Распределенная сеть (Wide-Area Network — WAN) представляет собой сеть передачи данных, охватывающую значительное географическое пространство. В ней часто используются передающие устройства, предоставленные открытыми операторами связи, например, местными или государственными телефонными компаниями.

Службы с коммутацией ячеек (cell-switched service) предоставляют механизмы передачи данных, которые работают на основе технологии коммутации ячеек, но при этом позволяют создавать виртуальные каналы. Передаваемые данные разбиваются на ячейки фиксированной длины и потом передаются по каналам связи с помощью цифровых технологий передачи сигналов.

Терминальное оборудование (Data Terminal Equipment — DTE) — это устройство, расположенное на пользовательском конце интерфейса пользователь-сеть, которое может выступать в качестве источника данных, получателя данных или в качестве и того, и другого. Устройство DTE соединяется с сетью данных посредством устройства DCE (например, модема) и для синхронизации зачастую использует временные сигналы, генерируемые DCE. Терминальное оборудование включает в себя такие устройства, как компьютеры, трансляторы протоколов и мультиплексоры.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Какое из приведенных ниже определений лучше всего характеризует распределенную сеть?

   а) Она объединяет локальные сети, разделенные большими расстояниями.

   а) Она объединяет рабочие станции, терминалы и другие устройства региональных вычислительных сетей.

   а) Она объединяет локальные сети в больших зданиях.

   а) Она объединяет рабочие станции, терминалы и другие устройства в больших зданиях.

2. Чем распределенные сети отличаются от локальных?

а) В распределенных сетях делается упор на доступ через последовательные интерфейсы, работающие на малых скоростях.

б) Распределенные сети обеспечивают высокоскоростной доступ ко множеству служб.

в) Распределенные сети обычно развертываются на малых географических площадях.

г) Для регулирования потока данных в распределенных сетях используются метки.

3. Какие из технологий относятся к глобальным сетям?

а) Token Ring, ARCNet.

б) Frame Relay, ISDN.

в) Star, Banyan VINES.

г) CSU/DSU, ARCView.

4. На каких уровнях эталонной модели OSI работает распределенная сеть?

а) На канальном и сетевом.

б) На канальном и уровне представления данных.

в) На физическом и уровне приложений.

г) На физическом и канальном.

5. Какое определение лучше всего описывает конечное оборудование линии передачи данных (DCE)?

а) Оно состоит из пользовательских устройств на границе сети.

б) Оно выступает в роли отправителя или получателя данных.

в) Оно состоит из физических устройств, таких, как трансляторы протоколов или мультиплексоры.

г) Оно состоит из физических устройств, расположенных на границе канала распределенной сети.

6. Какие из следующих компонентов сети обеспечивают работу голосовых служб, устройств CSU/DSU, связанных со службами T1/E1, и терминального адаптера или сетевого терминатора первого типа (TA/NT1), связанных со службами ISDN?

а) Коммутаторы.

б) Маршрутизаторы.

в) Модемы.

г) Серверы-шлюзы.

7. Какое из устройств обеспечивает удаленный доступ для пользователей?

а) Коммутаторы.

б) Маршрутизаторы.

в) Модемы.

г) Серверы-шлюзы.

8. Укажите стандарты распределенной сети физического и канального уровней.

а) EIA/TIA-232.

б) PPP.

в) Frame Relay.

г) Все вышеперечисленное.

9. Выберите правильную пару из двух предложенных ниже наборов.

1) RAM/DRAM.

2) NVRAM.

3) ROM.

4) Flash-память.

5) Интерфейс.

Варианты:

а) Оперативная память (RAM), которая сохраняет свое содержимое после выключения устройства.

б) Энергонезависимая память, которая может быть считана и записана микропроцессором.

в) Энергонезависимая память, которая может быть считана, но не может быть записана микропроцессором.

г) Энергонезависимая память, которая может быть очищена и перепрограммирована, поэтому в ней могут храниться образы программного обеспечения, которые при необходимости можно перезаписать.

д) Соединение между двумя системами или устройствами.

Выберите правильный ответ:

а) 1-б, 2-а, 3-в, 4-д, 5-г.

б) 1-а, 2-б, 3-в, 4-д, 5-г.

в) 1-б, 2-а, 3-д, 4-в, 5-г.

г) 1-б, 2-а, 3-в, 4-г, 5-д.

10. Любое взаимодействие сетей будет, вероятно, соответствовать критериям, которые указаны ниже.

а) Последовательная конечная адресация и полоса пропускания, зависящая от приоритета.

б) Адресация, которая соответствует сетевой топологии, и гарантированное качество обслуживания.

в) Выбор наилучшего пути и динамическая маршрутизация.

г) Все вышеперечисленное.

11. Какие из перечисленных ниже технологий являются инкапсуляцией канального уровня в распределенной сети?

а) HLDC.

б) Frame Relay.

в) PPP.

г) Все вышеперечисленное.

12. Укажите основные функции маршрутизаторов.

а) Определение оптимального маршрута для входящих пакетов данных и передача их на соответствующий выходной интерфейс.

б) Передача ARP-запросов между узлами из различных локальных сетей.

в) Создание таблиц маршрутизации и обмен сетевой информацией с другими маршрутизаторами.

г) Варианты а и б.

13. Какая технология канального уровня распределенной сети, разработанная компанией IBM для среды SNA, была впоследствии заменена более гибким протоколом HDLC?

а) Протокол SLIP.

б) Протокол PPP.

в) Протокол SDCL.

г) Протокол SDLCP.

14. Какой протокол канального уровня распределенных сетей используется для передачи сигналов и установления соединения в D-канале сети ISDN?

а) LAPD.

б) LAPF.

в) LAPB.

г) LAPR.

15. Укажите службу или службы распределенной сети, которые работают по принципу коммутации каналов.

а) POTS.

б) Сеть ISDN с максимальной пропускной способностью 1,544 Мбит/с.

в) Сеть Frame Relay.

г) Варианты а и б.

16. Какая из служб распределенных сетей является более высокоскоростным последователем службы X.25 и имеет максимальную пропускную способность 44,736 Мбит/с? В Соединенных Штатах Америки широко используются кратные скорости работы этой службы по 56 Кбит/с и 384 Кбит/с.

а) Frame Relay.

б) X.25.

в) POTS.

г) ATM.

17. Укажите наиболее часто используемые разновидности DSL-технологии.

а) HDSL.

б) SDSL.

в) ADSL.

г) Все перечисленные варианты.

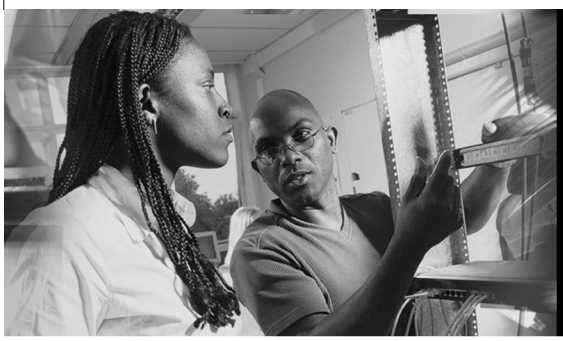
18. Какие сверхвысокоскоростные технологии физического уровня на основе оптических каналов способны обеспечивать скорость передачи данных от 51,84 Мбит/с (OC-1) до 9952 Мбит/с (OC-192) при использовании технологии спектрального уплотнения (WDM)?

а) SONET.

б) HDSL.

в) ATM.

г) SMDS.



ГЛАВА 13

Основы работы с маршрутизаторами

В этой главе...

- описано, как создать сеанс связи в HyperTerminal;
- описан процесс входа в систему маршрутизатора;
- показано, как использовать интерактивную справку командной строки маршрутизатора;
- рассмотрен процесс поиска ошибок в командной строке;
- описаны принципы работы операционной системы Cisco IOS и ее особенности;
- рассмотрен процесс поиска и устранения неисправностей при работе с операционной системой маршрутизаторов;
- рассмотрены примеры использования команды **`show version`**;
- приведено описание режимов интерфейса пользователя маршрутизатора и рассказано, для чего каждый из них предназначен;
- описаны функции операционной системы Cisco IOS;
- перечислены методы установления сеанса с программным обеспечением маршрутизатора для работы с устройством посредством интерфейса командной строки;
- перечислены команды, которые используются для переключения между режимом обычного пользователя и привилегированным.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

межсетевая операционная система корпорации Cisco, с. 632,
интерфейс командной строки, с. 632,
процесс начальной загрузки, с. 638,
память NVRAM, с. 639,
самотестирование, с. 639,
flash-память, с. 640,
светодиодные индикаторы, с. 644,
дочерняя плата, с. 660.

В этой главе рассказывается о том, как произвести первую загрузку маршрутизатора, используя необходимые команды, а также о том, как создать начальную конфигурацию маршрутизатора. Кроме того, в главе рассматривается последовательность запуска маршрутизатора и системный диалог, который служит для создания файла начальной конфигурации для используемой версии операционной системы Cisco IOS.

В процессе ознакомления с материалом главы обратите внимание на относящиеся к ней интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в данной главе.

Операционная система Cisco IOS

В основе большинства технологий корпорации Cisco лежит специализированная операционная система — *межсетевая операционная система корпорации Cisco (Internetwork Operating System — IOS),* которая представляет собой специфическое программное обеспечение, управляемое функциями маршрутизации и коммутации устройств. Глубокое знание этой операционной системы необходимо каждому сетевому администратору для уверенного выполнения своих обязанностей. В этой главе описываются основные функции и приемы работы с системой Cisco IOS, а также представлены примеры практического их применения.

Для чего нужна операционная система Cisco IOS

Подобно любому компьютеру, маршрутизатор или коммутатор не могут функционировать без операционной системы. В большинстве маршрутизаторов компании Cisco и коммутаторов Catalyst используется специализированная операционная система Cisco Internetwork Operating System, или сокращенно — Cisco IOS (межсетевая операционная система Cisco). В некоторых коммутаторах Catalyst также используется интерфейс командной строки (Command Line Interface — CLI). Маршрутизатор будет бесполезным набором деталей до тех пор, пока в нем не будет загружена операционная система. Операционная система Cisco IOS обеспечивает работу таких сетевых служб:

- основных служб маршрутизации и коммутации;
- функции надежного и безопасного доступа к сетевым ресурсам;
- средств масштабирования сети.

Пользовательский интерфейс маршрутизатора

В качестве традиционной интерактивной среды в операционной системе Cisco IOS используется *интерфейс командной строки (CLI — Command Line Interface*). Операционная система Cisco IOS является основной технологией, на которой базируется

большинство продуктов компании Cisco. Особенности работы с интерфейсом изменяются в зависимости от конкретного межсетевого устройства.

Доступ к среде командной строки можно получить несколькими методами.

- К интерфейсу командной строки доступ можно получить посредством сеанса связи через консольный порт маршрутизатора. В этом случае используется низкоскоростное последовательное соединение с терминалом или компьютером, эмулирующим этот терминал. Для этого метода доступа не требуется настройка сетевых служб маршрутизатора.
- К интерфейсу командной строки доступ можно получить посредством коммутируемого соединения с использованием модема или нуль-модемного соединения с портом AUX маршрутизатора. Для этого метода доступа не требуется настройка сетевых служб маршрутизатора.
- К интерфейсу командной строки доступ можно получить посредством Telnet-сеанса с маршрутизатором в виде виртуального терминала. Для создания Telnet-сеанса связи с маршрутизатором должен быть настроен, по крайней мере, один интерфейс для работы с IP-протоколом. Виртуальному терминалу должно быть задано пользовательское имя и пароль.

Пользовательский интерфейс маршрутизатора и его режимы

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

Операционная система Cisco IOS обеспечивает работу интерпретатора команд (EXEC). Интерпретатор проверяет и выполняет все команды, введенные в консоли.

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

В пользовательском режиме доступен ограниченный набор основных команд, которые позволяют отследить режимы работы маршрутизатора. Часто этот режим упоминается как режим просмотра. Пользовательский режим не допускает изменения файла конфигурации маршрутизатора. Слово “пользовательский” в названии этого режима не означает, что доступ к устройству может получить любой обычный пользователь сети. Этот режим предназначен для специалистов по информационным технологиям, технических специалистов и сотрудников, которым нужен доступ к устройству только для проведения мониторинга, но не нужны права на изменение конфигурации коммутатора, маршрутизатора и т.п. В командной строке этот режим идентифицируется символом “>”.

Привилегированный режим доступа дает возможность использовать все команды маршрутизатора. Доступ к этому режиму только авторизированный, он может быть ограничен паролем и идентификатором пользователя. Для выполнения команд настройки и управления маршрутизатором системному администратору необходимо войти в привилегированный режим. Доступ к режиму глобальной конфигурации и другим специальным режимам может быть получен только из привилегированного режима. В командной строке этот режим идентифицируется символом "#".

Для перехода в привилегированный режим необходимо ввести команду **enable** в командной строке с приглашением, которое оканчивается символом ">". Если пароль был установлен, то для продолжения работы маршрутизатор его потребует. В целях безопасности сетевые устройства Cisco не отображают вводимые символы пароля. Если введенный пароль верен, то приглашение командной строки маршрутизатора меняется на "#", и маршрутизатор входит в привилегированный EXEC-режим. Введя символ **?** в привилегированном режиме, вы увидите объемный список доступных команд; к некоторым из них можно получить доступ также из пользовательского режима.

Функции операционной системы Cisco IOS

Корпорация Cisco разрабатывает операционные системы Cisco IOS для широкого круга сетевых платформ. Для оптимизации операционных систем конкретно под каждое устройство компании приходится выпускать множество различных вариантов образов ОС Cisco IOS. Каждая операционная система имеет собственный набор функций, которые предназначены для работы с определенным устройством, и связана с наличием определенного объема памяти у устройства и потребностями покупателей.

Для различных типов устройств Cisco существует множество специализированных образов операционных систем. Однако основная структура команд остается неизменной. Поэтому опыт, полученный при работе с одним сетевым устройством корпорации Cisco, может быть очень полезен при работе с другим устройством.

Названия различных версий операционной системы регулируются соглашением и состоят из трех частей:

- кода платформы, для которой предназначена версия операционной системы;
- кода-признака специальных возможностей, поддерживаемых данной версией операционной системы;
- кода, который указывает, откуда образ операционной системы должен выполняться и сжат или заархивирован образ.

Более подробно вопрос особенностей операционной системы и условных обозначений рассматривается в главе 16, "Управление программным обеспечением Cisco IOS".

Соглашение об именовании образов операционной системы Cisco IOS, функции определенных образов операционной системы и много другое может быть в будущем изменено.

При выборе новой версии операционной системы Cisco IOS прежде всего следует рассмотреть требования к объему оперативной и Flash-памяти. Обычно, чем новее версия операционной системы, тем больше функций в нее включено, следовательно, тем больших аппаратных ресурсов, в частности, памяти они будут требовать. Для проверки текущей версии операционной системы и свободной Flash-памяти используйте команду **show version**, как показано в примере 13.1. На Web-сайте корпорации Cisco вы сможете найти вспомогательные инструменты, которые позволят определить объем Flash-памяти и объем оперативной памяти, необходимый для работы каждой из версий операционной системы.

После того как определены функции, которые необходимы в сети, следует выбирать нужную версию операционной системы Cisco IOS, которая поддерживает имеющееся оборудование. Требования каждого сетевого устройства перечислены в разделе "Cisco Product Documentation" (Информация об устройствах Cisco) компакт-диска с документацией. Наиболее свежую информацию всегда можно получить при помощи интерактивного инструмента Cisco Software Advisor (Консультант по программному обеспечению Cisco) на Web-сайте корпорации.

Перед установкой образа операционной системы Cisco IOS в маршрутизаторе следует проверить наличие достаточного количества памяти для установки новой версии. Для проверки объема ОЗУ используйте команду **show version**, как показано в примере 13.1.

Пример 13.1. Результат выполнения команды show version

```
Cisco> show version

Cisco Internetwork Operating System Software
--- Часть информации опущена ---
image file is "flash:/c2500-i-l.121-16.bin"

Cisco 2600 (68030) processor (revision N) with 6144K/2048K bytes of
memory.
```

В последней строке показан общий объем и объем разделяемой памяти в маршрутизаторе. В некоторых системах используется динамическое распределение оперативной памяти. Для работы операционной системы важен как общий объем памяти, так и объем разделяемой памяти, поэтому при установке новой версии Cisco IOS нужно принимать во внимание оба параметра.

Чтобы определить объем доступной Flash-памяти[1], используется команда **show flash**, как показано в примере 13.2.

[1] *Следует обратить внимание на то, что в данном случае память доступна только для чтения (фраза "Read ONLY" в последней строке). Такая надпись свидетельствует о том, что операционная система работает непосредственно из Flash-памяти, в оперативную память подгружаются только некоторые службы, и она не может быть обновлена в режиме нормальной работы маршрутизатора. — Прим. ред.*

Пример 13.2. Результаты работы команды `show flash`

```
Cisco> show flash

System flash directory:
File Length   Name/status
  1  8022152  /c2500-i-l.121-16.bin
[8022216 bytes used, 366392 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

Устранение неполадок в работе операционной системы Cisco IOS

Нормальная загрузка маршрутизатора может прерваться или вообще не начаться по одной из следующих причин:

- в файле конфигурации отсутствует параметр **`boot system`** или его значение установлено неверно;
- введено некорректное значение конфигурационного регистра;
- данные во Flash-памяти повреждены;
- произошел аппаратный сбой.

При загрузке маршрутизатора он ищет в файле конфигурации параметр **`boot system`**. Этот параметр может применяться для загрузки маршрутизатора с использованием альтернативного образа операционной системы вместо того, который находится во Flash-памяти. Для проверки текущего образа операционной системы введите команду **`show version`**, как показано в примере 13.3.

Пример 13.3. Проверка текущего образа операционной системы

```
Cisco> show version
--- Часть информации опущена ---

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTLDR: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c),
RELEASE
   SOFTWARE (fc1)
```

Нормальной загрузке операционной системы Cisco IOS может помешать неправильное значение регистра настройки. Это значение указывает маршрутизатору, откуда следует брать образ операционной системы для загрузки. Для проверки текущего месторасположения образа операционной системы используется команда **`show version`**, как показано в примере 13.4.

Пример 13.4. Настройка регистров

```
Cisco> show version
--- Часть информации опущена ---

Configuration register is 0x2102
```

Правильное значение конфигурационного регистра зависит от конкретной аппаратной платформы. В документацию по операционной системе Cisco IOS также включена печатная версия результатов работы команды **show version**. Если же документация отсутствует, то правильное значение регистра настройки можно найти на компакт-диске с документацией или же на Web-узле Cisco.com. Измените регистр настройки в соответствии с используемой платформой и сохраните это значение в стартовой конфигурации.

Если же проблема не устранена, то, вероятнее всего, поврежден образ операционной системы, хранящийся во Flash-памяти. В этом случае во время загрузки могут выдаваться различные сообщения об ошибках, например, такое:

```
open: read error...requested 0x4 bytes, got 0x0
trouble reading device magic number
boot: cannot open "flash:"
boot: cannot determine first file name on device "flash:"å
```

Если образ операционной системы во Flash-памяти поврежден, необходимо загрузить новую версию. Если же и после этого проблемы в работе не устранены, то, вероятнее всего, в машрутизаторе происходит сбой аппаратных средств. В таком случае необходимо связаться с представителем корпорации Cisco. Несмотря на то что аппаратные сбои крайне редки, тем не менее, иногда они могут возникать.

В табл. 13.1 приведен список полезных команд для проверки состояния маршрутизатора. Список всех **show**-команд можно получить, введя в командной строке слово **show**, а затем после пробела — символ **?**.

Таблица 13.1. Команды проверки состояния маршрутизатора

Команда	Описание
show version	Отображает конфигурацию аппаратных средств системы, версию программного обеспечения, названия и источники файлов конфигурации, загрузочные образы, а также причину последней перезагрузки системы
show processes	Отображает информацию об активных процессах
show protocols	Отображает настроенные протоколы. Эта команда показывает состояние всех протоколов третьего уровня (сетевой уровень)
show memory	Отображает статистику о памяти маршрутизатора, включая информацию о пуле свободной памяти
show stacks	Мониторинг использования стека процессов и процедур прерывания
show buffers	Обеспечивает просмотр статистики буферов маршрутизатора
show flash	Показывает информацию об устройстве Flash-памяти

Окончание табл. 13.1

Команда	Описание
`show running-config` (`write term` для операционной системы Cisco IOS Software версии 10.3 и меньше)	Отображает активный файл конфигурации
`show startup-config` (`show config` для операционной системы Cisco IOS Software версии 10.3 и ниже)	Отображает резервный файл конфигурации
`show interface`	Отображает статистические данные обо всех настроенных интерфейсах

Запуск и режимы работы операционной системы Cisco IOS

В операционной системе Cisco IOS есть три различных режима работы:

- ROM-монитор;
- загрузка из ПЗУ (Boot ROM);
- полнофункциональный режим Cisco IOS.

В процессе запуска в нормальном режиме маршрутизатор обычно загружает в оперативную память (RAM) операционную систему и работает в соответствующем режиме. Для установки или проверки параметров загрузки устройства и режимов работы используются значения, которые установлены в конфигурационные регистры.

Программное обеспечение ROM-монитора выполняет *процесс начальной загрузки* и обеспечивает работу и диагностику аппаратного обеспечения маршрутизатора на нижнем уровне. Этот программный код используется для восстановления системы после сбоев, а также для восстановления утраченных паролей. Доступ к режиму ROM-монитора не может быть получен через сетевые интерфейсы, а только посредством консольного сеанса.

Когда маршрутизатор загружается в режиме работы из ПЗУ, то доступны лишь ограниченные функции, предоставляемые операционной системой. При загрузке из ПЗУ пользователь имеет возможность записывать образ системы во Flash-память; он прежде всего используется для замены операционной системы Cisco IOS, хранимой во Flash-памяти. При помощи команды **`copy tftp flash`**, которая копирует образ операционной системы, хранимой на TFTP-сервере, во Flash-память, пользователь или администратор имеет возможность обновить версию операционной системы маршрутизатора в нормальном полнофункциональном режиме работы.

Для нормальной работы маршрутизатору необходимо наличие полной версии операционной системы Cisco IOS, хранящейся во Flash-памяти. В некоторых устройствах операционная система работает непосредственно из Flash-памяти, без считывания ее в оперативную память. Однако большинство маршрутизаторов копирует

образ операционной системы из Flash-памяти в оперативную память (ОЗУ) и запускает ее уже из ОЗУ. Некоторые образы операционной системы Cisco IOS хранятся во Flash-памяти в сжатом виде и перед запуском распаковываются.

Определить название и версию текущей операционной системы маршрутизатора можно с помощью команды **show version**, которая также отображает настройку конфигурационных регистров. Команда **show flash** используется, как показано в примере 13.5, для того чтобы удостовериться, что Flash-память доступна и в нее можно записывать, а также для того, чтобы проверить, что маршрутизатор имеет достаточно места во Flash-памяти, чтобы вместить образ операционной системы IOS.

Пример 13.5. Проверка Flash-памяти и образа операционной системы Cisco IOS

```
Cisco> show flash

System flash directory:
File  Length    Name/status
 1     8022152  /c2500-i-l.121-16.bin
[8022216 bytes used, 366392 available, 8388608 total]
8192K bytes of processor board System flash (Read ONLY)
```

Запуск маршрутизатора

Многие задачи по конфигурированию сети, от самых простых до самых сложных, фактически сводятся к конфигурированию маршрутизаторов. В этой части главы описаны средства и методы запуска и конфигурирования маршрутизатора, которые, несомненно, пригодятся в практической работе.

Последовательность начальной загрузки маршрутизатора и режим начальной настройки

При инициализации маршрутизатора последовательно загружается *программа начальной загрузки* (bootstrap), операционная система и файл конфигурации. Если при инициализации маршрутизатор не обнаруживает конфигурационный файл, то он автоматически входит в *режим начальной настройки (setup mode)*. Резервная копия нового файла конфигурации, создаваемого в режиме настройки, сохраняется в энергонезависимой памяти с произвольным доступом (NonVolatile Random Access Memory — NVRAM).

После включения питания маршрутизатор Cisco выполняет *самотестирование* (POST — Power-On Self-Test). Программа самотестирования записана в постоянном запоминающем устройстве (Read Only Memory — ROM). При самотестировании происходит проверка работоспособности всех аппаратных компонентов маршрутизатора: центрального процессора, памяти и портов сетевых интерфейсов. После проверки аппаратных средств маршрутизатор запускает процесс инициализации программного обеспечения, который состоит из двух этапов:

- системные стартовые подпрограммы инициализируют программное обеспечение маршрутизатора;
- резервные подпрограммы, предназначенные для восстановления программного обеспечения, по мере необходимости выполняют альтернативный запуск программного обеспечения.

Стартовые подпрограммы предназначены для запуска операционной системы машрутизатора Cisco IOS. Маршрутизатор должен обеспечить надежное взаимодействие объединенных сетей согласно заданной конфигурации. Для достижения требуемой цели стартовые подпрограммы должны выполнить следующие действия:

1. удостовериться в том, что аппаратные средства маршрутизатора проверены и нормально функционируют;
2. найти и загрузить основную операционную систему Cisco IOS;
3. найти и применить стартовый конфигурационный файл или, в случае его отсутствия, войти в режим начальной настройки.

Последовательность запуска маршрутизатора

После выполнения процедур самотестирования при инициализации маршрутизатора происходят перечисленные ниже события.

1. Выполняется программа начальной загрузки, которая находится в постоянном запоминающем устройстве (ROM). Она представляет собой простую, предустановленную программу, которая способна выполнять элементарные инструкции. Кроме всего прочего, эта программа может загружать в память альтернативные инструкции или переводить маршрутизатор в другие режимы конфигурирования.
2. Образ операционной системы может находиться в нескольких местах. Для определения местоположения операционной системы используется загрузочное поле конфигурационного регистра. Если загрузочное поле указывает на *Flash-память* или на загрузку из сети, то команда **`boot system`** в конфигурационном файле указывает имя и местоположения файла-образа операционной системы. Конфигурационный файл, называемый стартовым, хранится в памяти NVRAM и содержит команды, которые администратор заранее внес в конфигурацию и сохранил в маршрутизаторе. Если в стартовом конфигурационном файле явно не указано, откуда маршрутизатор должен загружать образ операционной системы Cisco IOS, стандартно устройство ищет его во Flash-памяти.
3. Далее загружается образ операционной системы Cisco IOS. После загрузки операционная система создает список программных и аппаратных компонентов, который выводится в терминальное приложение консоли.
4. В основную память загружается и построчно выполняется файл стартовой конфигурации, который сохранен в энергонезависимой памяти (NVRAM). Команды этого файла запускают процессы маршрутизации, задают адреса интерфейсов, устанавливают характеристики носителей и т.д.

5. Если в памяти NVRAM хранится неправильный файл конфигурации или эта память очищена, то после перезагрузки операционная система вызывает программу начальной конфигурации, также называемую диалогом начальной настройки.

На рис. 13.1 проиллюстрирована последовательность загрузки маршрутизатора.

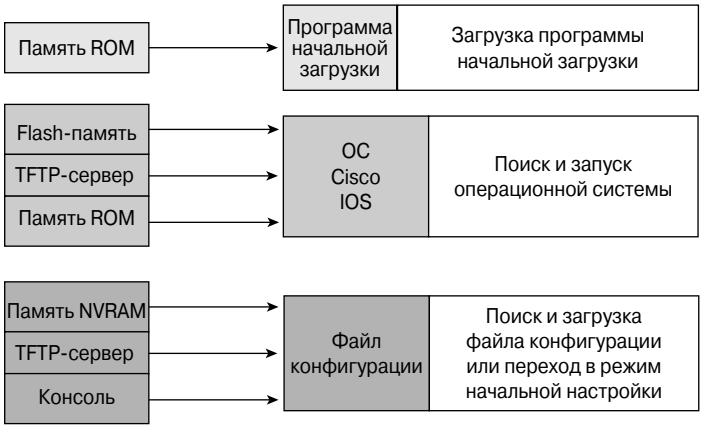


Рис. 13.1. Последовательность загрузки маршрутизатора

Дополнительная информация: диалог начальной настройки системы

Диалог начальной настройки системы не предназначен для конфигурирования сложных свойств протоколов в маршрутизаторе. Основным его предназначением является создание минимальной конфигурации, необходимой для запуска маршрутизатора, если маршутизатор не может получить конфигурацию из других источников. Этот режим не рекомендуется использовать в качестве основного средства конфигурирования маршрутизатора. Большинству администраторов проще выйти из такого режима и сконфигурировать устройство через интерфейс командной строки операционной системы Cisco IOS.

Для большинства запросов в процессе работы диалога начальной настройки системы в квадратных скобках (**[]**) указываются ответы, которые будут использоваться стандартно, если пользователь не введет другой вариант. Для того чтобы использовать стандартное значение, следует просто нажать клавишу <Enter> (возврат каретки).

Если система уже была предварительно настроена, то в квадратных скобках будут отображаться текущие значения запрашиваемых параметров. Для того чтобы очистить текущую конфигурацию маршрутизатора и удалить ее из NVRAM-памяти, используется команда **`erase stratup-config`**. Команда **`reload`** перезагружает маршрутизатор и заново запускает диалог начальной настройки системы. Если система настраивается впервые, то стандартно будут отображаться параметры, установленные на заводе-изготовителе. Если на заводе-изготовителе не было указано никакое значение, например, не был установлен пароль, то после вопросительного знака **?** в диалоге не будет ничего отображаться. В процессе настройки системы в любой момент можно нажать сочетание клавиш <Crtl>+<C>, чтобы прервать процесс настройки и начать его заново. После завершения процедуры начальной установки конфигурации все интерфейсы находятся в выключенном состоянии (shutdown). В примере 13.6 проиллюстрирована работа диалога начальной настройки, запускаемого с помощью команды **`setup`**.

Пример 13.6. Команда `setup`

```
# setup

-- System Configuration Dialog --
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: no

First, would you like to see the current interface summary? [yes]: yes

Interface  IP-Address     OK? Method  Status                Protocol
Ethernet0  198.133.219.1  YES NVRAM   up                        down
Serial0    unassigned     YES NVRAM   administratively down     down
Serial1    unassigned     YES NVRAM   administratively down     down
```

После завершения процесса настройки маршрутизатора на экран выводится созданный конфигурационный файл. На запрос, использовать ли эту конфигурацию, следует ответить **yes** (да), в результате чего конфигурационный файл будет сохранен в NVRAM-память. Если же будет введено ключевое слово **no** (нет), то конфигурационный файл не будет сохранен, и процесс настройки начнется заново. Если в режиме отображения конфигурации будет выведена строка `-- More --`, то для просмотра следующей страницы информации нужно нажать пробел на клавиатуре.

Установка глобальных параметров

После просмотра информации об интерфейсах будет выведен запрос на настройку глобальных параметров маршрутизатора, как показано в примере 13.7. Выводимые параметры полностью соответствуют информации, которую администратор вводил в ответах на вопросы диалога начального конфигурирования устройства.

Первое сообщение операционной системы указывает на то, что в данный момент конфигурируются глобальные параметры маршрутизатора. В качестве первого глобального параметра необходимо указать имя маршрутизатора. Это имя будет являться частью приглашения командной строки операционной системы Cisco IOS Software для всех режимов работы. В начальной конфигурации стандартно маршрутизатору уже присвоено имя, которое отображается в квадратных скобках [*Router*]. После указания имени маршрутизатора следует задать различные пароли, которые используются в машрутизаторе.

На данном этапе следует установить пароль, который впоследствии позволит получить доступ к привилегированным режимам настройки маршрутизатора. В качестве альтернативы такой настройке можно указать секретный пароль, который шифруется по специальному алгоритму, разработанному компанией Cisco, что повышает его безопасность. Если посторонний человек взглянет на файл конфигурации, то строка секретного пароля будет выглядеть бессмысленным набором символов.

Пример 13.7. Установка глобальных параметров

```
Configuring global parameters:

  Enter host name [Router]: Cisco

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: cougars

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: lumberjacks

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: matadors
  Configure SNMP Network Management? [yes]: no
```

При начальной настройке рекомендуется, но не требуется, чтобы *пароль доступа к режимам конфигурации* (enable password) отличался от *секретного пароля* (enable secret word). Секретный пароль кодируется односторонним алгоритмом и может быть использован вместо пароля доступа к режимам конфигурации. Пароль доступа к различным режимам настройки используется лишь в том случае, когда в маршрутизаторе не задан секретный пароль. Поскольку для шифрования секретного пароля используется одностороннее шифрование, если он забыт или утерян, его невозможно будет восстановить. Пароль доступа к режимам конфигурирования хранится в открытом виде и может быть прочитан из файла конфигурации.

Все пароли чувствительны к регистру символов и могут содержать буквы, цифры и некоторые другие символы.

Дополнительно маршрутизатор позволяет установить пароль на доступ к отдельным портам. В примере 13.8 показана команда **line console 0,** после которой следуют подкоманды **login** и **password**, которые устанавливают пароль для доступа к консоли устройства. Такая настройка выполняется для того, чтобы пользователю необходимо было ввести свое имя и пароль. прежде чем он получит доступ к консольному порту устройства. Параметр **console 0** задает консольное соединение маршрутизатора, параметр **login** необходим для того, чтобы перед получением доступа к консоли пользователю необходимо было ввести имя и пароль.

Пример 13.8. Настройка пароля доступа к консоли маршрутизатора

```
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password Cisco
```

Как показано в примере 13.9, команда **line vty 0 4,** после которой следуют подкоманды **login** и **password,** позволяет установить пароль на входящие Telnet-сеансы.

Пример 13.9. Настройка пароля виртуальных терминалов маршрутизатора

```
Router(config)# line vty 0 4
Router(config-line)# login
Router(config-line)# password sanjose
```

После того как введены пароли для доступа к различным портам, необходимо выбрать протоколы маршрутизации, которые будут использоваться, как показано в примере 13.10. На запросы системного диалога следует вводить значения, которые вы выбрали для вашего маршрутизатора. Если на какой-либо запрос администратор дает положительный ответ (**yes**), то ему будет необходимо ответить на дополнительные вопросы, касающиеся выбранного протокола.

Пример 13.10. Настройка протоколов маршрутизации

```
Configure IP? [yes]:
    Configure IGRP routing? [yes]: 200
% Please answer 'yes' or 'no'.
    Configure IGRP routing? [yes]: yes
      Your IGRP autonomous system number [1]: 200
Configuring interface parameters:

Do you want to configure Ethernet0 interface? [yes]: yes
    Configure IP on this interface? [yes]: yes
      IP address for this interface: 10.10.10.1
      Subnet mask for this interface [255.0.0.0] :
      Class A network is 10.0.0.0, 8 subnet bits; mask is /8

Do you want to configure Serial0 interface? [yes]: n

Do you want to configure Serial1 interface? [yes]: n

The following configuration command script was created:

hostname Cisco
enable secret 5 $1$37Kq$vA6UckClKEBzOIWGIF54U/
enable password lumberjacks
line vty 0 4
password sanjose
no snmp-server
!
no bridge 1
ip routing
!
interface Ethernet0
ip address 10.10.10.1 255.0.0.0
!
! --- Остальная часть конфигурации опущена ---
```

Практическое задание 13.2.1. Конфигурирование маршрутизатора при помощи диалога начальной настройки

В этом задании необходимо использовать диалог начальной настройки маршрутизатора для задания основных параметров устройства.

Светодиодные индикаторы маршрутизатора

Для отображения текущего состояния маршрутизатора используются *светодиодные индикаторы (LED-индикаторы)*. Назначение и количество индикаторов зависит от модели машрутизатора Cisco.

Верхний индикатор на дочерней плате показывает активность последовательного порта 1 дочерней платы. Нижний индикатор показывает активность порта сети WAN или соединения BRI. На рис. 13.2 и 13.3 показаны светодиодные индикаторы маршрутизаторов различных типов.

Индикаторы на маршрутизаторах показывают активность соответствующих интерфейсов. Если индикатор не светится, но интерфейс корректно подсоединен к сети, то это свидетельствует о проблемах в работе оборудования. Если же интерфейс маршрутизатора загружен в полной мере, то индикатор будет светиться постоянно. На обоих платах интерфейсов распределенной сети (WAN) в случае успешной их инициализации должен светиться зеленый индикатор.

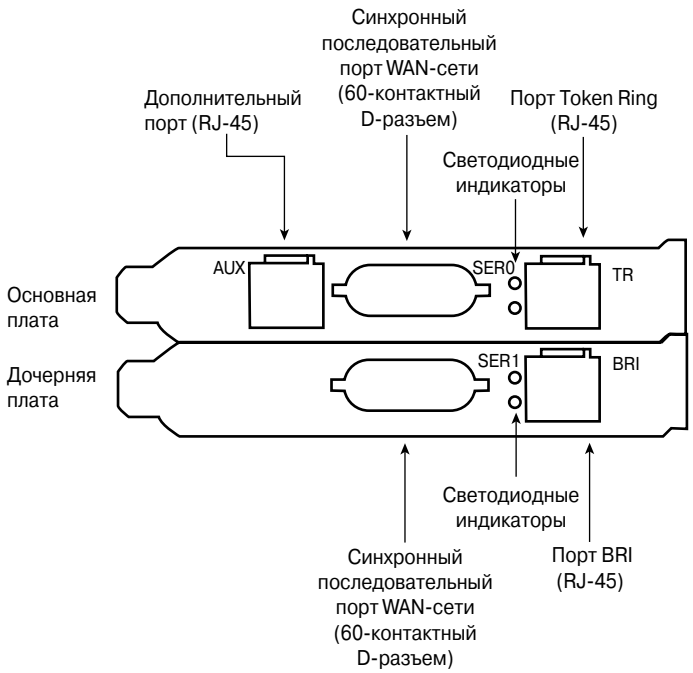


Рис. 13.2. Индикаторы машрутизатора серии 2500

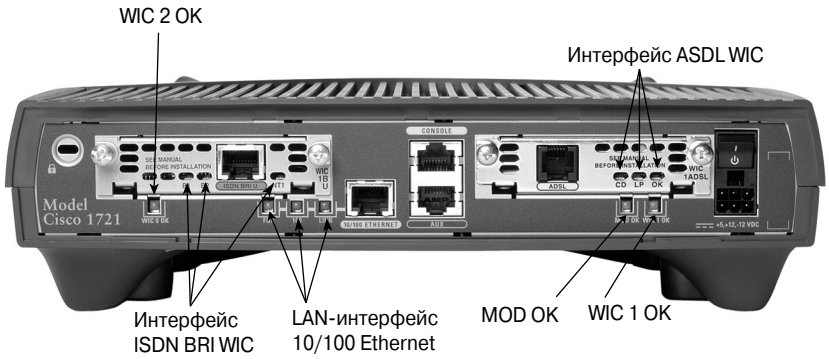


Рис. 13.3. Индикаторы машрутизатора серии 1721

Информация, выводимая при загрузке маршрутизатора

Загрузка маршрутизатора проходит по описанному ниже сценарию.

1. Для проверки работоспособности основных компонентов — центрального процессора, памяти и интерфейсов — маршрутизатор выполняет процедуру самодиагностики POST.
2. Для проверки корректной работы программы начальной загрузки отрабатывается образ загрузочного программного обеспечения, а также ищется подходящий образ программного обеспечения Cisco IOS (операционной системы маршрутизатора). Источником, содержащим образ операционной системы Cisco IOS, может быть Flash-память устройства или TFTP-сервер, что определяется конфигурацией регистров маршрутизатора. Стандартное значение регистров устанавливается на заводе-изготовителе и равно `0x2102`. Оно указывает маршрутизатору, что следует загружать операционную систему из Flash-памяти вне зависимости от того, что указано в качестве параметра команды **`boot system`**. Эта команда используется для того, чтобы указать порядок следования источников, в которых устройство будет искать образ операционной системы Cisco IOS. Если команда **`boot system`** с какими-либо параметрами в конфигурационном файле отсутствует (т.е. отсутствует в памяти NVRAM), маршрутизатор использует стандартную последовательность резервной загрузки операционной системы, т.е. устройство сначала ищет образ системы IOS во Flash-памяти.
3. Если после пяти попыток во Flash-памяти не обнаруживается подходящий образ операционной системы, то маршрутизатор загружается, используя программное обеспечение, хранимое в постоянном запоминающем устройстве (памяти ROM). Такое урезанное программное обеспечение используется для установки или обновления образов операционной системы Cisco IOS.
4. Если подходящий образ операционной системы все же был найден, то далее маршрутизатор пытается найти подходящий файл конфигурации.

5. Если файл конфигурации не обнаружен в NVRAM-памяти, то машрутизатор ищет его на TFTP-сервере, последовательно перебирая все интерфейсы. Если файл конфигурации не найден, машрутизатор запускает диалог для ручной настройки устройства.

В примерах 13.11 и 13.12 показаны различные сообщения, выводимые маршрутизаторами в зависимости от типа маршрутизатора и версии операционной системы Cisco IOS.

Пример 13.11. Ошибка чтения из NVRAM-памяти

```
System Bootstrap, Version X.X(XXXX) [XXXXX XX], RELEASE SOFTWARE
Copyright (c) 1986-199X by Cisco Systems
1721 processor with 4096 Kbytes of main memory

Notice: NVRAM invalid, possibly due to write erase.

--- Остальная часть информации опущена ---
```

Пример 13.12. Номер версии загрузочной программы и версия операционной системы Cisco IOS

```
--- Часть информации опущена ---

IOS (tm) 1721 Software (XXX-X-X), Version [XXXXX XXX]
Copyright (c) 1986-199X by Cisco Systems, Inc.
```

ВНИМАНИЕ!

Ошибка чтения из NVRAM-памяти может быть результатом намеренного или непреднамеренного выполнения команды **`erase start`** или более старой версии команды **`write erase`**.

Обратите внимание на ошибку чтения из NVRAM-памяти, которая показана в примере 13.11. Такое сообщение может означать, что энергонезависимая память полностью очищена. Что в свою очередь означает, что маршрутизатор не был настроен и без предварительного конфигурирования он не может быть использован.

Из информации, которая показана в примере 13.12, можно определить версию начальной загрузочной программы и версию операционной системы Cisco IOS, которая используется в маршрутизаторе. Также пользователь может уточнить модель маршрутизатора, серию используемого процессора и количество системной памяти. Остальная информация, выводимая при загрузке маршрутизатора, показана в примере 13.13 и содержит:

- количество интерфейсов маршрутизатора;
- перечисление типов интерфейсов машрутизатора;

- объем NVRAM-памяти;
- объем Flash-памяти.

Пример 13.13. Информация, выводимая в процессе загрузки маршрутизатора Cisco

```
Processor board ID 10226279
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
MICA-6DM Firmware: CP ver 2730 - 5/23/2001, SP ver 2730 - 5/23/2001.
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
Primary Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
24 Serial network interface(s)
4 Low-speed serial(sync/async) network interface(s)
6 terminal line(s)
1 Channelized T1/PRI port(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
32768K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Установка консольного соединения

Все маршрутизаторы Cisco имеют асинхронный последовательный порт консоли (RJ-45) стандарта EIA/TIA-232. Для соединения консольного терминала (ASCII-терминал или компьютер с запущенной программой эмуляции терминала) с портом консоли требуется кабель и переходники. Для соединения порта консоли маршрутизатора с персональным компьютером, на котором запущена программа эмуляции терминала, следует использовать кабель с разъемами RJ-45 и переходники из RJ-45 в DB-9 или из RJ-45 в DB-25 (в зависимости от типа распайки последовательного порта компьютера).

Стандартно порт консоли работает на скорости 9600 бод, в режиме передачи восьми битов данных, отсутствует контроль по четности, используется один стоповый бит и нет управления потоком, поскольку порт консоли не поддерживает аппаратное управление потоком.

Для подключения терминала к порту консоли следует выполнить описанные ниже действия.

1. Подсоедините терминал или персональный компьютер при помощи консольного кабеля с разъемами RJ-45 и переходниками RJ-45–DB-9 или RJ-45–DB-25.
2. Настройте терминал или программу эмуляции терминала на персональном компьютере на скорость 9600 бод, режим передачи — 8 битов данных, без контроля четности, с использованием одного стопового бита и без управления потоком.

На рис. 13.4 показан пример подключения консольного порта к персональному компьютеру для создания HyperTerminal-сеанса.

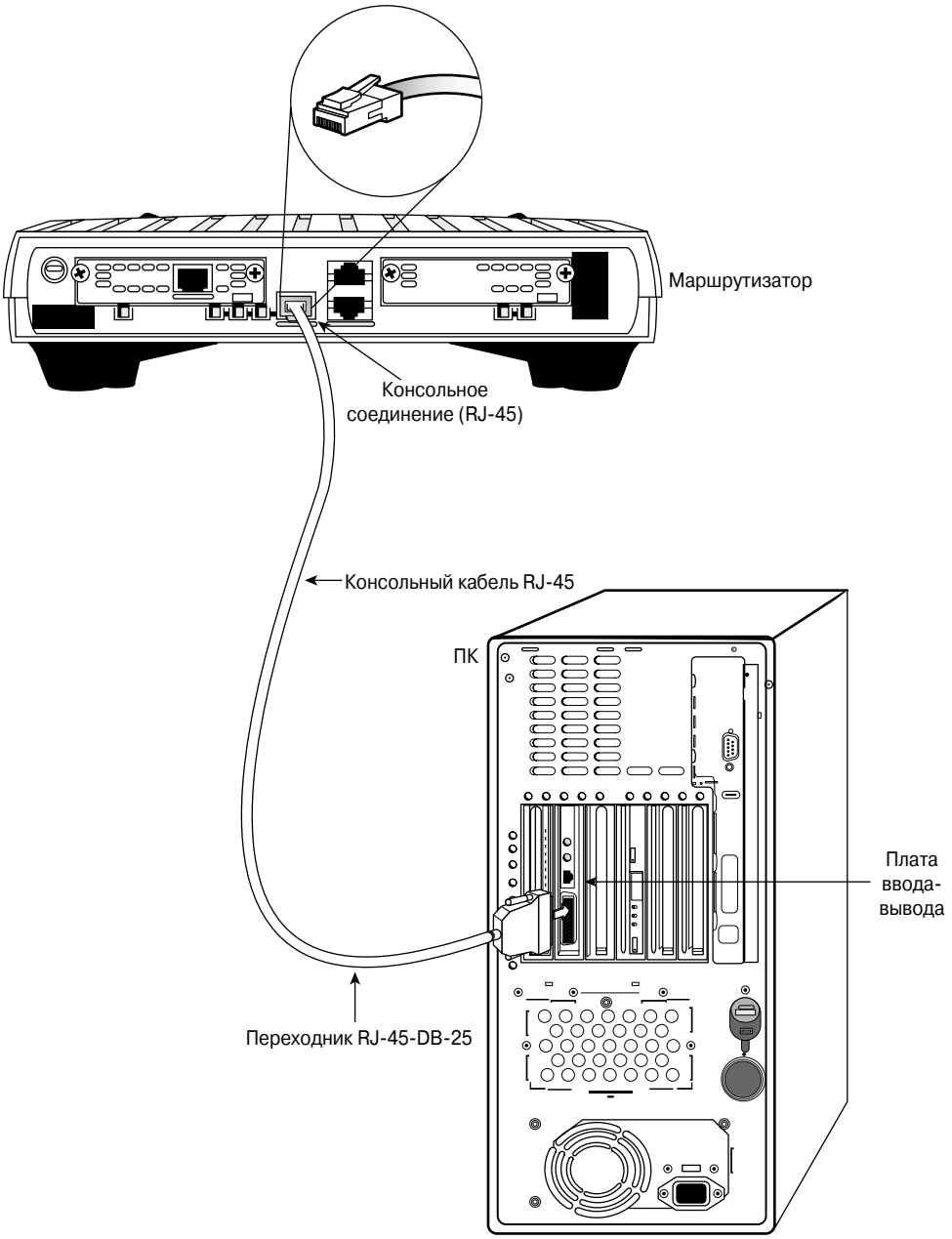


Рис. 13.4. Кабель для соединения с консольным терминалом

В табл. 13.2 приведен список операционных систем и программ эмуляции терминалов, которые могут использоваться в каждой операционной системе.

Таблица 13.2. Программы эмуляции терминала

Операционная система персонального компьютера	Программа
Windows 9x, NT, 2000 и XP	HyperTerminal (программа входит в стандартное программное обеспечение Windows), ProComm Plus
Windows 3.1	Terminal (программа входит в стандартное программное обеспечение Windows)
Macintosh	ProComm, VersaTerm, ZTerm

Практическое задание 13.2.4. Создание HyperTerminal-сеанса связи с маршрутизатором
В этом задании следует подсоединить рабочую станцию к маршрутизатору при помощи консольного кабеля, а также настроить и установить HyperTerminal-сеанс связи с машрутизатором.

Получение доступа к маршрутизатору

Для настройки машрутизатора Cisco администратор должен установить связь с устройством посредством терминального приложения или какого-нибудь средства удаленного доступа. Перед тем как выполнять какие-либо команды, администратор должен войти в систему.

В целях безопасности в маршрутизаторе предусмотрены два уровня доступа к командам, как показано в примере 13.14.

- **Пользовательский EXEC-режим.** Основным предназначением этого режима является проверка состояния маршрутизатора. В этом режиме запрещено изменение конфигурации маршрутизатора.
- **Привилегированный EXEC-режим.** Основным предназначением этого режима является изменение конфигурации маршрутизатора.

После входа в систему маршрутизатора выводится сообщение о том, что пользователь вошел в пользовательский EXEC-режим. Команды, доступные на этом уровне, являются подмножеством всех команд привилегированного режима. Таких команд вполне достаточно для просмотра параметров работы маршрутизатора без изменения его конфигурации.

Пример 13.14. Режимы работы маршрутизатора

```
Router> --------------- Пользовательский режим
Router>enable
Password:
Router# ---------------- Привилегированный режим
Router>disable
Router>
```

Для получения доступа к полному набору команд необходимо войти в привилегированный режим. Для этого в командной строке с приглашением “>” следует ввести команду **enable**. На запрос пароля нужно ввести пароль, который был задан с помощью команды **enable secret**. После успешного входа в привилегированный режим приглашение командной строки меняется на “#”. Из привилегированного режима может быть получен доступ к другим специальным режимам, включая следующие:

- режим конфигурирования интерфейса (`router(config-if)#`);
- режим конфигурирования подынтерфейса (`router(config-subif)#`);
- режим конфигурирования линии (`router(config-line)#`);
- режим конфигурирования маршрутизации (`router(config-router)#`);
- режим конфигурирования класса преобразования маршрутов (`router(config-map-class)#`).

Чтобы возвратиться в пользовательский режим, следует ввести команду **disable**. Для выхода из интерфейса командной строки операционной системы маршрутизатора введите команду **exit**. В зависимости от версии операционной системы маршрутизатора Cisco IOS и модели маршрутизатора будет выведена служебная информация.

Дополнительная информация: основы работы с операционной системой Cisco IOS

Операционная система Cisco Internetwork Operation System (IOS — межсетевая операционная система) реализована и используется во многих аппаратных устройствах, которые рассматриваются в обоих томах этого курса. Такая операционная система используется во всех маршрутизаторах корпорации Cisco.

Программное обеспечение Cisco IOS Software обеспечивает следующие сетевые службы в различных продуктах корпорации:

- службы обработки выбранных сетевых протоколов и функций;
- службы установления высокоскоростных соединений между сетевыми устройствами;
- безопасность управления доступом и предотвращение неавторизированного использования сети;
- масштабируемость при добавлении новых интерфейсов и возможность расширения сети;
- функции обеспечения надежного доступа к сетевым ресурсам.

Доступ к интерфейсу командной строки (CLI — Command Line Interface) операционной системы Cisco IOS может быть получен через консольное соединение посредством модемного соединения или же при помощи Telnet-сеанса. Вне зависимости от метода доступа к консоли операционной системы, обычно он называется EXEC-сеансом.

Вызов справочной информации в интерфейсе командной строки маршрутизатора

Как показано в примере 13.15, для просмотра списка всех доступных команд в пользовательском или привилегированном режиме в командной строке необходимо ввести знак вопроса <?>.

Обратите внимание на строку "`-- More --`", которая появляется внизу экрана. Одновременно на экране может быть отображено до 22 строк. И строка "`-- More --`" означает, что в выводимом списке команд присутствует больше одной страницы. При этом для просмотра следующей страницы необходимо нажать клавишу <пробел>. Чтобы отобразить следующую строку, следует нажать <Enter>. Для возвращения к командной строке нажмите любую другую клавишу.

ВНИМАНИЕ!

Список отображаемых команд зависит от контекста, т.е. от режима командной строки маршрутизатора. В зависимости от текущего режима, например, пользовательского или привилегированного режима конфигурирования интерфейса или режима глобальной конфигурации, будут отображены различные списки доступных команд.

Пример 13.15. Вызов справочной информации

```
?
Exec commands:
access-enable     Create a temporary Access-List entry
access-profile    Apply user-profile to interface
access-template   Create a temporary Access-List entry
archive           manage archive files
bfe               For manual emergency modes setting
cd                Change current directory
clear             Reset functions
clock             Manage the system clock
configure         Enter configuration mode
connect           Open a terminal connection
copy              Copy from one file to another
debug             Debugging functions (see also 'undebug')
delete            Delete a file
dir               List files on a filesystem
disable           Turn off privileged commands
disconnect        Disconnect an existing network connection
elog              Event-logging control commands
enable            Turn on privileged commands
erase             Erase a filesystem
exit              Exit from the EXEC
help              Description of the interactive help system

--More—
isdn             Make/disconnect an isdn data call on a BRI interface
lock              Lock the terminal
```

```
login              Log in as a particular user
logout             Exit from the EXEC
more               Display the contents of a file
mrinfo             Request neighbor and version information from
                         a multicast router
mrm                IP Multicast Routing Monitor Test
mstat              Show statistics after multiple multicast
                         traceroutes
mtrace             Trace reverse multicast path from destination
                         to source
name-connection    Name an existing network connection
no                 Disable debugging functions
pad                Open a X.29 PAD connection
ping               Send echo messages
ppp                Start IETF Point-to-Point Protocol (PPP)
pwd                Display current working directory
reload             Halt and perform a cold restart
resume             Resume an active network connection
rlogin             Open an rlogin connection
rsh                Execute a remote command
send               Send a message to other tty lines
setup              Run the SETUP command facility
show               Show running system information

--More—
slip               Start Serial-line IP (SLIP)
start-chat         Start a chat-script on a line
systat             Display information about terminal lines
telnet             Open a telnet connection
terminal           Set terminal line parameters
test               Test subsystems, memory, and interfaces
traceroute         Trace route to destination
tunnel             Open a tunnel connection
udptn              Open an udptn connection
undebug            Disable debugging functions (see also 'debug')
verify             Verify a file
where              List active connections
write              Write running configuration to memory, network,
                         or terminal
x28                Become an X.28 PAD
x3                 Set X.3 parameters on PAD
```

Для получения доступа к привилегированному режиму следует ввести команду **enable** или ее сокращенный вариант **ena**. После ввода этой команды будет выдан запрос на ввод пароля для доступа к привилегированному режиму. Для просмотра списка доступных команд привилегированного режима необходимо ввести знак вопроса <?> в командной строке (пример 13.16).

Пример 13.16. Команды привилегированного режима

```
Cisco# ?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  archive          manage archive files
  bfe              For manual emergency modes setting
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
  dir              List files on a filesystem
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  elog             Event-logging control commands
  enable           Turn on privileged commands
  erase            Erase a filesystem
  exit             Exit from the EXEC
  help             Description of the interactive help system
  --More—
```

Результаты введения команды **?** могут различаться[2] в зависимости от версии операционной системы Cisco IOS и конфигурации маршрутизатора.

Справочные функции маршрутизатора

Предположим, администратору необходимо настроить внутренние часы маршрутизатора. Если специалист не знает необходимой команды, то для получения информации о команде и ее синтаксисе он может воспользоваться интерактивной справкой маршрутизатора. В примере ниже проиллюстрировано одно из возможных применений справочной функции. Задача пользователя состоит в том, чтобы установить часы маршрутизатора. Предположим, команда ему не известна, поэтому для настройки часов необходимо будет выполнить действия, описанные ниже.

1. Чтобы найти правильную команду для установки внутренних часов маршрутизатора, воспользуйтесь командой **?**. В списке команд найдите команду **clock**.
2. Проверьте синтаксис команды для изменения времени.

[2] *Следует также обратить внимание на то, что количество доступных команд в привилегированном режиме в несколько раз больше, чем в режиме обычного пользователя. — Прим. ред.*

3. Необходимо установить текущее время: час, минуты и секунды. Если после ввода первого ключевого слова команды (**clock**) нажать возврат каретки, то операционная система выведет сообщение (`% Incomplete command.`) о том, что необходимо ввести дополнительную информацию. Интерактивная справка позволяет определить, что требуется дополнительно ввести ключевое слово **set** (пример 13.17).

Пример 13.17. Определение синтаксиса команды `clock set`

```
Cisco# clok
Translating "clok"...domain server (255.255.255.255)

% Unknown command or computer name, or unable to find computer address

Cisco# cl?
clear clock

Cisco# clock
% Incomplete command.

Cisco# clock ?
   set Set the time and date

Cisco# clock set
% Incomplete command.

Cisco# clock set ?
   hh:mm:ss Current Time
```

4. Введите время и дату в указанном формате. После указания двух ключевых слов и текущего времени операционная система опять выведет сообщение о том, что для установки времени требуется дополнительная информация (пример 13.18).

Пример 13.18. Установка системного времени и даты

```
Cisco# clock set 19:50:00
% Incomplete command.

Cisco# clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year

Cisco# clock set 19:50:00 14 7

                           ^
% Invalid input detected at '^' marker.

Cisco# clock set 19:50:00 14 July
% Incomplete command.
```

```
Cisco# clock set 19:50:00 14 July ?
<1993-2035> Year

Cisco# clock set 19:50:00 14 July 2003

Cisco#
```

1. Чтобы повторить введенную ранее команду, нажмите комбинацию клавиш **<Crtl>+<P>** или клавишу <↑> (стрелка вверх). После чего добавьте к команде пробел и знак вопроса **?**. После этого команда будет иметь завершенный вид.
2. Символ "^" указывает на то, что в команде допущена ошибка. Положение символа "^" указывает на возможное место ошибки. Чтобы определить правильный формат команды, следует ввести команду до такого места ошибки, а затем ввести знак вопроса **?**.
3. Введите год, используя правильный формат, и для завершения команды нажмите клавишу <Enter>.

Пользовательский интерфейс обеспечивает проверку синтаксиса команд, указывая местоположение ошибки посредством символа "^". Этот символ указывает на некорректную команду, ключевое слово или неправильный аргумент. Указатель на ошибку и интерактивная справочная система позволяют легко найти и исправить ошибки при интерактивном конфигурировании устройства.

Редактирование команд в операционной системе Cisco IOS

Интерфейс пользователя включает в себя усовершенствованный режим редактирования, позволяющий использовать набор функций редактирования, при помощи которых можно изменять текст, вводимый в командной строке. Для перемещения курсора, изменения или правки текста используются сочетания клавиш, показанные в табл. 13.3. Несмотря на то что стандартно при установке операционной системы усовершенствованный режим редактирования включен, его можно в любой момент отключить, в случае, если некоторые сценарии будут некорректно работать в этом режиме. Для отключения усовершенствования режима редактирования следует ввести команду **`terminal no editing`** в привилегированном режиме интерфейса командной строки маршрутизатора.

Зарезервированные комбинации клавиш для редактирования командной строки обеспечивают работу горизонтальной полосы прокрутки для команд, которые превышают длину экрана. Когда курсор достигает правой границы, то командная строка сдвигается на десять символов влево. При этом первые десять символов команды не будут видны, однако пользователь в любой момент может перейти к началу строки и проверить полный синтаксис команды. Для перехода на один символ влево нажмите сочетание клавиш <Ctrl>+<b>. Последовательное нажатие этого сочетания клавиш позволит вам перейти к началу команды. Соответственно, к концу команды можно вернуться при помощи сочетания клавиш <Ctrl>+<a>.

Таблица 13.3. Расширенные средства редактирования

Комбинация клавиш	Описание
<Ctrl>+<a>	Перемещение курсора в начало командной строки
<Ctrl>+<e>	Перемещение курсора в конец командной строки
<Esc>+<b>	Перемещение курсора назад на одно слово
<Ctrl>+<f>	Перемещение курсора вперед на один символ
<Ctrl>+<b>	Перемещение курсора на один символ назад
<Esc>+<f>	Перемещение курсора вперед на одно слово

ВНИМАНИЕ!

Большинство слушателей курсов и специалистов ленятся запоминать указанные в табл. 13.3 и 13.4 сочетания клавиш и пользуются только клавишами со стрелочками. Тем не менее, запоминать их нужно по двум причинам: первая — некоторые программы эмулирования терминала не поддерживают использование клавиш со стрелками, например, программы для установления Telnet-соединений в операционной системе DOS; вторая — в экзаменах на сертификат CCNA могут быть вопросы, которые проверяют знание таких команд. Проще всего для запоминания таких команд использовать только их для навигации по командной строке до тех пор, пока это не войдет в привычку.

В примере 13.19 показана команда, длина которой превышает размер экрана. Когда курсор достигает конца строки, строка смещается на десять символов влево и отображается с новой позиции. Символ “$” означает, что на экране отображается не полная строка, а лишь ее правая часть. Каждый раз при вводе команды, когда курсор достигает правой границы видимого изображения на экране, строка команды сдвигается на десять символов влево.

Пример 13.19. Команда, превышающая ширину экрана

```
Cisco>$ value for our customers, employees, investors, and partners
```

В зависимости от версии операционной системы Cisco IOS и конфигурации маршрутизатора, вид выводимой на экран информации может слегка изменяться.

Для выхода из режима настройки используется сочетание клавиш <Ctrl>+<z>. Эта комбинация возвращает пользователя в привилегированный EXEC-режим.

Журнал команд маршрутизатора

Интерфейс командной строки пользователя записывает журнал, или список команд, которые были введены пользователем. Эта функция особенно удобна при повторном вводе сложных либо длинных команд или выражений. Для журнала команд можно сконфигурировать следующие параметры:

- установить размер буфера журнала;
- включить повторный вызов команд;
- запретить ведение журнала команд.

Стандартно журнал команд ведется операционной системой, и в ее буфере хранятся последние десять команд, введенных пользователем. Для изменения количества команд, которые хранятся в буфере, используются команды **`terminal history size`** и **`history size`**. Максимальное количество команд, которые могут храниться в буфере, составляет 256. В табл. 13.4 перечислены команды и комбинации клавиш системного журнала введенных команд.

Таблица 13.4. Команды и комбинации клавиш системного журнала введенных команд маршрутизатора

Команда или комбинация клавиш	Описание
<Ctrl>+<p>	Это сочетание клавиш, а также клавиша <↑> (стрелка вверх), вызывают последнюю (предыдущую) введенную команду
<Ctrl>+<n>	Это сочетание клавиш, а также клавиша <↓> (стрелка вниз), вызывают первую введенную команду
`show history`	Отображает содержимое буфера команд
`terminal history` **`[size`** *`количество_строк`*`]`	Устанавливает размер буфера команд
`terminal no editing`	Отключает режим усовершенствованного редактирования
`terminal editing`	Включает режим усовершенствованного редактирования
<Tab>	Завершает выражение

Для повторного вызова команды, находящейся в буфере, начиная с самой последней введенной команды, нажмите комбинацию клавиш <Ctrl>+<p>. Продолжайте нажимать их до тех пор, пока не найдете необходимую вам команду. Для возвращения к более новым командам после нажатия сочетания клавиш <Ctrl>+<p> используется сочетание клавиш <Ctrl>+<n>.

При вводе команд можно использовать функцию автоматического завершения команды. Для этого нужно ввести несколько уникальных для команды первых символов, после чего нажать клавишу <Tab>. Если введенные первые символы команды однозначно определяют ее (т.е. больше никакая другая команда не начинается с этой комбинации символов), то маршрутизатор автоматически подставит недостающую часть названия команды.

В большинстве компьютеров доступны функции выделения и копирования текста. Все команды маршрутизатора могут быть скопированы, а затем вставлены в текущую командную строку.

Практическое задание 2.2.9. Основы работы с командной строкой
В этом задании необходимо войти в систему маршрутизатора в пользовательском и привилегированном режимах. Для определения настроек маршрутизатора придется использовать некоторые основные команды операционной системы. Кроме того, вы ознакомитесь со справочными средствами операционной системы маршрутизатора, а также научитесь использовать журнал команд и расширенные средства редактирования командной строки.

Интерактивная презентация: журнал команд маршрутизатора
В этой презентации показано, как правильно использовать комбинации клавиш в процессе работы с журналом команд маршрутизатора.

Поиск и исправление ошибок в командной строке

Ошибки в командной стоке обычно появляются в результате элементарных опечаток. Если команда или ключевое слово введены неправильно, то интерфейс командной строки пользователя сигнализирует об ошибке с помощью символа "^". Этот символ выводится строкой ниже именно в том месте, где найдена ошибка в команде, ключевом слове или аргументе. Такой индикатор значительно облегчает поиск и исправление ошибок в командной строке.

```
router#clock set 13:32:00 23 February 04
                                      ^
% Invalid input detected at '^' marker.
```

Символ "^" указывает, что неправильно введен аргумент "04". Чтобы проверить правильность синтаксиса, следует ввести команду до того места командной строки, в котором указана ошибка, и ввести знак вопроса (?).

```
router#clock set 13:32:00 23 February ?
  <1993-2035>  Year

router#clock set 13:32:00 23 February
```

Далее следует ввести правильную команду и нажать клавишу <Return> (или <Enter>, возврат каретки).

```
router#clock set 13:32:00 23 February 2004
```

Если команда была введена неправильно и интерфейс командной строки сообщает об ошибке, можно вызвать команду заново с помощью клавиши <↑> и удалить неправильный аргумент команды либо с помощью стрелочек "влево" и "вправо" на клавиатуре перейти к ошибке и исправить ее "вручную".

Команда show version

Команда **show version** выводит информацию о версии операционной системы IOS, выполняемой в данный момент на маршрутизаторе. В информации также присутствует значение регистров настройки и параметры загрузочного поля. С помощью этой команды можно получить информацию о:

- версии операционной системы Cisco IOS и ее краткое описание;
- версии загрузочной программы ПЗУ;
- версии урезанной операционной системы в ПЗУ;
- времени непрерывной работы маршрутизатора;
- последнем методе перезапуска маршрутизатора;
- имени образа системного файла и его месторасположении;
- номере аппаратной платформы маршрутизатора;
- настройках конфигурационных регистров.

Резюме

В этой главе были рассмотрены следующие ключевые понятия:

- процедура установления сеанса связи HyperTerminal;
- вход в систему маршрутизатора;
- использование справочной функции маршрутизатора в командной строке;
- использование расширенного режима редактирования команд;
- использование журнала команд;
- устранение неполадок в работе операционной системы Cisco IOS;
- маршрутизатор может загружаться в режиме ROM-монитора, загрузки из ПЗУ или в режиме операционной системы Cisco IOS;
- команды **show version** и **show flash** отображают информацию об операционной системе Cisco IOS, а также значения конфигурационного регистра и информацию об устройстве Flash-памяти;
- в пользовательском, привилегированном, режиме глобальной конфигурации и в специальных режимах команды вводятся при помощи интерфейса командной строки (CLI).

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Ключевые термины

Cisco IOS (Internetwork Operating System, Cisco IOS — межсетевая операционная система корпорации Cisco). Программное обеспечение межсетевой операционной системы корпорации Cisco обеспечивает функциональность, расширяемость и безопасность всех аппаратных продуктов. Программное обеспечение хранится в виде образа во Flash-памяти, загружается в оперативную память устройства и обеспечивает его работу и выполнение всех необходимых функций.

Интерфейс командной строки (Command-Line Interface — CLI) — интерфейс, который позволяет пользователям взаимодействовать с операционной системой посредством ввода специализированных команд и их аргументов.

Дочерняя плата (daughter card) подобна платам расширения, однако получает доступ непосредственно к компонентам маршрутизатора (памяти и центральному процессору) вместо использования медленной шины расширения.

Flash-память (flash memory) — это энергонезависимое запоминающее устройство, содержимое которого стирается и перепрограммируется по мере необходимости целыми блоками, а не отдельными байтами. Flash-память была разработана корпорацией Intel и лицензирована для использования другими производителями полупроводниковых приборов. Этот тип памяти широко используется в современных персональных компьютерах в качестве устройства BIOS, поскольку позволяет обновить версию записанного в устройство программного обеспечения. Микросхемы Flash-памяти также зачастую используются в модемах, поскольку позволяют производителям оборудования обеспечить поддержку новых протоколов, по мере того как они становятся стандартными.

Светодиодный индикатор (Light-Emitting Diode — LED) — полупроводниковое устройство, которое способно излучать свет при подаче на него напряжения. Обычно используется для отображения состояния в аппаратных устройствах.

NVRAM (NonVolatile RAM — энергонезависимая память) — оперативное запоминающее устройство, содержимое которого сохраняется при отключении питания.

Самотестирование при включении питания (Power-On Self-Test — POST) — набор диагностических средств, которые проверяют функционирование аппаратуры при включении питания.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Как инициализируется маршрутизатор?

а) Загружает содержимое памяти NVRAM, запускает процедуру начальной настройки и операционную систему.

б) Выполняет программу начальной загрузки, загружает операционную систему и файл конфигурации.

в) Выполняет программу начальной загрузки, запускает процедуру начальной настройки, загружает операционную систему.

2. В процессе работы с диалогом начальной настройки маршрутизатора какое сочетание клавиш используется для прерывания диалога?

а) <Ctrl>+<A>.

б) <Ctrl>+<E>.

в) <Ctrl>+<C>.

3. Выберите правильную пару параметров, которые нужно установить для создания HyperTerminal-сеанса.

а) BAUD	None.
б) DATA BITS	1.
в) PARITY	8.
г) STOP BITS	9600.
д) FLOW CONTROL	None.

4. Какое из выражений правильно описывает информацию, выводимую при начальной загрузке маршрутизатора?

а) Версию операционной системы Cisco IOS маршрутизатора из такой информации определить невозможно.

б) Версию операционной системы Cisco IOS маршрутизатора из такой информации можно определить.

5. Какое из выражений правильно описывает информацию, выводимую при начальной загрузке маршрутизатора?

а) Информация об объеме Flash-памяти устройства присутствует.

б) Информация об объеме Flash-памяти устройства отсутствует.

6. Какие команды правильно соответствуют описаниям?

а) <Ctrl>+<a> — выход из режима конфигурации.

б) <Ctrl>+<b> — перемещение курсора назад на одно слово.

в) <Ctrl>+<e> — перемещение курсора в конец командной строки.

г) <Ctrl>+<f> — перемещение курсора в начало командной строки.

д) <Esc>+<b> — перемещение курсора вперед на один символ.

е) <Esc>+<f> — перемещение курсора вперед на одно слово.

7. Какие команды правильно соответствуют описаниям?

а) <Tab> — включает режим усовершенствованного редактирования команд.

б) <Ctrl>+<p> — устанавливает размер буфера команд.

в) <Ctrl>+<n> — вызывает последнюю команду.

г) `show history` — показывает буфер команд.

д) `terminal history size #` — вызывает последнюю команду.

е) `terminal editing` — завершает выражение.

ж) `no terminal editing` — отключает режим расширенного редактирования команд.

8. Какой из методов маршрутизатор использует для загрузки операционной системы Cisco IOS?

а) Определяет в энергонезависимой памяти указания на источники резервных копий, чтобы использовать их при загрузке программного обеспечения.

б) Настраивает образ операционной системы Cisco IOS для использования ее в качестве программы начальной загрузки.

в) Ручная загрузка образа операционной системы через стандартно используемый виртуальный терминал.

г) Ручная загрузка образа операционной системы со стандартно используемого сетевого сервера.

9. Что из перечисленного ниже не является параметром загрузки, который может быть установлен в загрузочном поле конфигурационного регистра?

а) Загрузка Cisco IOS в режиме ROM-монитора.

б) Автоматическая загрузка Cisco IOS из ПЗУ.

в) Автоматическая загрузка Cisco IOS с Web-сервера.

г) Проверка NVRAM-памяти на наличие команд загрузки системы **`boot system`**.

10. Какая информация отображается операционной системой Cisco IOS при выполнении команды **`show version`**?

а) Подробная статистика о каждой странице памяти маршрутизатора.

б) Имя операционной системы.

в) Имя и размер всех файлов во Flash-памяти.

г) Состояние настроенных сетевых протоколов.

11. Какие из следующих показателей ограничивают выбор версии операционной системы Cisco IOS?

а) Оперативная память.

б) Flash-память.

в) TFTP-сервер.

г) Программа начальной загрузки.

12. Какая команда или комбинация клавиш используется для выхода из режима конфигурации?

а) **`exit`**.

б) **`no config-mode`**.

в) <Ctrl>+<e>.

г) <Ctrl>+<z>.

13. Как должно выглядеть приглашение командной строки при настройке интерфейса?

а) **`router(config)#`**.

б) **`router(config-in)#`**.

в) **`router(config-intf)#`**.

г) **`router(config-if)#`**.

14. Какая аббревиатура используется для обозначения пользовательского интерфейса операционной системы Cisco IOS?

а) CLI.

б) TCP/IP.

в) OSPF.

г) OSI.

15. Какие два режима доступа к командам операционной системы маршрутизатора Cisco существуют?

а) Пользовательский и привилегированный.

б) Пользовательский и гостевой.

в) Привилегированный и гостевой.

г) Гостевой и анонимный.

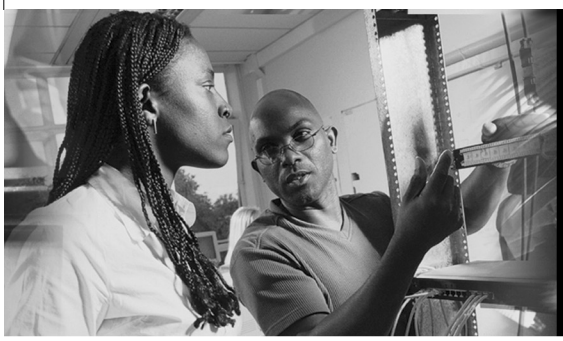
16. В каком режиме необходимо производить изменение конфигурации маршрутизатора Cisco?

а) Пользовательском.

б) Привилегированном.

в) Режиме администратора.

г) Root.



ГЛАВА 14

Настройка маршрутизаторов

В этой главе...

- описано, какие команды используются для присвоения имени маршрутизатору;
- рассказано, как установить пароли в маршрутизаторе;
- объясняется, для чего используются различные варианты команды **show**;
- перечислены команды и указана последовательность их использования при конфигурировании последовательного интерфейса;
- перечислены команды и указана последовательность их использования при конфигурировании Ethernet-интерфейса;
- рассказано, как произвести изменения в конфигурации маршрутизатора;
- описано, как сохранить изменения в конфигурации маршрутизатора;
- описаны команды, которые используются для описания интерфейса;
- указаны команды для конфигурирования приветственного сообщения и описана последовательность их применения;
- указаны команды, с помощью которых конфигурируется таблица узлов для устройства;
- рассказано, зачем необходима резервная документация;
- описана процедура восстановления паролей в устройстве.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

интерфейс, с. 667,

привилегированный режим, с. 667,

режим глобальной конфигурации, с. 670,

память NVRAM, с. 671,

простейший протокол передачи файлов, с. 683.

В этой главе рассматриваются режимы работы маршрутизатора и методы обновления файла конфигурации, а также основы операционной системы Cisco IOS и процедуры, которые необходимо выполнить для запуска маршрутизатора. Кроме этого, в главе рассматривается процедура восстановления забытых паролей маршрутизатора.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Конфигурирование маршрутизатора

Чтобы получить доступ к маршрутизатору, необходимо иметь соответствующую учетную запись. После того как администратор получил доступ к интерфейсу устройства, он может войти в один из возможных режимов конфигурирования устройства. Средства интерфейса командной строки должны интерпретировать команды, вводимые в каждом из режимов, и выполнять соответствующие им операции. Существуют два режима работы с командной строкой IOS-устройства:

- пользовательский;
- привилегированный.

В следующих разделах подробно описаны оба режима работы маршрутизатора и перечислены основные команды, которые в них используются.

Режимы интерфейса командной строки

Дополнительная информация: список команд пользовательского режима

При первом входе в систему пользователь-администратор автоматически попадает в пользовательский режим. Этот режим используется для ограниченной проверки маршрутизатора. В табл. 14.1 показаны команды пользовательского режима и представлены их описания.

Список команд привилегированного режима

Привилегированный режим обеспечивает детальную проверку маршрутизатора и позволяет вносить изменения в его конфигурацию. Этот режим используется в случае необходимости внесения изменений в конфигурацию маршрутизатора. Из привилегированного режима администратор может перейти во все остальные режимы маршрутизатора. Перед тем как перейти в другие режимы конфигурирования маршрутизатора, необходимо войти в привилегированный режим (более подробную информацию об этом вы сможете найти в разделе “Режимы конфигурации маршрутизатора”).

ВНИМАНИЕ!

Следует отметить, что список команд зависит от текущего режима маршрутизатора. Так, список команд пользовательского режима отличается от списка команд привилегированного режима, а список доступных команд в *режиме настройки глобальной конфигурации* отличается от списка режима *интерфейса*.

Таблица 14.1. Команды пользовательского режима

Команда	Описание
access-enable	Создание временной записи в списке доступа
atmsig	Выполнение команды ATM
cd	Переход на другое устройство хранения
clear	Сброс функций
connect	Создание терминального соединения
dir	Вывод списка файлов данного устройства
disable	Выход из привилегированного режима
disconnect	Отключение от устройства (в сетевом соединении)
enable	Переход в привилегированный режим
exit	Выход из интерфейса командной строки
help	Вызов интерактивной справочной системы
lat	Установление LAT-соединения
lock	Блокировка терминала
login	Вход в систему в качестве определенного пользователя
logout	Выход из режима настройки (отсоединение)
mrinfo	Запрос информации о соседних многоадресатных маршрутизаторах и их версии
mstat	Вывод статистики множественных многоадресатных трассировок маршрутов
mtrace	Трассировка обратного многоадресатного маршрута от получателя к отправителю
name-connection	Именование существующего сетевого соединения
pad	Открытие X.29 PAD-соединения
ping	Отправка пакетов эхо-тестирования
ppp	Запуск двухточечного протокола IETF (PPP)
pwd	Отображение текущего устройства
resume	Возвращение к работе с активным сетевым соединением
rlogin	Создание **rlogin**-соединения

Окончание табл. 14.1

Команда	Описание
show	Отображение информации о системе
slip	Запуск протокола SLIP
systat	Отображение информации о терминальных линиях
telnet	Создание telnet-соединения
terminal	Установка параметров терминальной линии
tn3270	Открытие TN3270-соединения
traceroute	Трассировка маршрута к получателю
tunnel	Создание тоннельного соединения
where	Список активных соединений
x3	Установка параметров X.3 сборщика/разборщика пакетов (PAD)
xremote	Вход в режим **Xremote**

Для доступа к *привилегированному режиму* (privileged mode) из пользовательского EXEC-режима введите команду **enable** (или ее сокращенный вариант **en**):

```
Router>enable
Password:

Router>en
Password:
```

После ввода команды будет запрошен пароль. Если в привилегированном режиме в командной строке вы введете символ **?**, то будет выведен длинный список доступных команд этого режима. В табл. 14.2 перечислены некоторые команды и даны их описания.

Следует отметить, что список команд может отличаться и зависит от используемой платформы маршрутизатора.

Таблица 14.2. Команды привилегированного режима

Команда	Описание
access-enable	Создание временной записи в списке доступа
access-template	Создание временной записи в списке доступа
appn	Отправка команды APPN-подсистеме
atmsig	Выполнение сигнальной ATM-команды
bfe	Ручная установка вспомогательного режима

Продолжение табл. 14.2

Команда	Описание
calendar	Управление аппаратным календарем
cd	Изменение текущего устройства
clear	Сброс функций
clock	Управление системными часами
cmt	Запуск или остановка функций управления соединением FDDI
configure	Вход в режим конфигурации маршрутизатора
connect	Создание терминального соединения
copy	Копирование конфигурационных данных или образа операционной системы
debug	Использование отладочных функций (см. также **undebug**)
delete	Удаление файла
dir	Получение списка файлов на текущем устройстве
disable	Выход из привилегированного режима
disconnect	Отключение всех существующих сетевых соединений
enable	Переход в привилегированный режим
erase	Очистка Flash-памяти или удаление конфигурации
exit	Выход из EXEC-режима
format	Разметка устройства
help	Получение информации при помощи интерактивной справочной системы
lat	Создание LAT-соединения
lock	Блокировка терминала
login	Вход в систему с атрибутами указанного пользователя
logout	Выход из EXEC-режима
mbranch	Многоадресатная трассировка маршрутов вниз по ветвям дерева
mrbranch	Многоадресатная трассировка вверх по ветвям дерева
mrinfo	Запрос информации у ближайших многоадресатных маршрутизаторов информации об их версии

Продолжение табл. 14.2

Команда	Описание
mstat	Отображение статистики после множественных многоадресатных трассировок
mtrace	Трассировка обратного многоадресатного маршрута от получателя к отправителю
name-connection	Именование существующего сетевого соединения
ncia	Запуск или остановка NCIA-сервера
pad	Создание X.29 PAD соединения
ping	Отправка эхо-запроса
ppp	Запуск двухточечного протокола IETF (PPP)
pwd	Отображение текущего устройства
reload	Остановка работы и выполнение “холодного” перезапуска
resume	Возвращение в активное сетевое соединение
rlogin	Создание **rlogin**-соединения
rsh	Выполнение удаленной команды
sdlc	Отправка проверочного фрейма SDLC
send	Передача сообщения через **tty**-линию
setup	Выполнение диалога начальной настройки системы **setup**
show	Отображение информации о работающей системе
slip	Запуск протокола SLIP
squeeze	Включение сжатия для устройства
start-chat	Запуск сценария на линии
systat	Отображение информации о терминальных линиях
tarp	Получение целевого идентификатора команд (Target ID Resolution Process)
telnet	Создание telnet-соединения
terminal	Установка параметров терминальной линии
test	Проверка подсистем, памяти и интерфейсов
tn3270	Создание соединения TN3270

Окончание табл. 14.2

Команда	Описание
traceroute	Трассировка маршрута к получателю
tunnel	Создание туннельного соединения
undebug	Отключение функций отладки (см. также **debug**)
undelete	Восстановление удаленного файла
verify	Проверка контрольной суммы Flash-файла
where	Список активных соединений
which-route	Поиск в таблице маршрутов OSI и отображение результатов
write	Запись файлов конфигурации в память, сеть или терминал
x3	Установка параметров X.3 устройства PAD
xremote	Вход в режим **Xremote**

Режимы конфигурации маршрутизатора

Чтобы применить настройки, которые оказывают влияние на всю систему, нужно воспользоваться командами глобальной конфигурации. Для входа в режим глобальной конфигурации используется команда привилегированного режима **configure**. После ввода этой команды будет запрошен источник команд конфигурации: можно будет выбрать терминал, энергонезависимое ОЗУ или сеть. Стандартно все команды конфигурации принимаются из консоли терминала. Для выбора этого режима конфигурирования достаточно нажать клавишу <Enter>.

Первый режим конфигурирования также называется режимом глобальной конфигурации, или коротко — глобальной конфигурацией. В табл. 14.3 показаны некоторые режимы конфигурирования маршрутизатора, доступ к которым можно получить из режима глобальной конфигурации.

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

В примере 14.1 проиллюстрировано переключение между различными режимами маршрутизатора.

Таблица 14.3. Режимы конфигурирования маршрутизатора

Режим	Приглашение командной строки
Интерфейс	`Router(config-if)#`
Подынтерфейс	`Router(config-subif)#`
Контроллер	`Router(config-controller)#`
Список преобразования	`Router(config-map-list)#`
Класс преобразования	`Router(config-map-class)#`
Линия	`Router(config-line)#`
Маршрутизатор	`Router(config-router)#`
IPX-маршрутизатор	`Router(config-ipx-router)#`
Преобразование маршрутизации	`Router(config-route-map)#`

Пример 14.1. Переход в привилегированный режим, режим глобальной конфигурации и специальные режимы настройки

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

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

Дополнительная информация: режимы начальной загрузки маршрутизатора

При доступе к маршрутизатору через консоль или посредством telnet-соединения маршрутизатор может находиться в одном из нескольких режимов. Каждый из указанных ниже режимов обеспечивает выполнение определенных функций.

- **Мониторинг с загрузкой из ПЗУ (ROM monitor)** — режим восстановления системы. Он позволяет выполнять такие задачи: восстановление утраченных паролей, загрузку новой версии программного обеспечения (IOS). Если маршрутизатор не обнаруживает корректный образ операционной системы в случае прерывания нормального хода загрузки, он входит в этот режим. В большинстве маршрутизаторов стандартно в режиме мониторинга с загрузкой из ПЗУ используется приглашение командной строки такого вида: `Rommon>`.
- **Режим начального конфигурирования (setup mode)** предоставляет пользователю интерактивный диалог, который помогает задать базовую первоначальную конфигурацию

маршрутизатора. Этот режим, по сути, является серией вопросов к пользователю, после которых в скобках указаны стандартные ответы. В режиме установки отсутствует приглашение командной строки. Если маршрутизатор не находит корректный файл начальной конфигурации, он предлагает пользователю перейти в режим установки. Также в этот режим можно попасть, набрав команду **`setup`** в привилегированном режиме. Следует отметить, что попасть в режим установки можно и вручную, очистив содержимое энергонезависимого ОЗУ (память NVRAM) и перезагрузив устройство.

- **Режим RXBoot** является специальным вспомогательным режимом, в котором можно изменить содержимое конфигурационных регистров и перезагрузить маршрутизатор. Режим `RXBoot` обеспечивает загрузку подмножества версий операционной системы Cisco IOS, а также вход в *дополнительный режим настройки* (streamlined setup mode). Дополнительный режим настройки отличается от стандартного тем, что в нем невозможно изменять глобальные параметры маршрутизатора. В дополнительном режиме настройки можно изменить параметры интерфейсов, с использованием которых маршрутизатору позволяется загружаться. Таким образом, настройка этих интерфейсов позволит маршрутизатору загрузить операционную систему даже в том случае, если во Flash-памяти не будет обнаружен корректный образ операционной системы Cisco IOS Software. Стандартно в этом режиме используется приглашение командной строки следующего вида: `<boot>`.

В табл. 14.4 кратко описаны команды, наиболее часто используемые для конфигурирования маршрутизатора.

Таблица 14.4. Команды, используемые для конфигурирования маршрутизатора

Команда	Описание
`configure terminal`	Ручная настройка из консоли терминала
`configure memory`	Загрузка информации о конфигурации из энергонезависимого ОЗУ (NVRAM)
`copy tftp running-config`	Загрузка информации о конфигурации из сетевого TFTP-сервера в ОЗУ
`show running-config`	Отображение текущей конфигурации, которая находится в ОЗУ
`copy running-config startup-config`	Сохранение текущей конфигурации из ОЗУ в энергонезависимое ОЗУ
`copy running-config tftp`	Сохранение текущей конфигурации из ОЗУ на сетевом TFTP-сервере
`show startup-config`	Отображение конфигурации, сохраненной в энергонезависимом ОЗУ
`erase startup-config`	Очистка содержимого энергонезависимого ОЗУ

Для работы с маршрутизатором с операционной системой Cisco IOS версии 11.0 или младше используйте команды, приведенные на рис. 14.1.

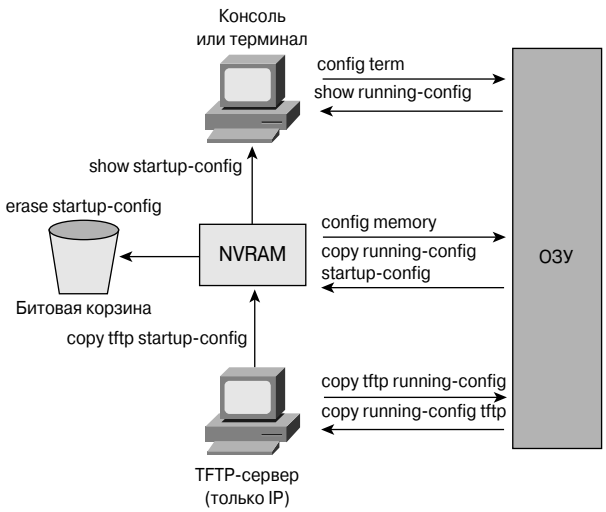


Рис. 14.1. Команды для настройки маршрутизатора

Настройка имени маршрутизатора

Одной из основных задач, которые необходимо решить при установке маршрутизатора, является задание его имени, как показано в примере 14.2.

Пример 14.2. Задание имени маршрутизатора

```
Router(config)#hostname SunDevils
SunDevils(config)#
```

Именование маршрутизатора позволяет повысить удобство администрирования сети. Имя маршрутизатора задается в *режиме настройки глобальной конфигурации* (global configuration mode), оно называется именем узла (hostname) и отображается в системном приглашении командной строки. Если пользователем не задано имя маршрутизатора, то по умолчанию используется имя `Router`.

Практическое задание 14.1.2. Режимы интерфейса командной строки и идентификация маршрутизатора

Это практическое задание поможет изучить основные пользовательские и привилегированные режимы маршрутизатора. Также ознакомьтесь с основными командами каждого из режимов. В дополнение задайте имя маршрутизатора.

Настройка защиты маршрутизатора паролями

Для защиты маршрутизатора от несанкционированного доступа используются пароли. Пароли могут быть установлены на доступ к виртуальной линии терминала

и к линии консоли. Также паролем может быть защищен привилегированный EXEC-режим.

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

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

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

Для установки пароля к сеансу telnet-связи используется команда **line vty 0 4**. В примере 14.3 показаны различные пути настройки и защиты пароля.

Пароль, заданный командой **enable secret,** не может быть прочитан; другой пользователь, получивший доступ к файлам конфигурации, может лишь перезаписать его, но никак не прочитать, поскольку для хранения пароля используется необратимое, одностороннее шифрование, что исключает восстановление пароля. Для запрета отображения пароля в виде открытого текста может быть использована команда **service password-encryption**. Ее следует вводить в режиме глобальной конфигурации. Эта команда действует на все пароли, кроме того, который был указан с помощью команды **enable secret**, поскольку он и так уже зашифрован. Команда **service password-encryption** позволяет зашифровать все пароли: привилегированного и непривилегированного пользователей, пароли доступа к консоли, через терминальные соединения, пароли линий и др.

Пример 14.3. Настройка защиты с помощью паролей

```
! Пароль консоли
Router(config)# line console 0
Router(config-line)# login
Router(config-line)# password Cisco
! Пароль виртуального терминала
Router(config)# line vty 0 4
```

```
Router(config-line)# login
Router(config-line)# password Cisco
! Пароль для доступа к привилегированному режиму
Router(config)# enable password san-fran
! Шифрование пароля
Router(config)# enable secret [пароль]
! Шифрование всех паролей
Router(config)# service password-encryption

! Отмена шифрования всех паролей
Router(config)# no service password-encryption
```

Практическое задание 14.1.3. Настройка паролей маршрутизатора
Это практическое задание поможет освоить команды настройки паролей для подключения к консоли, виртуальному терминалу и пароля доступа к привилегированному режиму.

Команды группы show

В маршрутизаторе существует большое количество типов команды **show**, которые позволяют просмотреть содержимое файлов; такие команды очень полезны при решении проблем в работе маршрутизатора. В каждом из режимов команда **show ?** отображает допустимые параметры команды. В табл. 14.5 приведен список некоторых параметров команды **show**.

Таблица 14.5. Список параметров команды show

Команда	Описание
show interfaces	Отображает статистику обо всех интерфейсах маршрутизатора. Если пользователю необходимо проанализировать статистические данные конкретного интерфейса, он может указать в команде **show interfaces** номер соответствующего интерфейса. Например: **Router# show interfaces serial 1**
show controllers serial	Отображает информацию об аппаратных средствах маршрутизатора
show clock	Отображает время, которое установлено в маршрутизаторе
show hosts	Отображает список кэшированных имен узлов и адресов
show users	Отображает список пользователей, подключенных к маршрутизатору
show history	Отображает журнал введенных команд
show flash	Отображает информацию о Flash-памяти и о файлах операционной системы Cisco IOS, хранимых в ней
show version	Отображает информацию об образе операционной системы Cisco IOS Software, которая находится в ОЗУ (RAM)

Окончание табл. 14.5

Команда	Описание
`show arp`	Отображает ARP-таблицу маршрутизатора
`show protocol`	Отображает глобальное состояние и состояние интерфейсов любого настроенного протокола третьего уровня
`show startup-configuration`	Отображает конфигурацию, сохраненную в энергонезависимом ОЗУ (NVRAM)
`show running-configuration`	Отображает конфигурацию, которая в настоящее время находится в ОЗУ (RAM)

В примерах 14.4-14.6 проиллюстрировано использование команд **`show protocol`**, **`show version`** и **`show interfaces`**.

Пример 14.4. Результат выполнения команды `show protocol`

```
Router# show protocols
Global values:
Internet Protocol routing is enabled
DECnet routing is enabled
XNS routing is enabled
Vines routing is enabled
AppleTalk routing is enabled
Novell routing is enabled
--More--
Ethernet0 is up, line protocol is up
Internet address is 183.8.126.2, subnet mask is 255.255.255.128
DECnet cost is 5
XNS address is 3010.aa00.0400.0284
CLNS enabled
Vines metric is 32
AppleTalk address is 3012.93, zone ld-e0
Novell address is 3010.aa00.0400.0284
--More—
```

Пример 14.5. Результат выполнения команды `show version`

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-J-M). Version 12.1.5
Copyright (c) 1986-1996 by Cisco Systems, Inc.
Compiled Fri 28-Jun-96 16:32 by rbeach
Image text-base: 0x600088A0, data-base: 0x6076E000
ROM: System Bootstrap, Version 5.1(1) RELEASE SOFTWARE (fc1)
ROM: 4500-XBOOT Bootstrap Software, Version 10.1(1) RELEASE SOFTWARE (fc1)
router uptime is 1 week, 3 days, 32 minutes
System restarted by reload
System image file is c4500-j-mz, booted via tftp from 171.69.1.129
--More--
```

Пример 14.6. Результат выполнения команды `show interfaces`

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

Практическое задание 14.1.4. Использование команд группы `show`

Это практическое задание ознакомит вас с командами маршрутизатора **`show`**. Команды **`show`** являются наиболее важными для получения информации о работе и состоянии маршрутизатора.

Настройка последовательного интерфейса

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

В последовательном соединении двух устройств одно из них должно быть объявлено DCE-устройством (т.е. передающим) и должно обеспечивать передачу синхронизирующих сигналов. Включение таймера синхронизации и его скорость задаются командой **`clockrate`**. Существуют такие возможные скорости передачи в битах в секунду: 1200, 2400, 9600, 19 200, 38 400, 56 000, 64 000, 72 000, 125 000, 148 000, 500 000, 800 000, 1 000 000, 1 300 000, 2 000 000 и 4 000 000. Однако некоторые устройства, в зависимости от их структуры, могут поддерживать не все скорости передачи данных.

Для настройки последовательного интерфейса необходимо выполнить действия, указанные ниже (пример 14.7).

Этап 1. Войти в режим глобальной конфигурации.

Этап 2. Войти в режим настройки требуемого интерфейса.

Этап 3. Сконфигурировать IP-адрес для интерфейса и маску подсети.

Этап 4. Указать полосу пропускания канала (необязательный этап)

Этап 5. Установить частоту синхронизирующих импульсов передающего (DCE) устройства (для принимающего устройства DTE этот этап следует пропустить).

Этап 6. Включить интерфейс.

Пример 14.7. Настройка последовательного интерфейса

```
Router# configure terminal
Router(config)# interface serial 1/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# bandwidth 56
Router(config-if)# clockrate 56000
Router(config-if)# no shutdown
```

Стандартно все интерфейсы отключены. Для включения интерфейса необходимо ввести команду **no shutdown**. Иногда интерфейсы необходимо отключить для проведения технического обслуживания аппаратных средств, изменения конфигурации интерфейса, устранения проблем в работе или проведения других регламентных действий. В этом случае для отключения интерфейса может использоваться команда **shutdown**.

Следующая команда отключает интерфейс:

```
Router(config-if)# shutdown
```

Указанная ниже команда включает отключенный интерфейс.

```
Router(config-if)# no shutdown
```

Для выхода из текущего режима настройки интерфейса используется такая команда:

```
Router(config-if)# exit
```

Практическое задание 14.1.6. Настройка последовательного интерфейса
В этом практическом задании необходимо настроить последовательные интерфейсы в двух маршрутизаторах таким образом, чтобы они смогли связаться друг с другом.

Внесение изменений в конфигурацию маршрутизатора

Для внесения изменений в конфигурацию маршрутизатора необходимо войти в соответствующий режим и произвести эти изменения. Например, если какой-либо интерфейс отключен, то для его включения необходимо войти в режим глобальной

конфигурации, затем — в режим настройки интерфейса и выполнить команду **no shutdown**.

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

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

Для сохранения конфигурационных переменных в энергонезависимом ОЗУ в привилегированном режиме выполните такую команду:

```
Router# copy running-configuration startup-configuration
```

В табл. 14.6 приведен список команд, позволяющих управлять содержимым энергонезависимой памяти в операционной системе Cisco IOS версии 11.x и более поздних.

Таблица 14.6. Команды, используемые для управления содержимым энергонезависимого ОЗУ в операционной системе Cisco IOS версии 11.x и более поздних

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

Практическое задание 14.1.6. Внесение изменений в конфигурацию маршрутизатора
В этом практическом задании следует внести изменения в существующую конфигурацию маршрутизатора. Необходимо отключить интерфейс, запустить его снова и просмотреть его состояние.

Настройка Ethernet-интерфейса

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

Для настройки интерфейса Ethernet необходимо выполнить действия, указанные ниже (пример 14.8):

Этап 1. Войти в режим глобальной конфигурации.

Этап 2. Войти в режим настройки требуемого интерфейса.

Этап 3. Сконфигурировать IP-адрес для интерфейса и маску подсети.

Этап 4. Включить интерфейс.

Пример 14.8. Настройка Ethernet-интерфейса

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

Стандартно все интерфейсы отключены. Для их включения используется команда **no shutdown**. Иногда интерфейсы необходимо отключить для проведения технического обслуживания аппаратных средств, изменения конфигурации интерфейса, устранения проблем в работе или проведения других действий. В этом случае для отключения интерфейса может использоваться команда **shutdown**.

Практическое задание 14.1.7. Настройка Ethernet-интерфейса
В этом практическом задании необходимо настроить интерфейсы Ethernet или FastEthernet в маршрутизаторе для локальной сети.

Завершение настройки маршрутизатора

Ниже перечислены действия, которые рекомендуется выполнить для завершения настройки маршрутизатора. В некоторых организациях некоторые действия, возможно, и не понадобятся.

- Установка стандартов конфигурации.
- Создание описаний интерфейсов.
- Настройка сообщений, которые отображаются при входе в систему.
- Настройка MOTD-сообщений.
- Указание имени узла.
- Создание резервных копий конфигурационных файлов и документации.

Важность использования стандартизированных конфигураций

В пределах одной организации очень удобно разработать единый стандарт файлов конфигурации маршрутизаторов. В этот стандарт необходимо включить контроль над количеством конфигурационных файлов, способом и местом хранения этих файлов.

Стандарт должен определять набор правил или процедур, которые широко используются или заданы официально. Без единого принятого стандарта, особенно в крупной организации, в сети будет царить хаос в случае прерывания работы служб.

Для управления сетью должна существовать централизованная поддержка ее стандартов. Для нормальной работы сети ее настройка, обеспечение безопасности и другие параметры должны настраиваться согласованно друг с другом. Создание единых сетевых стандартов позволит избежать излишней сложности структуры сети и уменьшить незапланированное время ее простоя, а также выявить события, которые имеют наибольшее влияние на производительность всей сети в целом.

Создание описаний интерфейсов

Для идентификации важной информации, такой, как имя соседнего маршрутизатора, номера сети или определенного сетевого сегмента, следует использовать строку описания интерфейсов. Строка описания интерфейса позволит пользователю вспомнить особенную информацию о конкретном интерфейсе, например, о сетевых службах. В следующем разделе приведен конкретный пример создания и настройки текстового описания интерфейса маршрутизатора.

Описание интерфейса является всего лишь комментарием к интерфейсу и никак не влияет на его работу, хотя и находится в файле конфигурации. Описания создаются согласно специальному формату и могут включать в себя назначение и размещение интерфейса, описание других устройств, подключенных к этому интерфейсу, и содержать идентификатор сети. Описания позволяют обслуживающему маршрутизатор персоналу быстрее и эффективнее выяснять причины проблем и устранять их.

Настройка описаний интерфейсов

Для настройки строк-описаний интерфейсов войдите в режим глобальной конфигурации и выполните действия, описанные ниже (пример 14.9).

Этап 1. Войдите в режим глобальной конфигурации, набрав команду **`configure terminal`**.

Этап 2. Войдите в режим конфигурирования соответствующего интерфейса (например, интерфейса Ethernet 0), введя команду **`interface ethernet 0`**.

Этап 3. Введите ключевое слово **`description`**, а затем строку-описание интерфейса (например, **`XYZ Network, Building 10`**).

Этап 4. Выйдите из режима настройки интерфейса в привилегированный режим, нажав сочетание клавиш <Ctrl>+<Z>.

Этап 5. Сохраните изменения в энергонезависимой памяти, используя команду **`copy running-config startup-config`**.

Пример 14.9. Настройка строки-описания интерфейса

```
Router(config)# interface ethernet 0
Router(config-if)# description SkyDome LAN Communication Building
Router(config-if)# exit

! Результат указания описания для интерфейса Ethernet0 можно увидеть
с помощью команд группы show:

  description SkyDome LAN Communication Building
  ip address 198.133.215.1 255.255.255.0
```

Практическое задание 14.2.3. Настройка описаний интерфейсов
В этом практическом задании необходимо выбрать описание для интерфейса и в режиме настройки интерфейса ввести это описание.

Сообщение, отображаемое при входе в систему

Сообщением, отображаемым при входе в систему (login banner), называется надпись, которая выводится над строкой приглашения при входе в систему пользователя. Такой текстовый фрагмент может быть использован для передачи сообщений, которые относятся ко всем пользователям сети, например, сообщения о предстоящем выключении системы.

Сообщение, отображаемое при входе в систему, может быть прочитано любым пользователем. Поэтому при составлении такого сообщения следует придерживаться основных требований безопасности.

Сообщение, отображаемое при входе в систему, должно предупреждать пользователей о том, что в вход в систему невозможен без предварительной авторизации. Так, сообщение "**This is a secure system, authorized access only!**" (Это защищенная система, разрешен только авторизированный доступ!) предупреждает нежелательных пользователей о том, что любое неавторизированное вторжение является нелегальным. В примере 14.10 показано типичное сообщение, которое появляется при входе в систему.

Пример 14.10. Сообщение, отображаемое при входе в систему

```
Tokyo con0 is now available
Press RETURN to get started.


This is a secure system. Authorized Access ONLY!!!
User Access Verification
Password:
Tokyo>enable
Password:
Tokyo#
```

Настройка сообщения дня

Сообщение дня (Message Of The Day — MOTD) или сообщение, которое отображается при входе в систему, могут отображаться во всех подключенных терминалах.

Для настройки сообщения MOTD следует войти в режим глобальной конфигурации. Для ввода сообщения дня используется команда **`banner motd`**, после которой следует текст сообщения, выделенный символами пробела и "#", как показано в примере 14.11.

Для создания сообщения дня выполните описанные ниже действия.

Этап 1. Войдите в режим глобальной конфигурации, набрав команду **`configure terminal`**.

Этап 2. Введите команду **`banner motd # The message of the day goes here #`**.

Этап 3. Сохраните изменения, используя команду **`copy running-configuration startup-configuration`** или ее сокращенный вариант **`copy run start`**.

Пример 14.11. Настройка сообщения дня

```
Tokyo(config)# banner motd #
You have entered a secure system, authorized access ONLY! #
```

Практическое задание 14.2.5. Отображение сообщения дня
В этом практическом задании необходимо, используя режим глобальной конфигурации, ввести новость дня в маршрутизатор. Такая процедура позволит всем пользователям увидеть сообщение при входе в маршрутизатор.

Определение имени узла

Определением имени узла называется процесс, при котором компьютерная система ставит в соответствие сетевому адресу символьное имя узла.

Для идентификации сетевого устройства в протоколах и приложениях, например, таких, как **`telnet`** или **`ping`** или соответствующих им командах, используются имена сетевых узлов. Для того чтобы, используя сетевое имя, сетевое устройство могло взаимодействовать с другими IP-устройствами, такими, как маршрутизаторы, имена должны преобразовываться в IP-адреса и обратно. Список имен узлов и связанных с ними IP-адресов хранится в *таблице узлов* (host table). Таблица узлов может включать все устройства в сети организации. Каждому уникальному IP-адресу может соответствовать имя узла. Операционная система Cisco IOS выполняет кэширование таблицы узлов для использования в EXEC-командах. Кэширование позволяет значительно ускорить процесс преобразования имени в адрес.

Имя узла — это не доменное имя (DNS-имя), оно используется только в тех маршрутизаторах, которые настроены на его использование.

Чтобы настроить таблицу преобразования имен узлов устройства, следует выполнить описанные ниже действия.

Этап 1. Войдите в режим глобальной конфигурации, набрав команду **`configure terminal`**.

Этап 2. Введите команду **`ip host`** с нужными параметрами, которые включают в себя имя маршрутизатора и IP-адрес или адреса, установленные на интерфейсах соответствующего устройства.

Этап 3. Выполните этап 2 для всех устройств, которые необходимо включить в таблицу узлов.

Этап 4. Выйдите из режима глобального конфигурирования в привилегированный режим, нажав сочетание клавиш <Ctrl>+<Z>.

Этап 5. Сохраните изменения в энергонезависимой памяти, используя команду **`copy running-config startup-config`**.

Практическое задание 14.2.7. Настройка таблицы узлов
В этом практическом задании необходимо, используя режим глобальной конфигурации, создать таблицу узлов, которая позволит маршрутизатору транслировать имена узлов на каждом из интерфейсов.

Настройка резервного копирования и документация

Конфигурация сетевых устройств определяет их поведение и взаимодействие в сети. Управление конфигурацией устройств включает в себя такие действия:

- поддержание списка и сравнение файлов конфигурации действующих устройств;
- сохранение файлов конфигурации на сетевых серверах;
- установку программного обеспечения и его обновлений.

При возникновении проблем в работе маршрутизатора следует сделать резервные копии файлов конфигурации. Они могут создаваться на сетевом сервере, на *TFTP-сервере (Trivial File Transfer Protocol — простейший протокол передачи файлов*) или на диске, хранимом в надежном месте. В эти независимые копии также должна включаться документация.

Сохранить конфигурацию маршрутизатора можно также на жестком диске путем захвата текста конфигурации маршрутизатора. Такой файл конфигурации в дальнейшем можно передать на маршрутизатор посредством копирования блоков текста и вставки их в окно терминального приложения. Методы сохранения и восстановления конфигурации маршрутизатора рассматриваются в главе 16, “Управление программным обеспечением Cisco IOS”.

На рис. 14.2 показана блок-схема процесса настройки маршрутизатора.

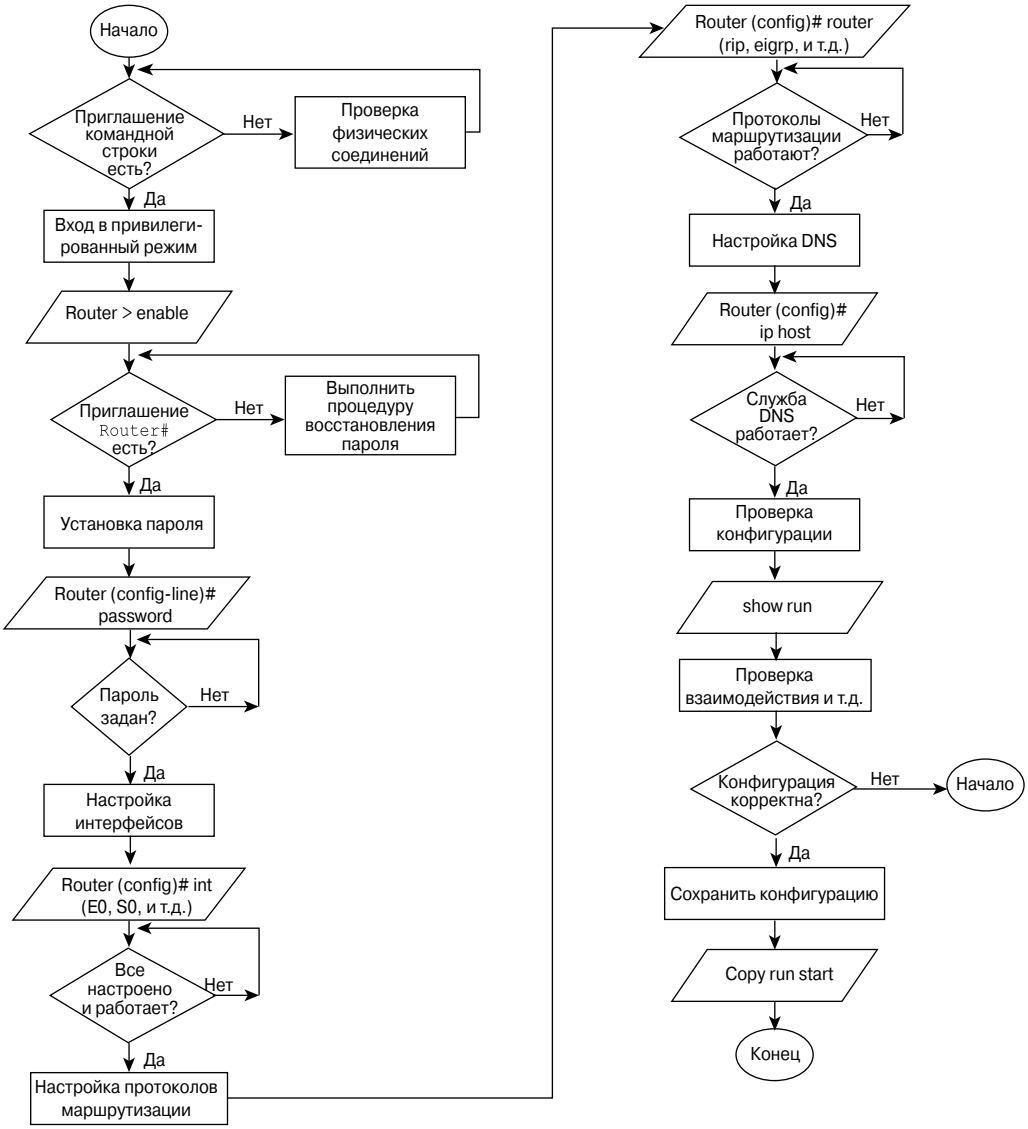


Рис. 14.2. Блок-схема процесса настройки маршрутизатора

Сохранение резервной копии конфигурационных файлов

Текущий вариант конфигурационного файла маршрутизатора может быть сохранен на TFTP-сервере, для чего используется команда **`copy running-config tftp`**. Чтобы сохранить конфигурационный файл на сервере, выполните действия, описание которых приводится ниже.

Этап 1. Выполните команду **`copy running-config tftp`**.

Этап 2. В ответ на запрос интерфейса командной строки операционной системы введите IP-адрес узла, на котором будет сохранена конфигурация.

Этап 3. Введите имя, которое будет присвоено файлу конфигурации при сохранении его на сервере.

Этап 4. Для подтверждения своего выбора ответьте несколько раз утвердительно на запросы системы.

Конфигурационный файл, который хранится на одном из сетевых серверов, может быть использован для конфигурирования устройства. Чтобы переписать файл с сетевого сервера, нужно выполнить указанные ниже действия.

Этап 1. Выполните команду **`copy tftp running-config`**.

Этап 2. В приглашении диалога интерфейса командной строки выберите узел или сетевой конфигурационный файл. Сетевой конфигурационный файл содержит набор команд, который применим ко всем маршрутизаторам и терминальным серверам в сети. В системном приглашении следует указать IP-адрес узла, на котором запущена служба TFTP. Например, в качестве адреса можно указать 10.10.1.2.

Этап 3. В системном приглашении следует ввести название конфигурационного файла либо принять стандартное значение. Стандартное имя имеет вид **`hostname-config`** (имя-узла-config) для узловой конфигурации и network-config (сеть-config) — для сетевой. В операционной системе DOS длина имени файла не может превышать восемь символов плюс три символа расширения файла (например, **`router.cfg`**). Подтвердите правильность введения адреса и названия файла и завершите процесс.

Конфигурация маршрутизатора также может быть сохранена на жестком диске любого компьютера посредством захвата текста из терминального приложения. Чтобы восстановить конфигурацию устройства заново или вставить в нее необходимые команды, можно воспользоваться функциями редактирования текста программы-эмулятора терминала.

Дополнительная информация: восстановление паролей

В этом разделе рассматриваются методы и средства восстановления паролей для маршрутизаторов Cisco и коммутаторов Catalyst. На большинстве платформ восстановить пароли можно без переключения перемычек на платах, однако такой процесс на всех системах обязательно включает в себя перезагрузку маршрутизатора. Восстановить пароли можно только при помощи порта консоли (физически подключенного к маршрутизатору).

Обзор методов восстановления паролей

Существуют три метода восстановления доступа к маршрутизатору в случае утраты пароля. Вы можете просмотреть пароль, изменить его или полностью очистить память, в которой хранится конфигурация.

Каждый из этих методов включает в себя основные действия, описанные ниже.

Этап 1. Настройте маршрутизатор таким образом, чтобы он не восстанавливал конфигурацию из энергонезависимой памяти (NVRAM). Такая конфигурация зачастую носит название тестового режима, режима загрузки из ПЗУ или boot-режима.

Этап 2. Перезагрузите систему.

Этап 3. Создайте временную запись в списке доступа (если регистры конфигурации были установлены корректно в пункте 1, это может быть сделано без пароля).

Этап 4. Просмотрите или измените пароль, либо очистите память маршрутизатора.

Этап 5. Настройте маршрутизатор на нормальный режим чтения энергонезависимой памяти при загрузке.

Этап 6. Перезагрузите систему.

Для восстановления некоторых паролей может понадобиться передача сигнала BREAK; для этого можно воспользоваться терминалом или ПК с эмулятором терминала. Например, в терминале ProComm нажатие сочетания клавиш <Ctrl>+<B> генерирует сигнал BREAK; в Windows-программе HyperTerminal для передачи сигнала BREAK следует нажать <Break> или комбинацию клавиш <Ctrl>+<Break>. Кроме того, программа HyperTerminal позволяет назначить функциональную клавишу для отправки сигнала BREAK. В окна терминала выберите пункт меню Функциональные клавиши и укажите комбинацию для отправки сигнала `Break`, введя символы ^$B (<Shift>+<6>, <Shift>+<4> и символ <B> в верхнем регистре). В сети Internet вы также сможете найти и другие бесплатно распространяемые программы эмуляции терминала и выбрать любую, оптимально соответствующую вашим требованиям.

В следующих разделах приведены подробные инструкции для определенных моделей маршрутизаторов Cisco. Перед тем как начать восстановление пароля в маршрутизаторе, определите его модель и следуйте соответствующей инструкции.

Метод восстановления пароля № 1

Этот метод восстановления пароля применим к маршрутизаторам Cisco таких моделей:

- серии 2500;
- серии 3000;
- серии 7000 с операционной системой Cisco IOS версии 10.0 или более поздней, которая установлена в ПЗУ.

Рассматриваемый метод может быть использован для маршрутизаторов Cisco 7000 и Cisco 7010 только в том случае, если в маршрутизаторе установлена ОС Cisco IOS на плате процессора маршрутизации (Router Processor — RP). Операционная система Cisco IOS также может быть загружена из Flash-памяти, однако она должна присутствовать в ПЗУ на плате процессора. Указанные ниже действия реализуют первый метод восстановления пароля.

Этап 1. Присоедините терминал или ПК с запущенной программой эмуляции терминала к порту консоли маршрутизатора. Для подсоединения ПК можно использовать нуль-модемный кабель (авторы этой книги использовали кабель Tandy Null Modem Adapter №26-1496). Подсоедините нуль-модемный кабель к порту консоли, а противоположную его сторону — к нуль-модемному адаптеру.

Этап 2. Введите команду **show version** и запишите значения конфигурационных регистров. Обычно они составляют **0x2102** или **0x102**. Если вы не получили доступа к командной строке маршрутизатора и у вас не получилось выполнить команду **show version**, то значения регистров конфигурации можно посмотреть в подобных моделях маршрутизаторов или попробовать использовать значение **0x2102**.

Этап 3. Выключите и включите маршрутизатор.

Этап 4. Нажмите и задержите в таком положении комбинацию клавиш **BREAK**-последовательности в терминале в течение 60 секунд после включения питания маршрутизатора. Вы должны увидеть приглашение командной строки > без названия маршрутизатора. Если приглашение не появилось, значит, скорее всего, терминал не отправляет корректный сигнал **BREAK** маршрутизатору. В таком случае проверьте терминал или настройки программы эмуляции терминала.

Этап 5. В командной строке введите команду **o/r 0x42** для загрузки из Flash-памяти или команду **o/r 0x41** для загрузки из ПЗУ (следует заметить, что первым символом команды является символ буквы **o**, а не цифры **0**). Если у вас есть Flash-память с образом операционной системы, то оптимальным решением будет загрузка именно с него. Стандартно используется именно загрузка с Flash-носителя. Команду **0x41** следует использовать только когда Flash-память очищена или же не установлена. Введя **0x41,** вы можете просмотреть или очистить конфигурацию маршрутизатора. Изменить пароль таким образом не удастся.

Этап 6. В командной строке с приглашением **>** введите команду **i**. При этом маршрутизатор перезагрузится и проигнорирует сохраненную конфигурацию.

Этап 7. На все вопросы диалога начальной установки отвечайте **no** или нажимайте <Ctrl>+<C>.

Этап 8. В приглашении командной строки вида **Router>** введите команду **enable**. Войдя в привилегированный режим, вы увидите приглашение командной строки вида **Router#**.

Этап 9. Выполните необходимое действие.

а) Для просмотра пароля введите команду **show start**.

б) Для изменения пароля (например, если старый пароль зашифрован) выполните следующее:

- серии 2500;
- серии 3000;
- серии 7000 с операционной системой Cisco IOS версии 10.0 или более поздней, которая установлена в ПЗУ.
- чтобы скопировать содержимое энергонезависимого ОЗУ в оперативную память, введите команду **copy start run**;
- выполните команду **show run**;
- если использовалось шифрование пароля, выполните такие действия:

  1) введите команду **config term** и внесите необходимые изменения;

  2) введите команду **enable secret** *новый_пароль*;

  3) нажмите комбинацию клавиш <Ctrl>+<Z.>;
- если вы не использовали команду **enable secret** *пароль*, то выполните команду **enable password** *новый_пароль* и нажмите комбинацию клавиш <Ctrl>+<Z>;

- для сохранения и подтверждения изменений введите команду **copy run start**.

Этап 10. Введите команду **config term** в интерфейсе командной строки.

Этап 11. Введите команду **config-register 0x2102** или значение, которое вы использовали в пункте 2.

Этап 12. Чтобы возвратиться в привилегированный режим, нажмите <Ctrl>+<Z>.

Этап 13. В командной строке введите **reload**. Записывать конфигурацию в память не обязательно.

Метод восстановления пароля №2

Этот метод восстановления пароля применим к маршрутизаторам Cisco таких моделей:

- 1003;
- серии 1600;
- серии 2600;
- серии 3600;
- серии 4500;
- серии 7100;
- серии 7200;
- серии 7500;
- маршрутизаторам, основанным на системе обнаружения вторжений (IDT) Orion;
- платформам AS5200 и AS5300.

Для восстановления пароля следует выполнить действия в той последовательности, в какой они указаны ниже.

Этап 1. Присоедините терминал или ПК с запущенной программой эмуляции терминала к порту консоли маршрутизатора.

Этап 2. Введите команду **show version** и запишите значения конфигурационных регистров. Обычно они составляют `0x2102` или `0x102`.

Значения конфигурационных регистров, как правило, выводятся в последней строке. Следует отметить, что конфигурационные регистры также позволяют разрешить или запретить обработку сигнала прерывания BREAK.

Стандартно в маршрутизаторе конфигурационный регистр имеет значение `0x2102`. Третий символ слева — `1`, он означает запрет сигнала прерывания BREAK. Если это значение не равно `1`, то сигнал BREAK разрешен.

Этап 3. Выключите маршрутизатор и включите его снова.

Этап 4. Нажмите клавишу или комбинацию клавиш для отправки сигнала прерывания в приложении терминала в течение 60-ти секунд после включения питания маршрутизатора. Вы должны увидеть приглашение командной строки > без названия маршрутизатора. Если приглашение не появилось, то, скорее всего, терминал не отправляет корректный сигнал прерывания BREAK маршрутизатору. В таком случае проверьте корректность работы терминала или настройки программы эмуляции терминала.

Этап 5. В командной строке введите команду **confreg**. Будет выдан такой запрос:

```
Do you wish to change configuration [y/n]?
```

(Вы хотите изменить конфигурацию [да/нет]?)

Этап 6. Введите “yes” (да) и нажмите клавишу <Enter> (возврат каретки).

Этап 7. На все последующие вопросы отвечайте “no” (нет) до появления вопроса:

```
ignore system config info [y/n]?
```

(Игнорировать информацию о конфигурации системы [да/нет]?).

Этап 8. Выберите “yes” (да).

Этап 9. На все последующие вопросы отвечайте “no” (нет) до появления вопроса:

```
change boot characteristics [y/n]?
```

(Изменить характеристики загрузки [да/нет]?).

Этап 10. Выберите “yes” (да). Будет получен такой запрос:

```
enter to boot:
```

Этап 11. На этот запрос для загрузки из Flash-памяти введите 2 или, если Flash-память очищена, введите 1.

Если содержимое Flash-памяти уничтожено, то маршрутизатор Cisco 4500 должен быть возвращен в сервисный центр компании Cisco. Если вы введете 1, то сможете лишь только просмотреть или очистить конфигурацию; пароль в этом случае не может быть изменен.

После завершения настройки будет выдан такой запрос:

```
Do you wish change configuration [y/n]?
```

(Вы хотите изменить конфигурацию [да/нет]?).

Этап 12. Введите “no” (нет) и нажмите клавишу <Enter>.

Этап 13. Введите команду **`reset`** в привилегированном режиме или, для маршрутизаторов серии Cisco 4500 и Cisco 7500, выключите и снова включите питание маршрутизатора.

Этап 14. После загрузки маршрутизатора на все вопросы отвечайте “no” (нет) до появления приглашения командной строки вида

```
Router>
```

Этап 15. Для входа в привилегированный режим выполните команду **`enable`**. Будет выдано приглашение командной строки вида `Router#`.

Этап 16. Выберите один из следующих пунктов:

- чтобы просмотреть пароль, если он не зашифрован, введите команду **`more nvram:startup-config`**;
- чтобы изменить пароль (например, в том случае, если он зашифрован), введите такую последовательность команд:

```
Router# configure memory
Router# configure terminal
Router(config) enable secret 1234abcd
! Нажмите комбинацию клавиш ctrl-z
Router# write memory[1]
```

Команда **`enable secret`** обеспечивает дополнительную безопасность путем

[1] *Эта команда считается устаревшей и реализована в новых версиях операционной системы для совместимости со старыми вариантами. Она может быть убрана из любой последующей версии операционной системы, поэтому рекомендуется использовать команду* **`copy running startup`**. *— Прим. ред.*

сохранения пароля с использованием необратимых криптографических функций; однако, если вы забудете зашифрованный пароль, то восстановить его будет практически невозможно.

Этап 17. В командной строке введите команду **`configure terminal`**.

Этап 18. Введите команду **`congif-register`** и значение, которое вы использовали в пункте 2.

Этап 19. Нажмите комбинацию клавиш <Ctrl>+<Z> для выхода из режима редактирования конфигурации.

Этап 20. Наберите на клавиатуре команду **`reload`**, а затем **`write memory`** для сохранения конфигурации.

Резюме

В этой главе были рассмотрены ключевые моменты настройки маршрутизаторов:

- маршрутизатор может работать в одном из следующих режимов:
  - пользовательском;
  - привилегированном;
  - режиме глобальной конфигурации;
  - других режимах конфигурирования;
- для изменения конфигурации маршрутизатора используется интерфейс командной строки (CLI), который позволяет выполнить такие действия:
  - установить имя узла;
  - задать пароли;
  - настроить интерфейсы;
  - изменить конфигурацию маршрутизатора;
  - отобразить текущую конфигурацию маршрутизатора;
- описания интерфейсов маршрутизатора должны включать важную информацию, которая помогает администраторам решать проблемы, возникающие при работе сети;
- сообщение, которое отображается при входе в систему, и сообщение дня предназначены для передачи информации пользователям, работающим с маршрутизатором;
- благодаря таблице узлов имя узла может быть быстро преобразовано маршрутизатором в IP-адрес;

- существуют три метода получения доступа к маршрутизатору в случае утраты пароля:
  - можно просмотреть пароль;
  - можно изменить пароль;
  - можно очистить конфигурацию маршрутизатора и заново установить систему;
- стандартизация конфигураций маршрутизаторов в пределах одного предприятия существенно повышает эффективность работы и обслуживания этой сети. Кроме того, очень важен процесс создания резервных копий конфигураций и документации маршрутизаторов.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Ключевые термины

Интерфейс командной строки (Command Line Interface — CLI) — интерфейс, который позволяет пользователю взаимодействовать с операционной системой путем ввода команд и их параметров.

Интерфейс представляет собой соединение между двумя системами или устройствами. В терминологии маршрутизаторов интерфейс — это сетевое соединение.

Привилегированный режим используется для копирования и выполнения других действий с файлами конфигурации и настройки устройства.

Протокол TFTP представляет собой упрощенную версию протокола FTP, которая позволяет передавать по сети файлы от одного устройства другому, обычно без использования аутентификации клиента (без пользовательского имени и пароля).

Режим глобальной конфигурации (global configuration mode) используется для введения команд в одной строке и команд, которые вносят изменения в глобальную конфигурацию маршрутизатора.

Энергонезависимая память (non-volatile random access memory — NVRAM, энергонезависимое ОЗУ) — это ОЗУ, которое сохраняет данные после отключения питания.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Что такое стандарт?
   а) Формальный набор правил и соглашений, которые описывают процесс обмена информацией между сетевыми устройствами.
   б) Набор правил и процедур, которые часто используются или утверждены официально.
   в) Путь, по которому сетевые устройства получают доступ к сетевой среде.
2. Что такое описание интерфейса?
   а) Приглашение-сообщение для пользователей маршрутизатора.
   б) Предупредительное сообщение для пользователей маршрутизатора.
   в) Содержит строку-комментарий для интерфейса маршрутизатора.
3. Хорошим примером сообщения, отображаемого пользователю при входе в систему, является:
   а) Добро пожаловать всем.
   б) Пожалуйста, для входа в систему введите имя и пароль.
   в) Разрешен только авторизированный доступ.
4. Что представляет собой определение имени узла?
   а) Процесс соотнесения имени с сетевым адресом.
   б) Процесс отображения сообщения о входе в систему.
   в) Процесс отображения описания маршрутизатора.
5. Создание резервных копий конфигурации и документации маршрутизаторов необходимо для обеспечения нормальной работы сети?
   а) Да.
   б) Нет.
6. Создание резервных копий файлов конфигурации не обязательно?
   а) Да.
   б) Нет.
7. TFTP-сервер является только хранилищем резервных копий файлов?
   а) Да.
   б) Нет.
8. Если вы хотите произвести настройку интерфейса, то как должно выглядеть приглашение командной строки?
   а) `router(config)#`
   б) `router(config-in)#`
   в) `router(config-intf)#`
   г) `router(config-if)#`

9. Какой из следующих списков содержит правильную последовательность действий, необходимых для настройки маршрутизатора? (Предполагается, что уже были выполнены какие-то изменения в режиме конфигурирования).

а) Сохранение изменений в резервные копии, решение о том, какие изменения необходимо внести в конфигурацию и какие необходимо получить результаты, проверка результатов и резервных файлов.

б) Проверка результатов, решение о том, какие изменения необходимо внести в конфигурацию и какие необходимо получить результаты, сохранение изменений в резервных копиях.

в) Решение о том, какие изменения необходимо внести в конфигурацию и какие необходимо получить результаты, проверка резервных копий, сохранение изменений в резервных копиях и проверка результатов.

г) Проверка результатов, сохранение изменений в резервных копиях, решение о том, какие изменения необходимо внести в конфигурацию и какие необходимо получить результаты и проверка резервных файлов.

10. Какая из команд используется для сохранения изменений в конфигурации маршрутизатора в резервной копии?

а) `Router# copy running-config ftp`

б) `Router# show running-config`

в) `Router# config mem`

г) `Router# copy tftp running-config`

11. Какое из утверждений не соответствует процессу настройки пароля маршрутизатора?

а) Пароль может быть задан в любом режиме работы маршрутизатора.

б) Пароль может быть задан в любой консоли терминала.

в) Для пароля, задаваемого командой `enable secret`, используется шифрование, в отличие от обычного пароля.

г) Любая установка пароля начинается в режиме глобальной конфигурации.

12. Команды какого режима используются для изменения главных настроек маршрутизатора?

а) Режима глобальной конфигурации.

б) Привилегированного режима.

в) Пользовательского EXEC-режима.

г) Режима настройки интерфейса.

13. Что делает команда **`exit`** в режиме конфигурации с приглашением командной строки `Router(config-if)#`?

а) Выходит из текущего режима настройки интерфейса.

б) Переходит к командной строке привилегированного EXEC-режима.

в) Выходит из маршрутизатора.

г) Переключает в пользовательский EXEC-режим.

14. Какие элементы являются основными элементами типичной конфигурации маршрутизатора?

а) Пароль, интерфейсы, протокол маршрутизации, DNS.

б) Последовательность загрузки, интерфейсы, TFTP-сервер, энергонезависимое ОЗУ (NVRAM).

в) Энергонезависимое ОЗУ (NVRAM), ПЗУ (ROM), динамическое ОЗУ (DRAM), интерфейсы.

г) Интерфейсы, протоколы маршрутизации, регистры конфигурации, Flash-память.

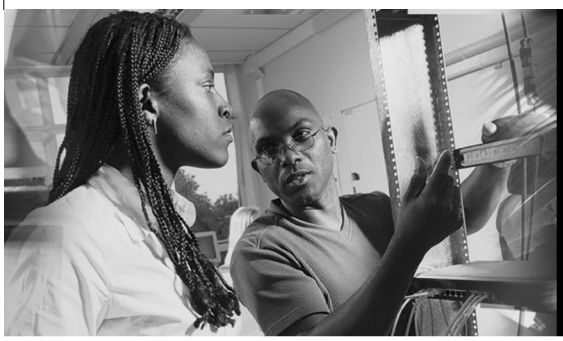
15. В процедуре восстановления пароля сразу же после нажатия клавиш <Ctrl>+<Break> (или другой комбинации, которая прерывает загрузку) во время загрузки маршрутизатора какое значение находится в регистре конфигурации?

а) `0x2102.`

б) `0x2142.`

в) `0x0000.`

г) `0x10F.`



ГЛАВА 15

Получение информации о соседних устройствах

В этой главе...

- описано, как включить протокол CDP, производить мониторинг и поддерживать его работу;
- рассмотрен процесс создания карты сети протоколом CDP;
- приведены команды для отключения протокола CDP, поиска и устранения в нем неисправностей;
- объясняется, зачем необходимо подключаться к другим маршрутизаторам с помощью telnet-службы;
- перечислены команды, которые позволяют проверить, отсоединить или приостановить telnet-соединение;
- указано, как выполнить альтернативную проверку межсетевого взаимодействия;
- рассмотрены примеры применения команды **`show cdp neighbors`**;
- описано, как определить, какое соседнее устройство к какому именно локальному интерфейсу подключено;
- описано, как протокол CDP собирает информацию об адресах соседних устройств;
- рассмотрены методы поиска и устранения неисправностей для удаленных терминальных соединений.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

протокол обнаружения устройств Cisco, с. 698,
протокол доступа к подсети, с. 698,
простой протокол сетевого управления, с. 699,
тип-длина-значение, с. 701,
ping, с. 706,
traceroute, с. 706,
telnet, с. 706,
команда отладки, с. 716.

В этой главе рассмотрены вопросы внедрения, мониторинга и поддержания работоспособности протокола Cisco Discovery Protocol (CDP) при помощи соответствующих команд маршрутизатора. Кроме того, в главе рассмотрены основные команды, предназначенные для восстановления работоспособности маршрутизатора.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Обнаружение соседних устройств и подключение к ним

Иногда сетевые специалисты сталкиваются с нештатной ситуацией и при этом обнаруживают, что документация сети неполная или составлена неаккуратно. Протокол CDP (Cisco Discovery Protocol — протокол обнаружения устройств Cisco) в такой ситуации будет бесценным инструментом сетевого администратора, поскольку он поможет построить базовую схему структуры сети. Несмотря на то что этот протокол показывает информацию исключительно только о непосредственно подключенных к данному узлу соседних устройствах, он все же представляет собой очень мощное средство отладки сети.

Введение в CDP

Протокол обнаружения устройств Cisco (Cisco Discovery Protocol — CDP) работает на канальном уровне, который объединяет физическую среду передачи данных нижнего уровня с протоколами верхних сетевых уровней (рис. 15.1). Протокол CDP используется для получения информации о соседних сетевых устройствах корпорации Cisco. Получаемая информация включает в себя типы подключенных устройств, интерфейсы маршрутизатора, к которым соседние устройства подключены, интерфейсы, использующиеся для создания соединений, а также модели устройств. Протокол CDP не зависит от среды передачи и от протоколов, работает с любым оборудованием корпорации Cisco и в качестве своей основы использует *протокол доступа к подсети* (SNAP — Subnetwork Access Protocol). CDP является собственным протоколом сетевых устройств Cisco и работает только с сетевыми устройствами, выпущенными компанией Cisco.

Самой последней версией протокола CDP является версия 2 (CDPv2). Поддержка протокола CDPv2 уже включена в операционную систему Cisco IOS Software версии 12.0(3)T и более поздние. Стандартно во всех операционных системах Cisco IOS версий, начиная с 10.3, доступен протокол CDP версии 1 (CDPv1).

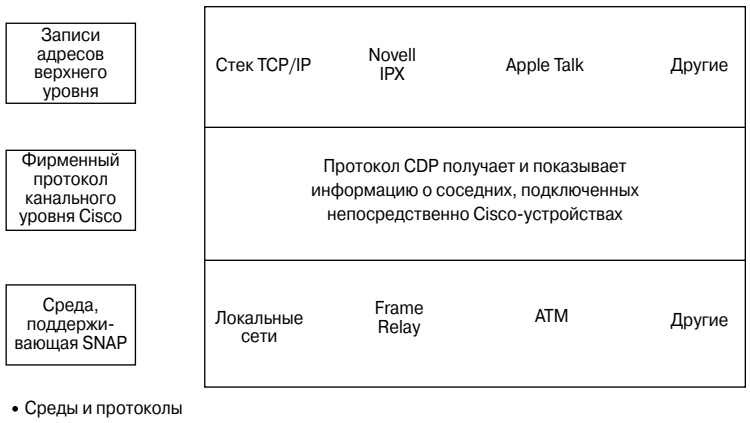


Рис. 15.1. Расположение протокола CDP

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

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

Информация, которую можно получить через протокол CDP

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

Дополнительная информация: отображение CDP-записи

Как показано в примере 15.1, для отображения одной кэшированной записи CDP используется команда `show cdp entry` *[имя устройства]*.

Пример 15.1. Использование команды `show cdp entry`

```
routerA# show cdp entry routerB
-------------------------------
Device ID: routerB
Entry address(es):
IP address: 198.92.68.18
Platform: 2501. Capabilities: Router
Interface: Ethernet), Port ID (outgoing port): Ethernet0
Holdtime: 155 sec

--- Часть информации удалена ---
```

Обратите внимание, что результат выполнения указанной в примере команды включает в себя все адреса уровня 3 соседнего маршрутизатора, RouterB. Введя команду на маршрутизаторе A, администратор имеет возможность получить информацию об IP-адресах соседнего маршрутизатора B. Параметр времени удержания информации определяет время, в течение которого хранится CDP-фрейм, полученный от соседнего устройства. Сжатую информацию о соседнем маршрутизаторе RouterB можно получить, введя команду `show cdp entry` *[имя устройства]*. Информация о версии и параметрах соседних устройств упростит специалисту процесс определения физической топологии сети и поможет оптимально настроить устройства.

Отображение CDP-информации о соседних устройствах

На рис. 15.2 показано, как протокол CDP позволяет администратору получить полезную информацию о системе. Каждый маршрутизатор, на котором исполняется протокол CDP, обменивается со своими соседями информацией обо всех известных ему протоколах. Администратор может посмотреть результаты этого обмена CDP-информацией посредством консоли, подсоединенной к локальному маршрутизатору.

Для отображения информации о сетях, непосредственно подсоединенных к маршрутизатору, можно воспользоваться командой **`show cdp neighbors`**. Протокол CDP обеспечивает получение информации о каждом соседнем устройстве путем передачи информации в формате *TLV (Type Length Value — запись тип-длина-значение*). Записи TVL — это блоки информации, внедренные в CDP-анонсы.

Значения TVL конкретного устройства могут быть просмотрены путем использования команды **`show cdp neighbors`** и, как показано в примере 15.2, включают в себя такую информацию:

- идентификатор устройства;
- номер и тип локального интерфейса;
- время удержания информации;

- возможности устройства[1];
- платформу;
- идентификатор порта;
- доменное имя VTP (только в случае использования протокола CDPv2);
- номер собственной сети VLAN (только в случае использования протокола CDPv2);
- информацию о дуплексности соединения (только в случае использования протокола CDPv2).

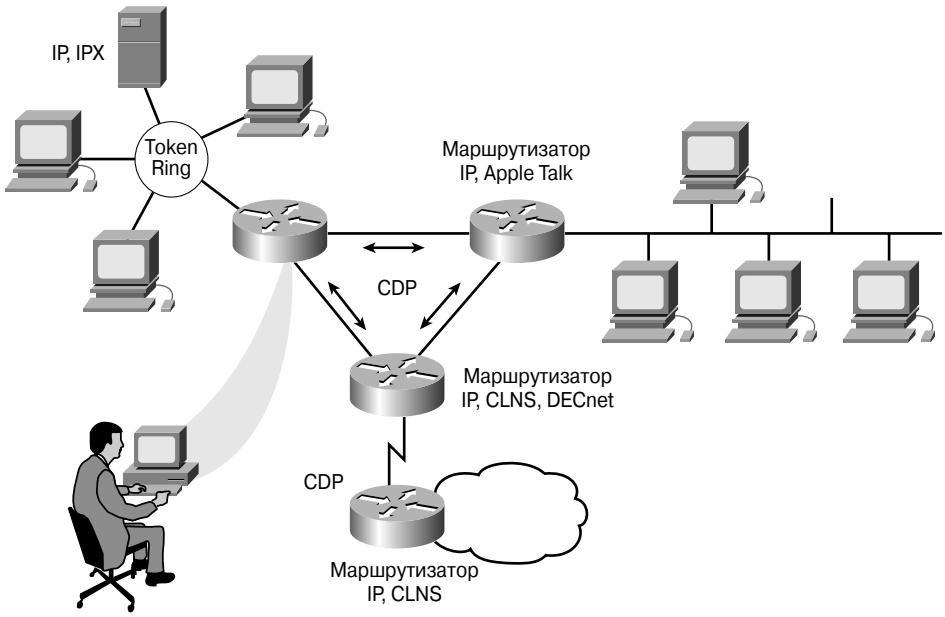


Рис. 15.2. Получение CDP-информации о соседних устройствах

Пример 15.2. Выводимая командой `show cdp neighbors` информация

```
routerA# show cdp neighbors
Capability Codes:
R — Router, T — Trans Bridge,
B — Source Route Bridge,
S — Switch, H — Host, I — IGMP

Device ID   Local Interface    Holdtime    Capability   Platform  Port    ID
routerB     Eth 0              151           R           2501      Eth    0
routerB     Ser 0              165           R            2501     Ser    0
```

[1] *Код, который указывает, является ли соседнее устройство маршрутизатором или же коммутатором. — Прим. ред.*

Для отображения всей информации, выводимой командой **show cdp neighbors**, например, как в случае команды **show cdp entry**, вы можете использовать указанную команду с дополнительным ключом **show cdp meighbors detail**, как показано в примере 15.3.

Пример 15.3. Выводимая командой show cdp neighbors информация

```
routerA# show cdp neighbors detail
Device ID: routerB
Entry address(es):
  IP address: 198.92.68.18
Platform: 2501, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): Ethernet0
Holdtime: 143 sec
```

Обратите внимание, что самый нижний маршрутизатор на рис. 15.2 непосредственно не соединен с маршрутизатором, к которому подключена консоль администратора. Для получения информации об этом маршрутизаторе администратору необходимо создать telnet-соединение с устройством, которое непосредственно к нему подключено. Как было сказано выше, информация об обсуждаемом протоколе поможет получить полное представление об устройствах, которые работают в сети, что даст более полное понимание физической топологии сети.

Включение протокола, мониторинг и получение CDP-информации

Для включения протокола CDP, получения и отслеживания CDP-информации используются команды, приведенные в табл. 15.1.

Таблица 15.1. Основные команды протокола CDP

Команда	Режим	Описание
`cdp run`	Режим глобальной конфигурации	Включает протокол CDP в маршрутизаторе
`cdp enable`	Режим настройки интерфейса	Разрешает использование протокола CDP на интерфейсе
`clear cdp counters`	Привилегированный EXEC-режим	Сбрасывает все счетчики переданных данных в начальное состояние
`show cdp`	Привилегированный EXEC-режим	Отображает интервалы между передачей CDP-анонсов, промежуток времени в секундах, в течение которого CDP-анонс будет действителен для данного порта, а также версию текущего анонса

Окончание табл. 15.1

Команда	Режим	Описание
show cdp entry [*entry-name* **[protocol|version]**	Привилегированный EXEC-режим	Отображает информацию об указанном соседнем устройстве. Результат ее выполнения может быть ограничен выводом информации только о протоколе или о версии
show cdp interface [*type number*]	Привилегированный EXEC-режим	Отображает информацию об интерфейсах, на которых разрешен CDP
show cdp neighbors [*type number*] **[detail]**	Привилегированный EXEC-режим	Отображает тип устройства, о котором получена информация, имя устройства, количество и тип локальных интерфейсов (портов), промежуток времени, в течение которого CDP-анонсы действительны для данного порта, тип устройства, серийный номер устройства и идентификатор порта. Если добавить в команду ключевое слово **detail**, то команда выдает информацию об идентификаторе собственной виртуальной сети (VLAN ID), о режиме дуплексности и доменном имени протокола VTP, которое установлено на соседнем устройстве

Для включения протокола CDP на маршрутизаторе используется команда **cdp run**. Для включения протокола CDP только на отдельном интерфейсе используется команда **cdp enable**. В операционной системе Cisco IOS версии 10.3 и более поздних протокол CDP может быть включен отдельно для каждого интерфейса с помощью команды **cdp enable**. Несмотря на то что стандартно протокол CDP выполняется на большинстве устройств Cisco, администратор может столкнуться с экземплярами, на которых придется вручную запустить его для каждого интерфейса. В качестве примера таких устройств можно привести коммутаторы серии 1900, которые не поддерживают команду **cdp run**. Для коммутаторов этой серии разрешать или запрещать протокол CDP нужно отдельно для каждого интерфейса. В качестве другого примера можно привести интерфейсы, в которых протокол CDP отключен в целях безопасности.

Дополнительная информация: команда show cdp interface

Чтобы получить информацию о сведениях, которые протокол CDP использует для анонсов, и о передаче фреймов, нужно использовать команду **show cdp interface**. В примере 15.4 проиллюстрировано использование этой команды. Выводимая информация помогает получить такие сведения, как время удержания информации, частота передачи CDP-пакетов, инкапсуляция на интерфейсе, состояние протокола на интерфейсе.

Пример 15.4. Выводимая командой `show cdp interface` информация

```
routerA# show cdp interface
Serial 0 is up, line protocol is up, encapsulation is Frame Relay
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
   Sending CDP packets every 60 seconds
   Holdtime is 180 seconds
```

Создание карты сети

Протокол CDP разрабатывался как простой, легкий в применении, не требующий больших ресурсов. Поскольку CDP-фрейм может быть очень маленьким, от соседних маршрутизаторов может запрашиваться большое количество полезной информации.

Команда **`show cdp neighbors`** может быть использована для получения следующей информации:

- идентификатора устройства;
- адреса;
- идентификатора порта;
- возможностей устройства;
- аппаратной платформы;
- префикса IP-сети (IP Network Prefix);
- доменного имени протокола VTP (только в случае использования протокола CDPv2);
- номера собственной сети VLAN (только в случае использования протокола CDPv2);
- информации о режиме дуплексности (только в случае использования CDPv2).

Все это позволяет создать карту сети объединенных устройств. Для получения информации об устройствах, подсоединенных к соседним устройствам, может использоваться telnet-подключение. Более подробную информацию о подключенных устройствах можно получить при помощи команды **`show cdp neighbors detail`**.

Практическое задание 15.1.4. Создание карты сети
В этом практическом задании необходимо, используя CDP-команды, получить информацию о соседних сетях и маршрутизаторах.

Отключение протокола CDP

Как было отмечено выше, стандартно протокол CDP запущен на большинстве маршрутизаторов. Для отключения протокола во всем устройстве используется команда **`no cdp run`** в режиме глобальной конфигурации. Если протокол CDP будет

запрещен этой командой, то невозможно будет включить его на отдельном интерфейсе. Например, администратор может глобально отключить протокол CDP из соображений безопасности, для того чтобы никто не смог получить информацию об этом устройстве.

В операционной системе Cisco IOS версии 10.3 или более поздних стандартно протокол CDP отключен для каждого из интерфейсов. Для его включения, чтобы интерфейсы могли принимать и отправлять CDP-сообщения, необходимо использовать команду **`cdp enable`**. Для отключения протокола CDP, после того как он был разрешен, следует использовать команду **`no cdp enable`** в соответствующем режиме конфигурации интерфейса.

Устранение неисправностей в протоколе CDP

В табл. 15.2 приведен список команд, которые используются для просмотра версии, обновления информации, получения информации о таблицах и потоке данных.

Таблица 15.2. Команды для устранения неполадок в работе протокола CDP

Команда	Описание
`clear cdp table`	Удаляет таблицу CDP-информации о соседних устройствах
`clear cdp counters`	Сброс счетчика потока данных в начальное состояние
`show cdp traffic`	Отображение значения CDP-счетчика, включая количество принятых и отправленных пакетов, а также ошибок контрольной суммы
`show debugging`	Отображение информации о типах отладки, включенных в маршрутизаторе
`debug cdp adjacency`	Отображение CDP-информации о соседних устройствах
`debug cdp events`	Отображение информации о CDP-событиях
`debug cdp ip`	Отображение сведений о CDP IP-информации
`debug cdp packets`	Отображение информации о CDP-пакетах
`cdp timers`	Определяет, как часто операционная система Cisco IOS будет отправлять CDP-обновления
`cdp holdtime`	Определяет время промежуточного хранения устройством CDP-пакетов
`show cdp`	Отображает информацию о CDP-анонсах

Практическое задание 15.1.6. Команды протокола CDP
В этом практическом задании необходимо, используя CDP-команды, получить информацию о соседних сетях и маршрутизаторах. Будет показана информация о настройке CDP-анонсов и о передаче фреймов.

Получение информации об удаленных устройствах

В этом разделе рассмотрены средства команд и программ *telnet*, *ping (эхо-запросы и ответы)* и *traceroute*[2] *(трассировка маршрута пакетов)*, которые помогают получить информацию об удаленных устройствах и используются в стандартном процессе тестирования сети, как показано на рис. 15.3.

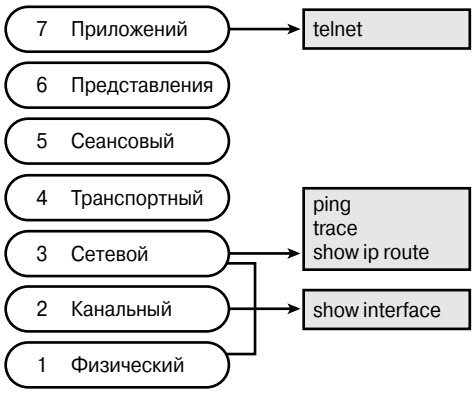


Рис. 15.3. Процесс тестирования сети

Telnet

Telnet — это виртуальный терминальный протокол, который является частью стека протоколов TCP/IP. Он позволяет создавать соединения с удаленными узлами, что дает возможность получать удаленный доступ к терминалу удаленной системы. Для проверки программного обеспечения уровня приложений между отправителем и получателем используется одноименная EXEC-команда операционной системы Cisco IOS. Эта команда является наиболее функциональным из доступных механизмов проверки.

Протокол telnet выполняется на уровне приложений модели OSI и построен на базе стека TCP, следовательно, он подразумевает корректную и последовательную доставку данных между клиентом и сервером.

Маршрутизатор может одновременно работать с несколькими входящими telnet-соединениями. Диапазон от 0 до 4 определяет пять виртуальных терминалов (vty) или telnet-линий. Таким образом, одновременно может быть создано до пяти telnet-сеансов.

Дополнительной функцией протокола telnet является проверка возможности установления соединения на уровне приложений. В основном эмулятор терминала telnet используется для соединения с удаленными устройствами, такими, как маршрутизатор, коммутатор и сервер, для получения информации или их технического

[2] *В операционной системе Windows корпорации Microsoft команда (и утилита) носит название* tracert. — *Прим. ред.*

обслуживания. Этот протокол и соответствующая команда представляют собой простое и универсальное средство тестирования.

Создание и проверка telnet-соединения

Команда **`telnet`** операционной системы Cisco IOS позволяет пользователю установить telnet-сеанс между двумя устройствами Cisco. При использовании в устройствах Cisco стека протоколов TCP/IP для создания telnet-соединения нет необходимости вводить команду **`connect`** или **`telnet`**, достаточно всего лишь ввести имя узла или IP-адрес удаленного маршрутизатора — и сеанс будет инициирован. Для разрыва telnet-сеанса используется EXEC-команда **`exit`** или **`logout`**. На рис. 15.4 проиллюстрировано создание и завершение telnet-соединения.

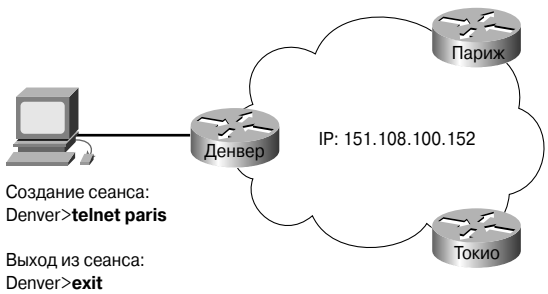


Рис. 15.4. Создание и разрыв telnet-соединения

Для работы с telnet-сеансом должна быть сконфигурирована таблица имен узлов или указан рабочий сервер DNS в конфигурации устройства; в противном случае в качестве аргумента необходимо вводить только IP-адрес узла, а не его имя. Для создания telnet-сеанса можно использовать один из следующих методов:

```
Denver>connect paris
Denver>paris
Denver>131.108.100.152
Denver>telnet paris
```

Служба telnet может использоваться для проверки доступности или недоступности удаленных маршрутизаторов. Как показано на рис. 15.5, при помощи telnet-соединения пользователь из Нью-Йорка может проверить доступность маршрутизатора, который находится в Париже. Такая операция может быть выполнена как в пользовательском режиме, так и в привилегированном.

Если доступ к удаленному маршрутизатору может быть получен посредством другого маршрутизатора, то на удаленном устройстве имеется, по крайней мере, одно TCP/IP-приложение. Удачное telnet-соединение означает правильную работу приложений верхнего уровня.

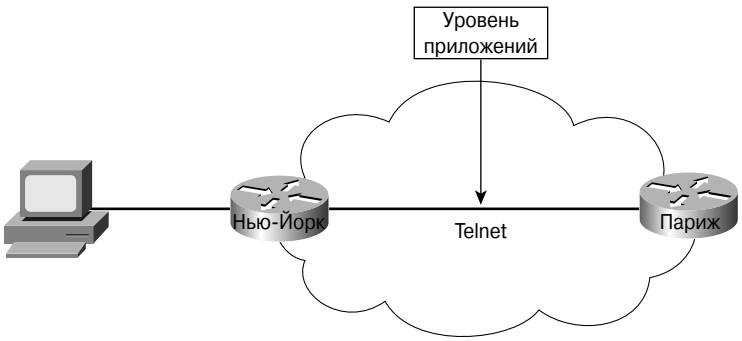


Рис. 15.5. Проверка уровня приложений

Telnet-соединение может быть успешно создано с одним маршрутизатором, однако с другим связь может быть невозможна по причине неправильной адресации, неправильного именования узлов или ограничений доступа. В общем случае получить в подобной ситуации telnet-доступ невозможно. В таком случае для проверки доступности маршрутизатора используется команда **`ping`**, которая позволяет проверить соединение между узлами на сетевом уровне.

После завершения telnet-сеанса следует отключиться от узла. Сеанс связи завершается, если в течение 10 минут пользователь не проявляет активности или же после ввода команды **`exit`**.

Практическое задание 15.2.2. Создание и проверка telnet-соединения
В этом практическом задании необходимо создать telnet-соединение с удаленным маршрутизатором и получить информацию о нем.

Отключение и приостановка telnet-сеансов

Одной из наиболее важных особенностей команды **`telnet`** является возможность приостановить сеанс связи. После приостановки сеанса возникает небольшая проблема, которая связана с тем, что когда telnet-сеанс или несколько сеансов приостановлены, то нажатие клавиши <Enter> в интерфейсе командной строки операционной системы Cisco IOS приводит к переключению в последний приостановленный сеанс. Клавиша <Enter> на клавиатуре — одна из самых наиболее часто используемых, поэтому вполне можно случайно переключиться на один из удаленных маршрутизаторов. Такое переключение представляет потенциальную опасность: можно случайно "испортить" конфигурацию в процессе внесения изменений или при работе в привилегированном режиме. Поэтому следует всегда внимательно следить за тем, в конфигурацию какого маршрутизатора вносятся изменения, например, по имени устройства в приглашении командной строки.

Сеанс может быть приостановлен на ограниченный промежуток времени. Чтобы вернуться в такой сеанс соединения с удаленным устройством, следует нажать клавишу <Enter>. С помощью команды **`show sessions`** можно посмотреть, какие сеансы установлены на данном маршрутизаторе.

Отключить сеанс связи с удаленным устройством можно двумя способами:

- введя команду **disconnect**;
- введя ту же команду с IP-адресом или именем маршрутизатора в качестве аргумента, например:

```
Denver>disconnect paris
```

Чтобы приостановить Telnet-сеанс, следует нажать комбинацию клавиш <Ctrl>+<Shift>+6 и потом — клавишу <x>.

Практическое задание 15.2.3. Остановка и разрыв telnet-соединений
В этом практическом задании необходимо создать telnet-соединение к удаленному маршрутизатору, затем временно остановить соединение и потом возобновить его.

Расширенные возможности службы telnet

Если на одном устройстве одновременно установлено несколько исходящих telnet-сеансов к удаленным устройствам, администратор может быстро и легко переключаться между ними. Количество одновременно разрешенных сеансов регулируется командой **session limit**.

Чтобы переключиться между сеансами, например, приостановить текущий сеанс и вернуться к запущенному ранее, следует сделать следующее:

- нажмите комбинацию клавиш <Ctrl>+<Shift>+6 и потом — клавишу <x>. Такая зарезервированная последовательность символов позволяет приостановить текущий сеанс с удаленным устройством и вернуться в приглашение командной строки локального маршрутизатора;
- далее следует ввести команду **resume**. Эта команда позволяет вернуться в приостановленный ранее сеанс. В качестве параметра для команды нужно указывать идентификатор удаленного соединения, в сеанс которого нужно переключиться.

Приостановив сеанс, можно установить новое подключение из интерфейса командной строки маршрутизатора.

С помощью указанной выше последовательности клавиш можно приостановить несколько сеансов. В сеанс можно вернуться, просто нажав клавишу <Enter> в приглашении командной строки локального устройства. Тем не менее, следует помнить, что после нажатия клавиши <Enter> операционная система Cisco IOS автоматически переключается в последний приостановленный сеанс. С помощью команды **resume** с идентификатором в качестве параметра можно переключиться в любой из ранее приостановленных сеансов; идентификаторы сеансов (или удаленных соединений) можно определить с помощью команды **show sessions**.

Практическое задание 15.2.4. Расширенные возможности службы telnet
В этом практическом задании необходимо использовать команду **`telnet`** для удаленного доступа к другим маршрутизаторам и проверить работоспособность уровня приложений между отправителем и получателем. Затем необходимо приостановить telnet-соединение и создать новые соединения. После этого вернуться к приостановленному соединению и отключить его.

Альтернативные методы проверки соединений

В этом разделе рассмотрены команды, которые могут использоваться для проверки соединения между сетевыми устройствами:

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

Команда ping

Большинство сетевых протоколов поддерживает эхо-протокол, который позволяет провести простейшую проверку сетевого соединения. Эхо-протокол позволяет проверить корректность маршрутизации сетевых пакетов.

Команда **`ping`** отправляет пакеты получателю и затем ждет ответных пакетов от этого узла. Результаты работы такого эхо-протокола могут помочь оценить надежность соединения, задержки передачи пакетов, а также работоспособность узла. Команда **`ping`** является основным механизмом тестирования соединения и может быть вызвана из пользовательского или привилегированного EXEC-режима.

Для проверки соединения при помощи команды **`ping`** следует выполнить действия, описанные ниже.

Этап 1. Ввести команду **`ping`** [*IP-address*] или [*name*] получателя.

Этап 2. Нажать клавишу <Enter>.

На рис. 15.6 приведена диаграмма сети, иллюстрирующая процесс работы службы отправки эхо-запросов и приема ответов.

Дополнительная информация: возвращаемые командой `ping` коды

В табл. 15.3 показаны расшифровки кодов, возвращаемых командой **`ping`**. Команда **`ping`** использует протокол ICMP.

Таблица 15.3. Коды, возвращаемые командой `ping`

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

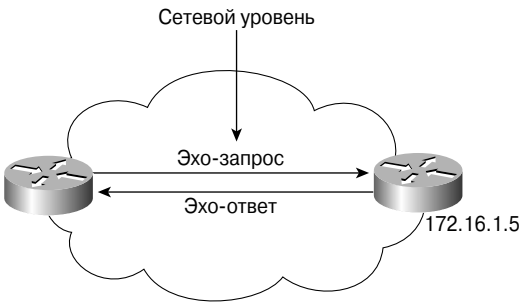


*Рис. 15.6. Проверка соединения при помощи команды **`ping`***

Как показано в следующем примере, проиллюстрированном на рис. 15.6, выполнялась команда **`ping`** для IP-адреса **`172.16.1.5`**.

```
Router> ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
```

```
!!!!
Success rate is 100 percent,
round-trip min/avg/max – 1/3/4/ ms
Router>
```

Каждый восклицательный знак означает успешный эхо-запрос (т.е. на запрос пришел вовремя ответ). Если в последовательности символов встретится одна точка (`.`), то это означает, что в приложении на маршрутизаторе истекло время ожидания для данного пакета.

Практическое задание 15.2.5а. Альтернативные методы проверки соединения
В этом практическом задании необходимо использовать команду **ping** для отправки дейтаграмм узлу-получателю и проверить работоспособность сетевого уровня стека протоколов TCP/IP между отправителем и получателем. Вы можете запросить информацию для проверки корректности маршрутизации, определить задержки передачи пакетов, а также доступность узла.

Команда traceroute

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

Команда **traceroute** используется следующим образом:

Этап 1. Введите команду **traceroute** [*IP-address*] или [*name*] (имя) получателя.

Этап 2. Нажмите клавишу <Enter>.

Дополнительная информация: возвращаемые командой traceroute коды

В табл. 15.4 представлены расшифровки кодов, возвращаемых командой **traceroute**.

Таблица 15.4. Коды, возвращаемые командой traceroute

Код	Значение	Возможная причина(ы)
nn **msec**	Время передачи пакета (в миллисекундах) между узлами	Трассировка прошла успешно
*	Истекло время ожидания запроса	Тестируемое устройство не получило запрос или не ответило на ICMP-сообщение “packet life exceeded” (“превышено время жизни пакета”)

Окончание табл. 15.4

Код	Значение	Возможная причина(ы)
`A`	Пересылка пакетов административно запрещена	Устройство на маршруте, например, такое, как маршрутизатор или брандмауэр, блокирует пакеты команды **`traceroute`**, однако пропускает все остальные пакеты
`Q`	Отправитель сбрасывает полученные ICMP-пакеты и требует подавления источника пакетов	Устройство на маршруте передачи, возможно, получатель, получило слишком много пакетов данных; проверьте статистику очередей пакетов
`H`	Получено нераспознанное ICMP-сообщение	Возможно, произошло зацикливание маршрутизации

В качестве демонстрации работы команды **`traceroute`** на рис. 15.7 приведена диаграмма сети для обмена сообщениями между удаленными маршрутизаторами.

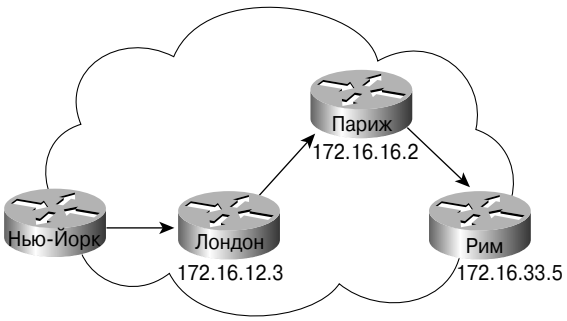


Рис. 15.7. Проверка соединения при помощи команды **`traceroute`**

В этом примере маршрут из Нью-Йорка в Рим был проверен следующим образом:

```
York# trace Rome
Type escape to abort.
Tracing the route to Rome (172.16.33.5)
1 LONDON (172.16.12.3) 1000 msec 8 msec 4 msec
2 PARIS (172.16.16.2) 8 msec 8 msec 8 msec
3 ROME (172.16.35.5) 8 msec 8 msec 4 msec

York#
```

В процессе проверки был протестирован маршрут, который проходил через Лондон и Париж. Если один из маршрутизаторов оказался бы недоступен, то в выводимой командой **`traceroute`** информации присутствовал бы символ "`*`". Команда **`traceroute`** будет повторять попытки перейти к следующему шагу до тех пор, пока не будет использовано сочетание клавиш <Ctrl>+<Shift>+<6>.

Команда **traceroute** использует сообщения об ошибках, генерируемые маршрутизаторами, когда истекает время жизни пакета (TTL) или превышается значение максимального числа переходов. Команда **traceroute** отправляет несколько ping-пакетов с увеличивающимся значением TTL и отображает время их прохождения. Поскольку каждый последовательно отправляемый пакет имеет меньшее время жизни, то каждый последующий уничтожается на более близком участке сети. Одним из применений команды **traceroute** является поиск неисправного участка сети.

Дополнительная информация: проверка сетевого уровня при помощи команды show ip route

В маршрутизаторе имеются мощные инструменты для анализа работы сети. Администратор может просмотреть таблицы маршрутизации, в которых содержится информация о путях передачи данных по сети, а также выполнить другие тесты сетевого уровня стека протоколов TCP/IP. Для просмотра таблицы маршрутизации используется команда **show ip route**, как показано в примере 15.5. В нем также показано, что сеть маршрутизатора Rome (131.108.33.0) доступна через интерфейс Ethernet1 (131.108.16.2) и сеть маршрутизатора Paris (рис. 15.7).

Пример 15.5. Выводимая командой show ip route информация

```
Paris# show ip route
Codes:    I – IGRP derived, R – RIP derived, O – OSPF derived
       C – connected, S – static, E – EGP derived, B – BGP derived
       i – IS-IS derived, D – EIGRP derived
       * - candidate default route, IA – OSPF inter area route
       E1 – OSPF external type 1 route, E2 – OSPF external type 2
       route L1 – IS-IS level-1 route, L2 – IS-IS level-2 route
       EX – EIGRP external route

Gateway of last resort is not set
I     144.253.0.0 [100/1300] via 133.3.32.2 0:00:22 Ethernet1
131.108.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
I     131.108.33.0 [100/180771] via 131.108.16.2, 0:01:29, Ethernet1
C     131.108.12.0 is directly connected, Ethernet1
C     101.108.16.0 is directly connected, Ethernet0
I     219.100.103.0 [100/1200] via 133.3.32.2, 0:00:22, Ethernet1
```

Проверка физического и канального уровней при помощи команды show interfaces serial

При проверке физического и канального уровней нужно ответить на следующие вопросы:

- имеется ли в сети сигнал несущей?
- имеется ли надежное физическое соединение между устройствами?
- принимаются ли тестовые пакеты соединения (keepalive message)?
- могут ли пакеты данных передаваться через физическое соединение?

Одной из наиболее важных частей информации, получаемой при помощи команды **show interfaces serial**, является справка о состоянии физического и канального уровней. На рис. 15.8 приведен пример работы этой команды.

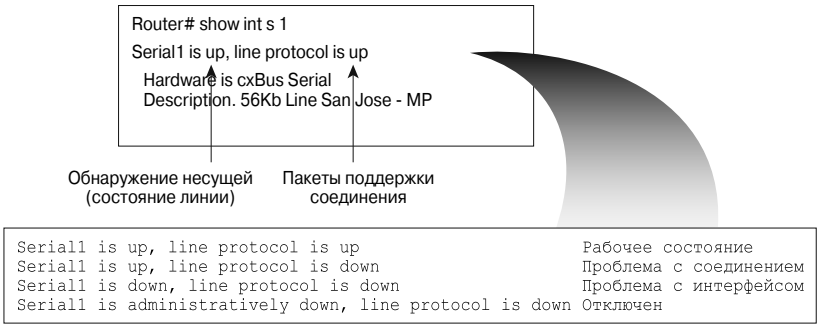


Рис. 15.8. Идентификация проблем в работе линии и протокола

В этом примере состояние линии переключается посредством сигнала несущей и отображает состояние физического уровня. Состояние протокола линии переключается автоматически тестовыми фреймами (keepalive) и отражает состояние канального уровня соединения (второго уровня эталонной модели OSI).

Использование команд `show interfaces` и `clear counters`

Маршрутизатор ведет статистику, которая содержит информацию об интерфейсах. Для просмотра этой статистики используется команда **`show interfaces`**, как показано в примере 15.6.

Пример 15.6. Выводимая командой `show interfaces` информация

```
Router# show interfaces serial 1
Serial1 is up, line protocol is up
Hardware is cxBus Serial
Description: 56Kb Line San Jose – MP
Internet address is 150.136.190.203, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:07, output 0:00:)), output hang never
Last clearing of show interfaces counters 2w4d
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
    16263 packets input, 1347238 bytes, no buffer
    Received 13983 broadcasts, 0 runts, 0 giants
    2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
    0 input packets with dribble condition detected
    22146 packets output, 2383680 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets, 0 restarts
    1 carrier transitions
```

Выводимая указанной командой статистика отражает работу маршрутизатора с момента последнего сброса счетчиков. Для сброса счетчиков в нуль используется команда **`clear counters`**. Картина работы маршрутизатора получается более точная, если анализ начинать с нулевых значений счетчиков. Также команда **`show interfaces`** может быть использована для проверки состояния интерфейсов других типов, например, Ethernet (E0), Fast Ethernet (Fa0) и ISDN (BRI0).

Проверка потока данных в реальном времени при помощи команды debug

Маршрутизатор включает в себя аппаратные средства и программное обеспечение для обнаружения и локализации проблем в работе на локальном маршрутизаторе или узле сети. Команда отладки привилегированного режима **debug** запускает в консоли отображение событий в сети в зависимости от указанного аргумента. Для перенаправления информации, выдаваемой этой командой, на терминал telnet-сеанса используется команда **terminal monitor**. Ее рекомендуется использовать *в каждом* удаленном telnet-сеансе, после ее указания *все* стандартные консольные сообщения устройства будут перенаправляться в такой сеанс. К сообщениям, которые стандартно выдаются в консольный порт, относятся уведомления от том, что какой-либо интерфейс был переключен из выключенного режима во включенный и обратно, уведомления об изменениях состояния соседнего устройства, например, переключение в нормальное финальное состояние протокола OSPF, и многие другие.

Для отключения средств отладки маршрутизатора служит команда **undebug all** (или **no debug all**). Режим отладки часто используется для решения проблем в работе маршрутизатора.

Стандартно маршрутизатор сообщения о системных ошибках и результаты работы команды **debug** отправляет на консоль терминала. Однако такой поток может быть перенаправлен на UNIX-узел или во внутренний буфер. Команда **terminal monitor** позволяет перенаправить эти сообщения на виртуальный терминал, который может использоваться в тех случаях, когда вы используете в административных целях UNIX-узел или Linux-узел вместо отдельного консольного устройства.

ВНИМАНИЕ!

Команду **debug** следует использовать в действующей сети с осторожностью. Использование этой команды в загруженной сети может существенно снизить скорость ее работы. Не оставляйте без надобности включенным режим отладки; его следует использовать только для диагностики проблем, после чего режим нужно отключить. Использование режима отладки на маршрутизаторе с установленным минимальным объемом ОЗУ может привести к перезагрузке маршрутизатора.

Поиск и устранение неполадок, связанных с IP-адресацией

Проблемы с адресацией часто возникают в IP-сетях; как правило, они являются следствием элементарных опечаток и невнимательности. Ниже указаны три наиболее часто используемые для решения таких неполадок команды:

- команда **ping** использует протокол ICMP для проверки соединения как на аппаратном уровне, так и IP-адреса на сетевом уровне. Она представляет собой базовое средство тестирования сети;
- команда **telnet** проверяет работоспособность уровня приложений эталонной модели OSI. Поскольку эта команда неявно проверяет все семь уровней эталонной модели, она является наиболее полным средством тестирования;
- команда **traceroute** используется для поиска точек отказа на маршруте следования пакета от отправителя к получателю. Она использует счетчик времени жизни пакета (Time-To-Live — TTL) в качестве механизма, обеспечивающего ответ от каждого транзитного маршрутизатора на пути к получателю.

Практическое задание. Решение проблем с IP-адресацией
В этом практическом задании необходимо настроить IP-адреса рабочих станций и проверить межсетевое взаимодействие между ними.

Резюме

В этой главе были рассмотрены следующие ключевые понятия:

- CDP является протоколом, не зависящим от среды и протоколов, является собственностью корпорации Cisco и используется для получения информации о соседних устройствах;
- протокол CDP предоставляет информацию лишь о тех устройствах, которые присоединены непосредственно к локальному узлу;
- протокол CDP используется для получения информации второго и третьего уровней о соседних устройствах;
- сетевое соединение может быть проверено на каждом уровне;
- команда **`ping`** использует ICMP-протокол для проверки наличия физического соединения и IP-адресов на сетевом уровне. Эта команда является простейшим средством сетевой проверки;
- команда **`telnet`** позволяет проверить программное обеспечение уровня приложений получателя и отправителя. Она предоставляет более широкие возможности по проверке сетевых устройств;
- команда **`traceroute`** позволяет локализовать сбойные участки сети на пути от отправителя к получателю. Эта команда, или ее сокращенный вариант — **`trace`**, использует TTL-значения для генерирования сообщений от каждого маршрутизатора на пути передачи пакетов.

Обратите внимание на относящиеся к настоящей главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Ключевые термины

Протокол обнаружения устройств Cisco (Cisco Descovery Protocol — CDP). Протокол CDP используется для получения информации о соседних устройствах, такой, как тип присоединенных устройств, интерфейсы маршрутизатора, которые в настоящий момент присоединены, и номера моделей устройств.

Отладка (debugging) используется для поиска и устранения ошибок и багов[3] в программах или моделях.

Ping (Packet Internet Groper — отправитель пакетов Internet) — программа, пересылающая эхо-сообщение и ответ на него в рамках протокола ICMP. Часто используется в IP-сетях для проверки связи с сетевым устройством.

Протокол доступа к подсети (Subnetwork Access Protocol — SNAP) представляет собой межсетевой протокол, который работает между сетевым объектом подсети и сетевым объектом в конечной системе. Протокол SNAP определяет стандартный метод инкапсуляции IP-дейтаграмм и ARP-сообщений в IEEE-сетях. SNAP-объект в конечной системе использует услуги, предоставляемые подсетью, и выполняет три ключевые функции: передачу данных, управление соединением и выбор параметров качества обслуживания (QoS).

Простой протокол управления сетью (Simple Network Management Protocol — SNMP) представляет собой протокол, используемый почти исключительно в TCP/IP-сетях. Протокол SNMP обеспечивает средства для мониторинга и управления сетевыми устройствами, а также для управления конфигурациями, сбором статистических данных, производительностью и защитой информации.

telnet — стандартный протокол эмуляции терминала из группы протоколов TCP/IP. Протокол telnet используется для организации соединений с удаленным терминалом и позволяет пользователям входить в удаленную систему и использовать ее ресурсы так, словно они подключены к локальной системе. Описан в RFC 854.

TLV (Type Length Values — тип-длина-значение) — это блоки информации, внедренные в CDP-анонсы.

Traceroute — программа, которая прослеживает путь пакета до пункта назначения. Используется главным образом для отладки процесса маршрутизации между узлами. Существует также протокол отслеживания, определенный в RFC 1393. Эта программа присутствует во многих операционных системах.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

[3] *Существует легенда, что термин* bar *(от англ.* bug *— насекомое, жук, клоп) появился достаточно давно, еще на заре вычислительной техники, когда в узлы первых электронно-механических вычислительных машин попадали насекомые, которые приводили к отказам. В настоящее время этот термин используется в программировании для обозначения ошибок в программном коде и иногда — применительно к аппаратным ошибкам. — Прим. ред.*

1. Что такое **`telnet`**?
   а) Команда, помогающая определить доступность определенного IP-адреса. Она отправляет пакеты данных по определенному адресу, а затем ожидает ответных пакетов.
   б) Команда, которая использует значение TTL для генерации сообщений от каждого маршрутизатора на пути следования пакетов.
   в) Команда используется для проверки программного обеспечения уровня приложений. Эта команда является самым полнофункциональным тестовым механизмом.
2. Какую информацию можно получить при помощи команды **`show interfaces serial`**?
   а) Состояние линии и протокола канального уровня.
   б) Информацию о том, как маршрутизатор направляет поток данных через сеть.
   в) Отображение пути пакетов, которые передаются через сеть.
   г) Отображение имен маршрутизаторов в сети.
3. Какая информация отображается для каждого соседнего CDP-устройства при выполнении команды **`show cdp neighbors`**?
   а) Идентификатор устройства.
   б) Список адресов.
   в) Идентификатор порта.
   г) Все вышеперечисленное.
4. Какую информацию можно получить для каждого соседнего CDP-устройства при выполнении команды **`show cdp interface`**?
   а) Значения CDP-таймеров и состояние интерфейса.
   б) Инкапсуляция протокола CDP для подтверждений и передачи фреймов.
   в) Конфигурация интерфейса соседних устройств.
   г) а и б.
5. Какой из следующих результатов дает команда **`show cdp entry`** *`[имя устройства]`*?
   а) Отображает все адреса 3-го уровня, представленные на соседнем маршрутизаторе.
   б) Отображает количество маршрутизируемых соседних устройств.
   в) Отображает список номеров устройств всех соседних маршрутизаторов.
   г) Отображает адреса второго уровня на интерфейсах соседних маршрутизаторов.

6. Какая из команд используется для получения информации, которая отображается командой **`show cdp neighbors`** и **`show cdp entry`** *`[имя устройства]`*?

   а) **`show cdp neighbors detail`**.

   б) **`show cdp interface entry`**.

   в) **`show cdp neighbors entry`**.

   г) **`show cdp details`**.

7. Какая информация отображается при выполнении команды **`show cdp neightbors`**?

   а) Идентификатор соседнего устройства.

   б) Тип локального порта и его номер.

   в) Декрементированное значение времени удержания информации.

   г) Все вышеперечисленное.

8. Какие четыре важные параметра можно получить, используя команду **`ping`**?

   а) Размер и количество ICMP-пакетов, время ожидания, частоту успешного выполнения и минимальное, среднее и максимальное время прохождения пакетов.

   б) Размер и количество ICMP-пакетов, MAC-адрес, частоту успешного выполнения и минимальное, среднее и максимальное время прохождения пакетов.

   в) Все вышеперечисленное.

   г) Ничего из вышеперечисленного.

9. Какая информация проверяется в сети с помощью команды **`traceroute`**?

   а) Работоспособность протокола линии.

   б) Существование записей в таблице маршрутизации для сети-получателя.

   в) Отмечает каждый маршрутизатор, через который проходят пакеты, прежде чем достичь получателя.

   г) Корректность работы приложений верхнего уровня.

10. Что означает символ восклицательного знака “**`!`**” в результатах работы команды **`ping`**?

    а) Количество удачных запросов.

    б) Количество неудачных запросов.

    в) Количество переходов перед достижением получателя.

    г) Все вышеперечисленное.

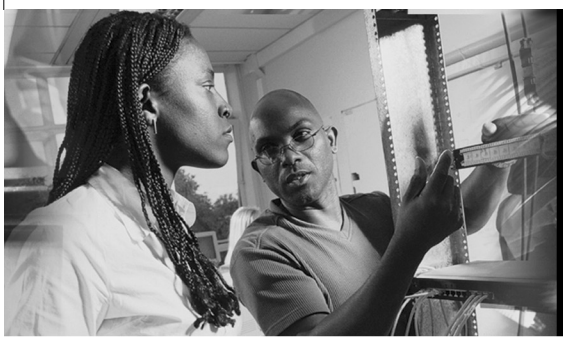
11. Какое из выражений является справедливым для команды **debug**?

а) Команда **debug** привилегированного режима запускает отображение сетевых параметров в консоли

б) Команда **undebug all** (или **no debug all**) отключает отладку.

в) Для буферизации входа в систему используется команда **buffer debug**.

г) а и б.



ГЛАВА 16

Управление программным обеспечением Cisco IOS

В этой главе...

- рассмотрены различные стадии загрузки маршрутизатора;
- описан процесс определения местонахождения и загрузки программного обеспечения Cisco IOS Cisco-устройством;
- описаны методы использования команды **`boot system`**;
- рассмотрены основные значения регистра конфигурации;
- описаны методы и механизмы определения местонахождения программного обеспечения IOS Cisco;
- рассмотрены процессы создания и загрузки образа программного обеспечения и используемые при этом команды, а также создание резервного файла конфигурации;
- описаны соглашения о названиях файлов программного обеспечения Cisco IOS;
- описаны файлы, используемые операционной системой Cisco IOS, и их предназначение;
- указано, где в маршрутизаторах размещены различные типы файлов;
- описано, что именно обозначает каждая часть названия операционной системы Cisco IOS;
- рассказано, какие действия необходимо предпринять, чтобы сохранить конфигурационный файл на TFTP-сервере или с помощью копирования и вставки текста, а также для того, чтобы восстановить утерянную конфигурацию;
- перечислены действия, которые необходимо выполнить, чтобы загрузить образ операционной системы Cisco IOS с TFTP-сервера;
- перечислены действия, которые необходимо выполнить, чтобы загрузить образ операционной системы Cisco IOS посредством протокола XModem;
- рассказано, как с помощью команд группы **`show`** проверить состояние файловой системы.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

процедура начальной загрузки, с. 725,
память NVRAM, с. 725,
простейший протокол передачи файлов, с. 727,
Flash-память, с. 727,
оперативная память, с. 734,
протокол удаленного копирования, с. 734.

В этой главе рассматриваются различные стадии загрузки маршрутизатора, включая определение местонахождения программного обеспечения Cisco IOS и его загрузку. В ней также описана команда **`boot system`** и показано, как эта команда может быть использована для указания параметров загрузки программного обеспечения маршрутизатора. Кроме того, в главе описаны несколько вариантов выбора источника, из которого можно выполнить загрузку программного обеспечения Cisco IOS в маршрутизатор, и необходимые для этого команды. Кроме того, в ней рассмотрены функции регистра конфигурации и методы определения версии операционной системы образа Cisco IOS. В последней части главы описано использование сервера TFTP в качестве источника программного обеспечения образов Cisco IOS и файлов конфигурации.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Загрузочная последовательность маршрутизатора и ее тестирование

Маршутизатор корпорации Cisco не может работать без специализированной межсетевой операционной системы (Internetwork Operation System — IOS). В каждом маршрутизаторе корпорации Cisco заранее сконфигурирована стандартная загрузочная последовательность, которая обнаруживает и загружает программное обеспечение системы Cisco IOS. В текущей главе основное внимание уделено этапам загрузки устройства и параметрам загрузочной процедуры.

Этапы загрузки маршрутизатора

При инициализации маршрутизатора выполняется *процедура начальной загрузки (программа самозагрузки, bootstrap)*, после которой происходит загрузка операционной системы и файла конфигурации. Если маршрутизатор не может найти файл конфигурации, он переходит в режим начальной настройки. Резервная копия нового файла конфигурации после выполнения диалога начальной настройки записывается в *энергонезависимую память* (*NonVolatile Random-Access Memory — память NVRAM*). На рис. 16.1 показаны операции, выполняемые при инициализации маршрутизатора.

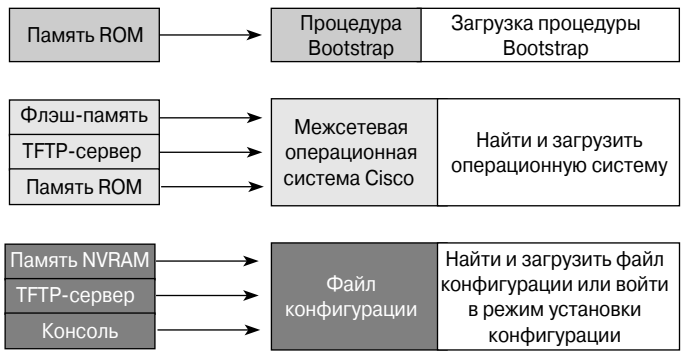


Рис. 16.1. Загрузочная последовательность маршрутизатора

Целью стандартной начальной загрузки программного обеспечения Cisco IOS является приведение маршрутизатора в рабочее состояние. Маршрутизатор должен обеспечить надежное функционирование соединений с сетями пользователей, которые он должен обслуживать в соответствии с заданной конфигурацией. Для этого следует выполнить следующие действия:

1. удостовериться в том, что маршрутизатор может загрузиться и использует память ROM;
2. найти и загрузить образ программного обеспечения Cisco IOS, который маршрутизатор будет использовать в качестве своей операционной системы;
3. найти и выполнить команды конфигурирования, включая функции различных протоколов и адреса интерфейсов.

Дополнительная информация: процедура POST

При включении питания маршрутизатора Cisco выполняется процедура автоматического самотестирования (Power-On Self Test — POST). В процессе выполнения такого автотеста маршрутизатор выполняет содержащиеся в его памяти ROM команды диагностики для всех аппаратных модулей. Эти команды диагностики тестируют базовые операции центрального процессора (CPU), памяти и портов сетевых интерфейсов. После тестирования функций аппаратного обеспечения маршрутизатор переходит к инициализации программного обеспечения.

Определение местонахождения и загрузка программного обеспечения Cisco IOS

Стандартно при загрузке источник программного обеспечения Cisco IOS определяется платформой аппаратного обеспечения. Однако обычно маршрутизатор сначала ищет сохраненные в памяти NVRAM команды **boot system**. Вместе с тем программное обеспечение Cisco IOS предоставляет пользователю несколько возможных альтернатив. В частности, пользователь может задать маршрутизатору другие источники для загрузки программного обеспечения. При необходимости для загрузки программного обеспечения маршрутизатор может также использовать свою собственную резервную загрузочную последовательность (fallback). На рис. 16.2 показан процесс поиска маршрутизатором образа программного обеспечения Cisco IOS.

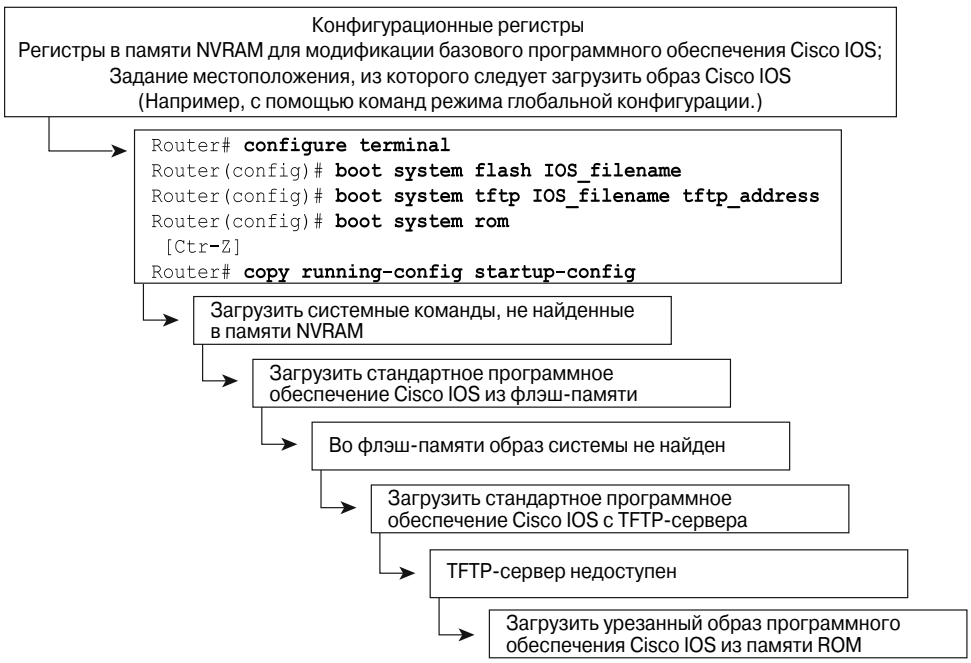


Рис. 16.2. Поиск местонахождения программного обеспечения Cisco IOS

Установка соответствующих значений конфигурационного регистра позволяет использовать приведенные ниже альтернативы.

- В режиме глобального конфигурирования пользователь может ввести несколько команд **boot system**, определяющих резервные источники (fallback), которые будет последовательно использовать маршрутизатор. В таком случае при повторном запуске маршрутизатор будет использовать эти команды.

- Если в памяти NVRAM отсутствуют команды **boot system**, которые мог бы использовать маршрутизатор, то стандартно он использует программное обеспечение Cisco IOS, которое записано во *Flash-память (flash memory)* устройства.
- Если во Flash-памяти образ Cisco IOS отсутствует, то для загрузки образа программного обеспечения из сети маршрутизатор пытается использовать *простейший протокол передачи файлов (Trivial File Transfer Protocol — TFTP*). Для указания имени файла, из которого будет загружаться стандартный образ системы, хранимый на сетевом сервере, маршрутизатор использует конфигурационный регистр.
- Если сервер TFTP недоступен, то маршрутизатор загружает сокращенную версию Cisco IOS, которая хранится в памяти ROM устройства.

Интерактивная презентация: процесс поиска и загрузки операционной системы Cisco IOS
В этой презентации подробно описаны и изучаются методы отыскания образа программного обеспечения Cisco IOS в процессе загрузки устройства.

Использование команды boot system

Для задания резервной последовательности (fallback) при загрузке программного обеспечения Cisco IOS можно ввести несколько команд **boot system**. Примеры 16.1-16.3 иллюстрируют использование команды **boot system** в различных формах, которые указывают, что программное обеспечение Cisco IOS должно сначала загружаться из Flash-памяти, в случае неудачи — с сетевого сервера и, как последний вариант, — из постоянной памяти ROM.

Команда **copy running-config startup-config** сохраняет команды текущей конфигурации в памяти NVRAM. При необходимости маршрутизатор выполняет команды **boot system** в том порядке, в каком они были первоначально введены в режиме конфигурирования. Для того чтобы узнать, имеются ли в файле конфигурации команды **boot system**, следует выполнить команду **show startup-config**.

Загрузка из Flash-памяти

При загрузке из Flash-памяти образ системы загружается из электронно перепрограммируемой постоянной памяти (Electrically Erasable Programmable Read-Only Memory — EEPROM). Преимущество такого способа загрузки состоит в том, что информация, сохраняемая во Flash-памяти, не подвержена сбоям в сети, которые могут произойти в случае загрузки образа системы с сервера TFTP. В примере 16.1 специальной командой **boot system** задается загрузка программного обеспечения Cisco IOS из Flash-памяти.

Пример 16.1. Загрузка из Flash-памяти

```
Router# configure terminal
Router#(config)# boot system flash c2691-a3js-mz.123-3.bin
! Нажать <Ctrl>+<Z>
Router# copy running-config startup-config
```

Загрузка с сетевого сервера

В случае повреждения Flash-памяти для образа системы можно получить резервную копию, указав, что она должна быть загружена с сервера TFTP. В примере 16.2 командой **boot system** указывается, что файл образа системы **test.ext** будет загружен с сервера TFTP, расположенного по IP-адресу 172.16.13.111.

Пример 16.2. Загрузка образа системы с сетевого сервера

```
Router# configure terminal
Router#(config)# boot system tftp IOS_image 172.16.13.111
! Нажать <Ctrl>+<Z>
Router# copy running-config startup-config
```

Загрузка образа системы из памяти ROM

Если Flash-память повреждена, а загрузить образ системы с сервера TFTP не удается, то последней программной возможностью загрузки образа является загрузка системы из постоянной памяти ROM. Однако в таком случае образ системы, загруженный из памяти ROM, вероятно, окажется лишь подмножеством программного обеспечения Cisco IOS. В этом подмножестве могут отсутствовать некоторые протоколы, функции и конфигурации полного набора Cisco IOS. Кроме того, если с момента приобретения маршрутизатора на нем выполнялась модернизация программного обеспечения, то, возможно, будет загружена старая версия IOS Cisco. В примере 16.3 показано использование указанного выше последнего способа загрузки программного обеспечения.

Пример 16.3. Загрузка образа системы из оперативной памяти ROM

```
Router# configure terminal
Router#(config)# boot system rom
! Нажать <Ctrl>+<Z>
Router# copy running-config startup-config
```

Практическое задание. Использование команды `boot system`

В этом задании требуется собрать информацию об образе операционной системы Cisco IOS и определить источник, из которого она была загружена. Следует также проверить установки регистра конфигурации и занести в регистрационный журнал последовательность резервной загрузки.

Конфигурационные регистры

Порядок, в котором маршрутизатор будет искать образ программного обеспечения Cisco IOS, зависит от значения в поле загрузки конфигурационного регистра маршрутизатора. Стандартную установку регистра конфигурации можно изменить с помощью команды режима глобального конфигурирования **config-register**. В качестве аргумента этой команды используется шестнадцатеричное число, как показано в примере 16.4.

Пример 16.4. Изменение значения поля загрузки в регистре конфигурации

```
Router# configure terminal
Router(config)# config-register 0x210F
! Нажать <Ctrl>+<Z>
```

При такой установке регистра конфигурации маршрутизатор прежде всего просматривает начальный файл в памяти NVRAM в поисках команд **boot system**. Регистр конфигурации имеет размер 16 битов и находится в памяти NVRAM. Младшие 4 бита (биты 3, 2, 1 и 0) образуют поле загрузки. Для того чтобы изменить поле загрузки и оставить все остальные биты без изменения, необходимо выполнить следующие операции:

- если требуется перейти в режим ROM-монитора (т.е. загрузки из памяти ROM), то значение регистра конфигурации следует установить равным 0xnnn0 (как nnn обозначены начальные стандартные установки регистров, которые не связаны с загрузкой). Такое действие позволяет установить именно для регистра загрузки двоичное значение 0000. После этого требуется перезагрузить устройство или выключить и включить питание, чтобы попасть в приглашение командной строки ROM-монитора. Для загрузки системы в командной строке монитора ROM следует ввести команду **b**;
- для автоматической загрузки системы из урезанного образа программного обеспечения Cisco IOS, находящегося в постоянном запоминающем устройстве (ROM), следует установить значение регистра конфигурации равным 0xnnn1, где символами nnn, как и выше, обозначены начальные стандартные установки регистров, которые не связаны с загрузкой.. При этом будет установлено двоичное значение загрузочного поля, равное 0001. В более старых платформах, как, например, маршрутизаторы Cisco 1600, 2500, будет выполнена загрузка урезанной версии операционной системы из памяти ROM. В новых устройствах, таких, как Cisco 1700 и 2600, а также в высокопроизводительных маршрутизаторах загрузка будет выполнена с использованием первого по счету образа операционной системы во Flash-памяти;
- чтобы сконфигурировать систему для использования команд **boot system** из памяти NVRAM, значение регистра конфигурации следует установить равным любому значению из интервала от 0xnnn2 до 0xnnnF (nnn обозначают установки регистров, которые не отвечают за загрузку устройства). Такая

установка является стандартной. При этом будет установлено одно из значений загрузочного поля из интервала от 0010 до 1111. Маршрутизатор последовательно обрабатывает каждую команду **boot system** в памяти NVRAM до тех пор, пока не дойдет до конца списка таких команд. Если команда **boot system** в стартовом конфигурационном файле отсутствует, маршрутизатор пытается загрузить операционную систему из Flash-памяти, т.е. действует по стандартному сценарию.

Если в памяти NVRAM отсутствуют команды **boot system**, то система обычно ищет образ программного обеспечения Cisco IOS во Flash-памяти.

В табл. 16.1 приведены значения загрузочного поля конфигурационного регистра.

Таблица 16.1. Значения загрузочного поля конфигурационного регистра

Значение	Описание
0x2100	Устанавливается для использования режима ROM-монитора (ручная загрузка с использованием команды **b** или **boot**)
0x2101	Автоматическая загрузка из постоянной памяти ROM (в новых устройствах загружается первый образ операционной системы из Flash-памяти. В более старых — урезанная версия операционной системы из памяти ROM. Стандартная установка, если в маршрутизаторе отсутствует Flash-память)
от 0x2102 до 0x210F	Включается поиск в NVRAM-памяти команд **boot system** (если в маршрутизаторе есть Flash-память, но нет команд **boot system** в конфигурации, то загружается первый образ операционной системы из Flash-памяти)

Для проверки значения загрузочного поля и тестирования команды **config-register** следует использовать команду **show version**.

Устранение неполадок при загрузке операционной системы Cisco IOS

Нормальная загрузка маршрутизатора может не состояться по следующим причинам:

- в конфигурационном файле отсутствуют или неправильно указаны команды **boot system**;
- в конфигурационном регистре установлено неправильное значение;
- образ операционной системы во Flash-памяти поврежден;
- произошел отказ какого-либо модуля аппаратного обеспечения.

Маршрутизатор в процессе загрузки ищет строки, которые содержат команду **boot system** в стартовом конфигурационном файле. Команда **boot system** с параметрами может привести к тому, что устройство загрузит альтернативный образ операционной системы вместо того, который размещен во Flash-памяти. Как

показано в примере 16.5, команда **show version** отображает информацию о текущей версии программного обеспечения Cisco IOS на маршрутизаторе. Эта информация о версии включает в себя установки регистра конфигурации и поля загрузки.

Пример 16.5. Конфигурационный регистр

```
Router# show version

Cisco Internetwork Operating System Software IOS (tm) 2500 Software
(C2500-JS-L), Version 12.1(5), RELEASE SOFTWARE (fc1) Copyright (c)
1986-2000 by Cisco Systems, Inc. Compiled Wed 25-Oct-00 05:18 by
cmong Image text-base: 0x03071DB0, data-base: 0x00001000
(C2500-JS-L),
chpt_14.fm
ROM: System Bootstrap, Version 5.2(8a), RELEASE SOFTWARE BOOTFLASH:
3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(8a), RELEASE
SOFTWARE (fc1)
Router uptime is 7 minutes System returned to ROM by reload System
image file
is "flash:c2500-js-l_121-5.bin"
Cisco 2500 (68030) processor (revision D) with 16384K/2048K bytes of
memory.
Processor board ID 03867477, with hardware revision 00000000 Bridg-
ing software.
X.25 software, Version 3.0.0. SuperLAT software (copyright 1990 by
Meridian Technology Corp). TN3270 Emulation software. 1 Token
Ring/IEEE 802.5
interface(s) 2 Serial network interface(s) 32K bytes of non-volatile
configuration memory. 16384K bytes of processor board System flash
(Read ONLY)
Configuration register is 0x2142
```

Для устранения проблем при загрузке операционной системы следует сначала воспользоваться командой **show running-config** и поискать выражения, которые начинаются с ключевых слов **boot system,** в самом начале стартового конфигурационного файла. Если команда **boot system** указывает на неправильный образ системы IOS, следует удалить ее, добавив ключевое слово **no** в начале соответствующей командной строки.

Неправильное значение в конфигурационном регистре может привести к тому, что операционная система Cisco IOS не будет загружена из Flash-памяти. Значение регистра указывает, откуда маршрутизатор должен брать программное обеспечение. Источник для загрузки может быть указан посредством команды **boot system** или в конфигурационном регистре. Настройки регистра можно проверить с помощью команды **show version**, его значение показано в последней строке выводимой информации. Правильное значение регистра для разных платформ может быть разным. Чтобы определить, какое именно значение регистра следует установить, обратитесь к документации по устройству. Если печатная документация недоступна, ее копию можно найти на компакт-диске или на Web-сайте корпорации Cisco, и по

такой информации идентифицировать, какие именно значения следует сконфигурировать. Необходимо установить правильные значения конфигурационного регистра и сохранить стартовую конфигурацию.

Если нормальная загрузка все же не происходит, можно предположить, что файл образа операционной системы во Flash-памяти поврежден. В таком случае при загрузке должно выводиться сообщение об ошибке в процессе загрузки устройства. Сообщение для разных устройств и разных типов отказов может отличаться. Некоторые примеры сообщений указаны ниже.

```
open: read error . . . requested 0x4 bytes, got 0x0
trouble reading device magic number
boot: cannot open “flash: ”
boot: cannot determine first file name on device “flash: ” ґ
```

Если образ операционной системы поврежден, его следует записать заново.

Если же ни одно из указанных выше сообщений на консоли не появляется, то, скорее всего, произошел отказ аппаратного обеспечения. В таком случае необходимо связаться с ближайшим центром службы технической поддержки корпорации Cisco (Cisco Technical Assistance — TAC). Следует заметить, что аппаратные сбои редки, тем не менее, они иногда происходят.

Практическое задание. Решение проблем загрузки системы, связанных с наличием ошибок в регистре конфигурации

В этой работе требуется проверить правильность установок конфигурационного регистра, связанных с методом загрузки, и сконфигурировать маршрутизатор на загрузку программного обеспечения Cisco IOS из Flash-памяти.

Дополнительная информация: проверка текущей версии образа операционной системы Cisco IOS

Команда **show version**, которая была показана в примере 16.5, позволяет получить информацию о том, какая именно версия операционной системы Cisco IOS используется маршрутизатором. В выводимой с помощью этой команды информации также присутствует значение конфигурационного регистра, и из него можно определить настройку загрузочного поля регистра.

В этом примере во второй строке вывода доступна информация о версии операционной системы Cisco IOS и ее описание. Информация получена из операционной системы версии 12.1(5). Следующий фрагмент вывода указывает файл образа системы c2500-js-l, загруженный из Flash-памяти. Следует отметить, что в имени файла указано, что этот образ предназначен для платформы Cisco 2500.

По мере того, как по команде **show version** печатается информация, на экран выводится информация о типе платформы, на которой в данный момент работает версия программного обеспечения Cisco IOS. Последний фрагмент вывода отражает результаты выполнения команды **config-register 0x2142**. Эта информация используется для ввода значений регистра конфигурации.

ВНИМАНИЕ!

Следует обратить внимание, что значения, которые установлены в конфигурационном регистре, нельзя определить ни с помощью команды **`show running-config`**, ни с помощью команды **`show startup-config`**.

Управление файловой системой Cisco

Межсетевые устройства корпорации Cisco для своей работы требуют нескольких файлов, к числу которых относятся образ (или образы) межсетевой операционной системы Cisco (Cisco Internetwork Operating System — Cisco IOS) и конфигурационные файлы. Если сетевой администратор желает, чтобы сеть работала "гладко" и надежно, он должен очень аккуратно обращаться с такими файлами, следить за тем, чтобы использовалась нужная версия и чтобы периодически с этих файлов снималась резервная копия. В этом разделе основное внимание уделено файлам и файловой системе корпорации Cisco и вспомогательному инструментарию, который позволяет ефективно управлять системой.

Основы файловой системы IOS

Работа маршрутизаторов и коммутаторов зависит от установленного на них программного обеспечения. Двумя типами программного обеспечения, необходимыми для их функционирования, являются операционная система и файл конфигурации.

В качестве операционной системы практически на всех устройствах Cisco используется межсетевая операционная система Cisco (Internetwork Operating System — IOS). Программное обеспечение Cisco IOS позволяет аппаратному устройству функционировать в качестве маршрутизатора или коммутатора. Файл программного обеспечения Cisco IOS имеет размер в несколько мегабайтов. Операционная система Cisco IOS представляет собой платформу, которая обеспечивает выполнение сетью всех ее функций, таких, как установка соединений, обеспечение надежности, поддержка в сети безопасности и качества обслуживания, масштабируемости и возможностей управления, требуемых приложениям.

Программное обеспечение, используемое маршрутизатором или коммутатором в качестве списка настроек, называется *файлом конфигурации,* или просто *конфигурацией*. Файл конфигурации содержит инструкции (команды), которые определяют, каким образом устройство должно выполнять маршрутизацию или коммутацию. Этот файл создается сетевым администратором, который определяет требуемые функции устройств корпорации Cisco. Примерами параметров и функций, задаваемых в файле конфигурации, являются IP-адреса интерфейсов, протоколы маршрутизации и анонсируемые сети. Обычно файл конфигурации имеет размер от нескольких сот до нескольких тысяч байтов.

Каждый из компонентов программного обеспечения хранится в памяти как отдельный файл. Разные файлы сохраняются в различных типах памяти.

Образ программного обеспечения IOS Cisco хранится в области памяти, называемой Flash-памятью (Flash-memory). Flash-память обеспечивает энергонезависимое хранение образа Cisco IOS, который может быть использован в начале работы операционной системы. Flash-память позволяет модернизировать программное обеспечение IOS, а также хранить несколько различных типов программного обеспечения. Во многих структурах маршрутизаторов образ программного обеспечения копируется из Flash-памяти в *оперативную (Random-Access Memory — RAM)*. Далее оперативная память используется в качестве хранилища для операционной системы в процессе работы.

Копия файла конфигурации хранится в памяти NVRAM для использования в качестве конфигурации при включении системы. Такая NVRAM-конфигурация называется *начальной,* или *стартовой конфигурацией* (*startup config*). Стартовая конфигурация копируется в оперативную память RAM во время загрузки системы. Конфигурация, которая находится в RAM-памяти, используется для управления маршрутизатором в процессе работы. Находящаяся в RAM-памяти конфигурация называется *текущей, или действующей конфигурацией (running config)*.

В 12-й версии программного обеспечения Cisco IOS имеется единый интерфейс для всех используемых маршрутизатором файловых систем. Эта версия программного обеспечения называется файловой системой Cisco IOS (IOS File System — IFS). Система IFS обеспечивает единый метод управления файловой системой, используемый маршрутизатором. Система IFS включает в себя файловые системы Flash-памяти, сети, а также чтение и запись данных. Файловые системы сети включают в себя протокол TFTP, *протокол удаленного копирования (remote copy protocol — RCP)* и протокол передачи файлов (File Transfer Protocol — FTP). Чтение и запись данных включают в себя память NVRAM, текущую конфигурацию и постоянную память ROM. Для обозначения устройств файловая система IFS использует общий набор префиксов. В табл. 16.2 приведен обзор системы IFS.

Таблица 16.2. Файловая система Cisco IOS

Префикс	Описание
bootflash:	Загрузить образ IOS Cisco из Flash-памяти
flash:	Flash-память. Этот префикс доступен на всех платформах. На платформах, в которых отсутствует устройство с именем Flash, этот префикс заменяется псевдонимом (alias) slot0:. Поэтому префикс *flash:* может применяться по отношению к главной области хранения Flash-памяти на всех платформах
flh:	Файлы журнала вспомогательной загрузки из Flash-памяти
Nvram:	Память NVRAM
Rcp:	Сетевой сервер протокола удаленного копирования (RCP)
Slot0:	Первая карта Flash-памяти PCMCIA
Slot1:	Вторая карта Flash-памяти PCMCIA
system:	Содержит системную память, включая текущую конфигурацию
Tftp:	Сетевой TFTP-сервер

Файловая система IFS использует соглашение об адресах URL (унифицированный указатель информационного ресурса — URL, Uniform Resource Locator) для указания файлов, расположенных на сетевых устройствах и в сети. Соглашение об адресах URL указывает местонахождение файлов конфигурации вслед за символом двоеточия ":" в таком виде: *[[[//location]/directory]/filename]*. Система IFS также поддерживает передачу файлов по протоколу FTP. В табл. 16.3 приведены команды, используемые для управления программным обеспечением Cisco IOS версии 12.0, и выполнен их сравнительный анализ с соответствующими командами версий, предшествовавших версии 12.0.

Таблица 16.3. Команды управления программным обеспечением IOS Cisco версии 12.0 и более ранних

Команды программного обеспечения Cisco IOS версий, предшествовавших версии 12.0	Команды программного обеспечения Cisco IOS версий 12.x

`configure network`
(в версиях Cisco IOS до версии 10.3)
`copy rcp running-config`
`copy tftp running-config`
	`copy ftp: system:running-config`
	`copy rcp running-config`
	`copy tftp running-config`

`configure overwrite-network`
(в версиях Cisco IOS до версии 10.3)
`copy rcp startup-config`
`copy tftp startup-config`
	`copy ftp: nvram:startup-config`
	`copy rcp: nvram:startup-config`
	`copy tftp: nvram:startup-config`

`show configuration` (в версиях Cisco IOS до версии 10.3) **`show startup-config`**	**`more nvram:startup-config`**
`write erase` (в версиях Cisco IOS до версии 10.3) **`erase startup-config`**	**`erase nvram:`**

`write memory`
(в версиях Cisco IOS до версии 10.3)
`copy running-config`
`startup-config`
	`copy system:running-config`
	`nvram:startup-config`

`write network`
(в версиях Cisco IOS до версии 10.3)
`copy running-config rcp`
`copy running-config tftp`
	`copy system:running-config ftp:`
	`copy system:running-config rcp:`
	`copy system:running-config tftp`

`write terminal`
(в версиях Cisco IOS до версии 10.3)
`show running-config`
	`more system:running-config`

Интерактивная презентация: обзор файловой системы IFS корпорации Cisco
В этой презентации перечислены конфигурационные файлы и указано их местоположение.

Соглашения об именах файлов программного обеспечения Cisco IOS

Корпорация Cisco разрабатывает много различных версий программного обеспечения. Это программное обеспечение поддерживает разнообразные платформы и функции. Корпорация Cisco регулярно выпускает новые версии операционной системы Cisco IOS.

Для различения разных версий программного обеспечения корпорация Cisco разработала специальные правила их обозначения, как показано на рис. 16.3.

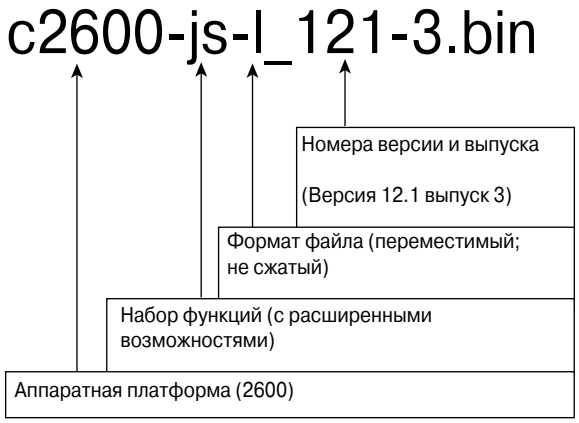


Рис. 16.3. Принятые корпорацией Cisco обозначения для имен файлов

Как показано на рис. 16.3, соглашения об обозначениях описывают значения нескольких полей в имени файла.

- **Аппаратная платформа.** Первая часть имени файла указывает аппаратную платформу, для которой предназначена эта версия.
- **Набор функций**. Вторая часть имени файла характеризует различные функции, которые реализует этот файл. Пользователь может выбрать любые наборы функций, которые упакованы в образы программного обеспечения. Каждый набор функций содержит определенное подмножество из всего набора функций программного обеспечения Cisco IOS. Примеры таких наборов приведены ниже.
  - **Базовый набор (Basic).** Включает в себя основные функции для всех аппаратных платформ. Примером функций базового набора является поддержка протоколов IP и IP/FW.

- **Дополнительные функции (набор Plus).** Набор Plus представляет собой базовый набор, к которому добавлены такие дополнительные функции, как Plus, IP/FW Plus и Enterprise Plus.
- **Шифрование.** Этот набор содержит функции 56-битового шифрования данных, добавленные к набору Basic или набору Plus. Примерами набора шифрования могут служить IP/ATM PLUS IPSEC 56 и Enterprise Plus 56. Начиная с версии 12.2, в версиях Cisco IOS для обозначения шифрования используются идентификаторы k8/k9. В версии 12.2 и более поздних идентификатор k8 указывает на 64-битовое шифрование или шифрование с меньшим количеством битов, в то время как k9 указывает на 64-битовое шифрование или шифрование с большим количеством битов.

- **Формат файла.** Третья часть имени файла IOS указывает его формат. Она показывает, хранится ли программное обеспечение IOS Cisco во Flash-памяти в сжатом виде (формате) и допускает ли образ IOS Cisco перемещение. Если Flash-образ хранится в сжатом виде, то в процессе загрузки он должен быть распакован, а сам образ скопирован в оперативную память RAM. Если образ допускает перемещение, он может быть скопирован в память RAM и запущен из нее. Неперемещаемый образ запускается непосредственно из Flash-памяти.
- **Версия и выпуск.** В четвертой части имени файла указывается номер версии и выпуска. По мере того как разрабатываются новые версии IOS Cisco, номер версии возрастает.

Интерактивная презентация: соглашения об именах файлов программного обеспечения Cisco IOS
В этой презентации проиллюстрировано, как можно идентифицировать различные части имени файла операционной системы **Cisco** IOS.

Управление файлом конфигурации с использованием протокола TFTP

На маршрутизаторе или коммутаторе Cisco активная конфигурация находится в оперативной памяти RAM. В случае, если она по каким-либо причинам утеряна, ее следует восстановить из резервной копии стартовой конфигурации. Одну из таких резервных копий можно хранить на сервере TFTP. Для восстановления конфигурации используется команда **`copy running-config tftp`**. Для создания резервной копии файла конфигурации необходимо выполнить описанные ниже действия.

Этап 1. Следует ввести команду **`copy tftp running-config`**.

Этап 2. Необходимо ввести в командной строке IP-адрес сервера TFTP, на котором будет храниться файл конфигурации.

Этап 3. Далее следует ввести имя для файла конфигурации или принять предложенное стандартное имя.

Этап 4. Подтвердить сделанные установки, каждый раз отвечая на вопросы “Yes” (Да).

В примере 16.6 проиллюстрирован процесс создания резервной копии файла конфигурации.

Пример 16.6. Создание резервной копии файла начальной конфигурации на сервере TFTP

```
Cougar# copy running-config tftp
Address or name of remote host [] 192.168.119.20
Destination file name [Cougar-config]?
!!!!!!!!!!!!!!!!!!!!!!!
624 bytes copied in 7.05 secs
Cougar#
```

ВНИМАНИЕ!

Если файл конфигурации маршрутизатора отсутствует или были использованы команды **erase startup-config** и **reload**, то в маршрутизаторе не будет ни одного сконфигурированного интерфейса. Для того чтобы сервер TFTP мог установить соединение, ему требуется знать IP-адрес соответствующего устройства, поэтому в данном случае необходимо подсоединиться к маршрутизатору через консольный порт и сконфигурировать IP-адрес интерфейса, который будет обеспечивать доступ к серверу.

Восстановить конфигурацию маршрутизатора можно путем загрузки резервной копии файла начальной конфигурации с сервера TFTP. Для восстановления конфигурации следует выполнить описанные ниже действия.

Этап 1. Ввести команду **copy tftp running-config**.

Этап 2. После появления системной подсказки выбрать файл конфигурации устройства или сети.

Этап 3. Ввести IP-адрес сервера TFTP, на котором хранится файл конфигурации.

Этап 4. После появления системной подсказки ввести имя файла конфигурации или принять предложенное по умолчанию имя.

Этап 5. Подтвердить правильность имени файла конфигурации и адреса TFTP-сервера, предлагаемых системой.

В примере 16.7 показан процесс восстановления файла конфигурации с сервера TFTP.

Пример 16.7. Восстановление начальной конфигурации с TFTP-сервера

```
Cougar# copy tftp running-config
Address or name of remote host [] 192.168.119.20
Source filename []? Cougar-confg
Destination filename [running-config]?
Accessing tftp://192.168.119.20/GAD-confg
Loading GAD-confg from 192.168.119.20
```

```
(via FastEthernet 0/0): !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK-624 bytes]
624 bytes copied in 9.45 secs Cougar#
```

Дополнительная информация: копирование файла конфигурации с TFTP-сервера на маршрутизатор

Для того чтобы скопировать файл конфигурации с TFTP-сервера на маршрутизатор, следует выполнить описанные ниже действия.

Этап 1. Войти в режим конфигурирования с помощью команды **`copy tftp running-config`**.

Этап 2. После появления системной подсказки следует выбрать файл конфигурации устройства или сети. Файл конфигурации сети содержит команды, которые будут применены ко всем маршрутизаторам и серверам терминалов всей сети. Файл конфигурации устройства содержит команды, которые будут применены только к конкретному маршрутизатору или коммутатору. При появлении системной подсказки следует ввести (необязательный) IP-адрес удаленного узла, на котором находится файл конфигурации. В примере 16.8 маршрутизатор конфигурируется с сервера TFTP, имеющего IP-адрес 131.108.2.155.

Этап 3. Ввести имя файла конфигурации или принять предлагаемое стандартное значение. При выборе стандартного имени файла используется соответствующее UNIX-соглашение. В соответствии с ним для файла конфигурации устройства выбирается имя **`hostname-config`**, а для файла конфигурации сети — **`network-config`**. В операционной среде DOS имена файлов ограничены восемью символами и трехсимвольным расширением. Примером такого имени может служить **`router.cfg`**. Далее следует подтвердить предлагаемые системой имя файла конфигурации и адрес сервера TFTP. Нужно обратить внимание на то, что в примере 16.8 имя маршрутизатора в командной строке сразу меняется на **`tokyo`**. Это изменение свидетельствует о том, что реконфигурирование происходит сразу после загрузки нового файла конфигурации.

В примере 16.8 проиллюстрирован процесс копирования файла конфигурации с TFTP-сервера.

Пример 16.8. Копирование файла конфигурации с TFTP-сервера

```
tokyo# copy tftp running-config
Host or network configuration file [host]?
IP address of remote host [255.255.255.255]? 131.108.2.155
Name of configuration file [Router-config]? tokyo.2
Configure using tokyo.2 from 131.108.2.155? [confirm] y
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
tokyo#
```

Практическое задание 5.2.3. Управление файлами конфигурации с помощью TFTP-сервера
В этой лабораторной работе необходимо скопировать файл конфигурации на TFTP-сервер, а затем сконфигурировать маршрутизатор путем копирования файла конфигурации с сервера TFTP.

Управление файлами конфигурации посредством копирования и вставки текста

Альтернативным способом создания резервной копии файла конфигурации является использование команды **show running-config**. Такое резервное копирование может быть сделано в ходе терминального сеанса путем копирования вывода в буфер, вставки в текстовый файл и последующего его сохранения в качестве резервной копии. Однако перед использованием этого файла в качестве резервной копии для восстановления конфигурации маршрутизатора его следует отредактировать. На рис. 16.4 проиллюстрированы операции копирования и вставки фрагментов конфигурации.

Для выбора требуемого текста конфигурации в программе HyperTerminal необходимо выполнить описанные ниже действия.

Этап 1. Выбрать опцию Передача.

Этап 2. Выбрать опцию Захват текста.

Этап 3. Задать имя текстового файла, в который будет копироваться конфигурация.

Этап 4. Выбрать опцию Начать, чтобы запустить процесс копирования текста.

Этап 5. Вывести на экран конфигурацию с помощью команды **show running-config**.

Этап 6. Нажимать клавишу пробела при каждом появлении сообщения "`--More--`", которое будет появляться до тех пор, пока не будет выведен весь файл конфигурации.

Этап 7. После того как будет выведен на экран весь файл конфигурации, следует прекратить копирование, выполнив следующие действия:

- выбрать в меню опцию Передача;
- выбрать опцию Захват текста;
- выбрать опцию Остановить.

После того как копирование закончено, необходимо отредактировать файл конфигурации для удаления лишнего текста. Для того чтобы преобразовать этот файл в вид, в котором он может быть скопирован в буфер и передан маршрутизатору, необходимо удалить из него всю ненужную информацию. Для лучшей ориентации в тексте можно вставить в него дополнительные комментарии. Для вставки комментария следует в начале строки ввести символ восклицательного знака (!). Полученный файл конфигурации можно отредактировать в любом текстовом редакторе, например, в программе Notepad. Для редактирования файла конфигурации в редакторе Notepad следует выполнить описанные ниже действия.

Этап 1. В меню Файл выбрать опцию Открыть.

Этап 2. Найти файл с захваченным текстом по имени.

Этап 3. Щелкнуть мышью на кнопке Открыть.

Из скопированного файла следует удалить строки следующего вида:

- *show running-config;*
- *Building configuration...;*
- *Current configuration:;*
- *-- More --;*
- все строки после слова *End*.

В конце каждого раздела команд отдельного интерфейса необходимо добавить команду **no shutdown**. После этого следует в меню Файл выбрать опцию Сохранить для сохранения готового файла конфигурации.

После того как вы сохранили файл, резервную конфигурацию можно восстановить в сеансе терминала. Однако перед ее восстановлением необходимо удалить на маршрутизаторе остатки текущей конфигурации, выполнив команду **erase startup-config** в командной строке, и ввести команду **reload**.

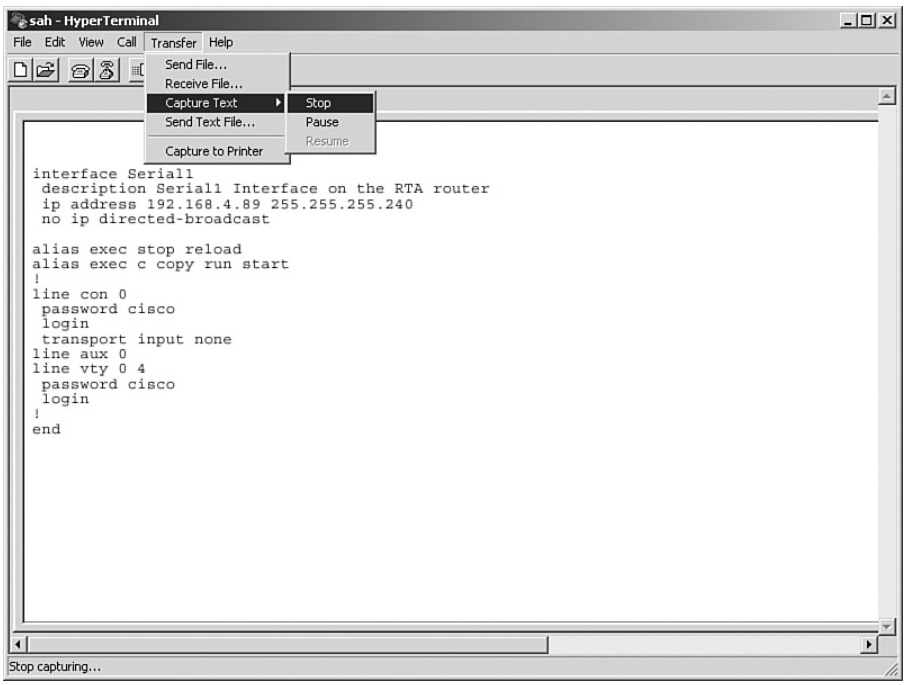


Рис. 16.4. Копирование файла конфигурации

После удаления остатков текущей конфигурации можно восстановить конфигурацию с помощью терминала. Для копирования резервного файла конфигурации следует выполнить описанные ниже действия.

Этап 1. Войти в режим глобального конфигурирования.

Этап 2. В терминальном приложении (HyperTerminal) выбрать опцию Передача, затем Переслать и в меню выбрать Текстовый файл.

Этап 3. Выбрать в списке имя фала сохраненной резервной конфигурации.

Этап 4. Строки резервного файла вводятся так, как если бы их текст набирался на клавиатуре.

Этап 5. Проверить текст конфигурации на наличие ошибок.

Этап 6. После того как введена вся конфигурация, следует нажать клавиши <Ctrl>+<z> для выхода из режима глобального конфигурирования.

Этап 7. Восстановить начальную конфигурацию с помощью команды **`copy running-config startup-config`**.

Управление образами программного обеспечения Cisco с помощью TFTP-сервера

Иногда требуется восстановить или обновить программное обеспечение маршрутизатора. При первом включении маршрутизатора следует сделать резервную копию операционной системы Cisco IOS на TFTP-сервере с помощью команды **`copy flash tftp`**. Этот образ системы Cisco IOS может быть сохранен на центральном сервере вместе с другими образами для восстановления или обновления программного обеспечения IOS на маршрутизаторах и коммутаторах объединенной сети.

На сетевом сервере должна функционировать служба протокола TFTP. Обновление программного обеспечения Cisco IOS осуществляется в привилегированном EXEC-режиме с помощью команды **`copy tftp flash`**, как показано в примере 16.9.

Пример 16.9. Создание резервной копии программного обеспечения Cisco IOS на TFTP-сервере

```
Cougar# copy tftp flash
Address or name of remote host []? 192.168.119.20
Destination filename [C2600-js-l_121-3.bin]?
Accessing tftp://192.168.119.20/C2600-js-l_121-3.bin
Erase flash: before copying? [confirm]
Erasing the flash file system will remove all files
Continue? [confirm]
Erasing device eeeeee...eeeeeeeeeeeee...erased
Loading C2600-js-l_121-3.bin from 192.168.119.20 (via FastEthernet
0/0):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Verifying Check sum……..OK
[OK-8906589 bytes]
8906589 bytes copied in 277.45 secs
Cougar#
```

ВНИМАНИЕ!

Символ “!” в строке означает, что загрузка файла во Flash-память происходит успешно. Символ “.” означает, что найти файл не удается (или пакет потерян). Если появляется символ “.”, то следует проверить правильность синтаксиса введенной команды.

При выполнении указанной выше операции маршрутизатор предлагает ввести IP-адрес сервера TFTP. После предложения ввести имя файла для образа программного обеспечения IOS маршрутизатор, возможно, предложит стереть данные из Flash-памяти. Такое предложение стереть данные часто выводится в том случае, когда во Flash-памяти недостаточно места для нового образа. По мере того, как стираются данные из Flash-памяти, на экран выводится серия символов “e”, отображающая процесс стирания данных.

При загрузке каждой дейтаграммы файла образа Cisco IOS на экран выводится символ “!”. Образ программного обеспечения IOS Cisco может иметь размер, достигающий нескольких мегабайтов и, соответственно, процесс его загрузки может оказаться достаточно длительным. После загрузки выполняется тестирование файла во Flash-памяти. После этого маршрутизатор готов к перезагрузке с использованием нового образа.

Дополнительная информация: копирование образа операционной системы Cisco IOS с TFTP-сервера в маршрутизатор

В примере 16.10 используются другой маршрутизатор и TFTP-сервер, а также предоставлена дополнительная информация об операциях, которые выполняются для копирования образа Cisco IOS с TFTP-сервера на маршрутизатор.

Как показано в примере 16.10, после ввода команды **copy tftp flash** система запрашивает IP-адрес (или имя) TFTP-сервера. Этот адрес или имя может быть установлено на другом маршрутизаторе, который предоставляет образ программного обеспечения из своей оперативной памяти или из Flash-памяти. Далее система запрашивает имя файла образа Cisco IOS.
В примере 16.10 показана выводимая устройством информация при копировании образа системы с именем C4500-I во Flash-память.

Пример 16.10. Копирование образа IOS Cisco с TFTP-сервера на маршрутизатор

```
Router# copy tftp flash
IP address or name of remote host [255.255.255.255]? 172.16.13.111
Name of tftp filename to copy into flash []? c4500-I
copy C4500-I already exists; it will be invalidated!
Copy C4500-I from 172.16.13.111 into flash memory? [confirm]
xxxxxxxx bytes available for writing without erasure.
erase flash before writing? [confirm]
Clearing and initializing flash memory [please wait] ####...##
Loading from 172.16.13.111: !!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
! Часть выводимого текста удалена
[OK – 324572/524212 bytes]
Verifying checksum...
VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
```

```
VVVVVVVVV
! Часть выводимого текста удалена
Flash verification successful. Length = 1204637, checksum = 0x95D9
```

При попытке скопировать во Flash-память файл, который там уже находится, появляется сообщение, в котором говорится о том, что файл с таким именем уже существует. При копировании нового файла во Flash-память такой файл будет уничтожен. Если во Flash-памяти достаточно места для обеих копий, то первая по-прежнему остается во Flash-памяти, но станет неиспользуемой в пользу новой версии; при использовании команды **show flash** она будет помечена тегом [deleted] (файл "удален").

Если прервать процесс копирования, то новый файл будет помечен как удаленный (deleted), поскольку он не был скопирован полностью, и, следовательно, недействителен. В таком случае первоначальный файл остается резидентным во Flash-памяти и доступным для системы.

Практическое задание 16.2.5. Управление образами операционной системы IOS с помощью TFTP-сервера

В этой работе необходимо сделать резервную копию образа Cisco IOS маршрутизатора на TFTP-сервере. После этого следует перезагрузить резервную копию с сервера во Flash-память маршрутизатора.

Управление образами программного обеспечения Cisco IOS с помощью протокола Xmodem

Если образ программного обеспечения Cisco IOS Cisco был удален или поврежден, его можно восстановить в режиме монитора памяти ROM (ROM monitor mode — ROMmon, или ROM-монитор). Во многих аппаратных структурах Cisco режим монитора ROMmon характеризуется наличием в командной строке служебного слова `rommon>`.

Первым действием в этом процессе восстановления операционной системы является выяснение того, почему образ Cisco IOS не загрузился из Flash-памяти. Проблема может быть вызвана повреждением файла или отсутствием образа, либо повреждением самой Flash-памяти. Для анализа ситуации следует выполнить команду **dir flash:**.

Если при этом будет обнаружен образ, который выглядит как действительный, то следует попытаться загрузить систему из этого образа. Эта попытка загрузки осуществляется с помощью команды **boot flash:**. Например, если имя образа `c2600-is-mz.121-5`, то вводимая команда будет иметь вид:

```
rommon > boot flash:c2600-is-mz.121-5
```

Если загрузка маршрутизатора прошла успешно, следует выполнить некоторые действия, для того чтобы выяснить, почему маршрутизатор загрузился в режиме ROMmon вместо использования программного обеспечения из Flash-памяти. Сначала нужно выполнить команду **show version** для проверки того, что в регистре конфигурации задана правильная последовательность стандартной загрузки. Если значение регистра конфигурации правильно, следует выполнить команду **show**

start-config. С помощью этой команды можно посмотреть, есть ли в файле конфигурации команда **boot system**, указывающая маршрутизатору на необходимость использовать программное обеспечение Cisco IOS для режима ROMmon.

Если маршрутизатор не загружается из образа или образ отсутствует, необходимо загрузить новый образ программного обеспечения Cisco IOS. Восстановить файл программного обеспечения IOS Cisco можно с помощью протокола Xmodem и консоли либо путем загрузки образа с TFTP-сервера в режиме ROMmon.

Загрузка образа Cisco IOS с помощью протокола Xmodem в режиме ROMmon

Для восстановления образа операционной системы Cisco IOS с помощью консоли на локальном персональном компьютере должна быть подлежащая восстановлению копия файла программного обеспечения IOS и программа эмуляции терминала, такая, например, как HyperTerminal. Восстановление образа системы IOS может быть выполнено на стандартной скорости консоли 9600 Бод. Для ускорения загрузки скорость можно увеличить вплоть до значения 115200 Бод. Скорость передачи в консоли можно изменить в режиме ROMmon с помощью команды **confreg**. После ввода команды **confreg** маршрутизатор запросит различные параметры, которые могут быть изменены, как показано в примере 16.11.

Пример 16.11. Изменение скорости передачи консоли

```
rommon 1 >confreg
Configuration Summary
! Часть выводимой информации опущена.
console baud: 9600
boot: the ROM Monitor
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]:
! Часть выводимой информации опущена.
enable "ignore system config info"? y/n [n]:
change console baud rate? y/n [n]: y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400
4 = 19200, 5 = 38400, 6 = 57600, 7 = 115200 [0]: 7
change the boot characteristics? y/n [n]:

Configuration Summary
enabled are:
break/abort has effect
console baud: 115200
boot: the ROM Monitor

do you wish to change the configuration? y/n [n]:
```

Для того чтобы новая конфигурация стала действующей, необходимо перезагрузить маршрутизатор или выключить и вновь включить его питание.

При появлении запроса “change console baud rate? y/n [n]:” (“Изменить скорость работы консоли в бодах? д/н [нет]:”)[1] и выборе ответа “y” (“да”) появляется предложение выбрать новую скорость. После изменения скорости консоли следует перезагрузить маршрутизатор и войти в режим ROMmon. При этом сеанс терминала со скоростью 9600 Бод заканчивается и начинается новый сеанс со скоростью 115200 Бод в соответствии со скоростью консоли.

В режиме ROMmon можно использовать команду **xmodem** для восстановления образа программного обеспечения Cisco IOS с персонального компьютера. Команда **xmodem** имеет следующий синтаксис:

xmodem -c image_file_name

Например, для восстановления файла образа с именем c2600-is-mz.122-10a.bin следует ввести команду, показанную в примере 16.12.

Пример 16.12. Восстановление файла образа Cisco IOS с помощью команды xmodem

```
rommon 1 >
rommon 1 >xmodem -?
    xmodem: illegal option -- ?
    usage: xmodem [-cyrx] <destination filename>
    -c CRC-16
              -y ymodem-batch protocol
              -r copy image to dram for launch
              -x do not launch on download completion
rommon 2 > xmodem -c c2600-is-mz.122-10a.bin

Do not start the sending program yet...

                Warning: All existing data in bootflash will be
lost!

Invoke this application only for disaster recovery.
Do you wish to continue? y/n [n]: y
Ready to receive file c2600-is-mz.122-10a.bin ...
```

Ключ —c в команде указывает процессу Xmodem на необходимость использовать контроль с помощью циклического избыточного кода (Cyclic Redundancy Check — CRC) для проверки ошибок при загрузке файла.

При этом на экран будет выведено сообщение от маршрутизатора “не начинать передачу” и отображено предупреждение. Такое сообщение указывает, что область файловой системы **bootflash** будет уничтожена, и маршрутизатор предлагает подтвердить продолжение процесса. Если такое подтверждение поступает, маршрутизатор делает запрос о начале передачи.

[1] *В квадратных скобках практически во всех диалогах системы указан стандартный ответ или установленное ранее значение. — Прим. ред.*

Начало передачи осуществляется с эмулятора терминала. Далее в консольной программе HyperTerminal следует выбрать опцию Передача и потом нажать Отправить. После этого в меню Пересылка файла следует указать имя и местоположение файла образа, выбрать в качестве протокола Xmodem и начать передачу. Процесс передачи отображается в окне Пересылка файла.

После окончания пересылки появляется сообщение о том, что образ во Flash-памяти уничтожен. За ним появляется сообщение "Загрузка завершена!". Перед повторным включением маршрутизатора необходимо установить на консоли прежнюю скорость 9600 Бод и в конфигурационном регистре установить значение 0x2102. Такое значение регистра конфигурации задается с помощью команды **`confreg 0x2102`** и устанавливается в привилегированном режиме EXEC.

При перезапуске маршрутизатора заканчивается сеанс на скорости 115200 Бод и начинается сеанс на стандартной скорости.

Практическое задание 16.2.6a. Процедуры восстановления пароля.
В этом задании необходимо получить полный доступ к устройству, пароль привилегированного режима которого утерян.

Практическое задание 16.2.6b. Управление образом IOS Cisco с помощью режима ROMmon и протокола Xmodem.
В этом практическом задании необходимо восстановить работоспособность маршрутизатора Cisco серии 1700 в режиме ROM-монитора в связи с повреждением или отсутствием образа Cisco IOS во Flash-памяти.

Использование переменных среды

Программное обеспечение Cisco IOS может быть также восстановлено в сеансе протокола TFTP. Самым быстрым способом восстановления образа операционной системы IOS в маршрутизаторе является его загрузка с помощью протокола TFTP в режиме ROMmon. Для этого требуется установить переменные среды и выполнить команду **`tftpdnld`**.

Поскольку режим ROMmon имеет ограниченные функции, при перезагрузке в него файл конфигурации не загружается. По этой причине на маршрутизаторе после загрузки отсутствуют протокол IP и конфигурации интерфейсов. Переменные среды обеспечивают минимальную конфигурацию, которая позволяет использовать протокол TFTP из образа программного обеспечения Cisco IOS. Передача по протоколу TFTP в режиме ROMmon может использоваться только с первым портом сети LAN, поэтому для этого интерфейса устанавливается только простой набор параметров. Для задания значения переменной среды ROMmon следует ввести имя переменной, знак равенства (=) и значение этой переменной (VARIABLE_NAME=значение, т.е. ИМЯ_ПЕРЕМЕННОЙ=значение). Например, для того чтобы установить IP-адрес равным 10.0.0.1, следует ввести в командной строке команду **`IP_ADDRESS=10.0.0.1`**.

ВНИМАНИЕ!

Все переменные среды чувствительны к регистру символов.

Минимально необходимые переменные для использования команды **tftpdnld** приведены ниже.

- **IP_ADDRESS** — IP-адрес LAN-интерфейса.
- **IP_SUBNET_MASK** — маска подсети для LAN-интерфейса.
- **DEFAULT_GATEWAY** — стандартный шлюз для LAN-интерфейса.
- **TFTP_SERVER** — IP-адрес TFTP-сервера.
- **TFTP_FILE** — имя файла программного обеспечения Cisco IOS на TFTP-сервере.

Для проверки установленных переменных среды ROMmon используется команда **set**, как показано в примере 16.13.

Пример 16.13. Проверка переменных среды ROMmon

```
rommon 10> set
IP_ADDRESS=10.0.0.1
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=10.0.0.254
TFTP_SERVER=192.168.1.1
TFTP_FILE=GAD/original_2003_Jan_22/c2600-i-mz.121-5
```

После установки переменных для загрузки программного обеспечения Cisco IOS следует ввести команду **tftpdnld** без аргументов, как показано в примере 16.14. При этом ROMmon отображает значения переменных и в командной строке появляется запрос на подтверждение загрузки с предупреждением, что выполнение этой операции приведет к уничтожению образа во Flash-памяти.

Пример 16.14. Выполнение команды tftpdnld

```
rommon 12 > tftpdnld
IP_ADDRESS: 10.0.0.1
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 10.0.0.254
TFTP_SERVER: 192.168.1.1
TFTP_FILE: GAD/original_2003_Jan_22/c2600-i-mz.121-5
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!
Do you wish to continue? y/n: [n]: y
Receiving GAD/original_2003_Jan_22/c2600-i-mz.121-5 from
192.168.1.1!!!!.!!!!!!!!!!!!!!!!!!!.!!
File reception completed.
Copying file GAD/original_2003_Jan_22/c2600-i-mz.121-5 to flash.
```

```
Erasing flash at 0x607c0000
program flash location 0x60440000
rommon 13>
```

При получении каждой дейтаграммы файла Cisco IOS на экране отображается символ "!". После полной загрузки файла операционной системы IOS образ во Flash-памяти уничтожается и записывается новый файл образа. После завершения процесса на экране отображаются соответствующие сообщения.

После того как новый образ записан во Flash-память и появилась командная строка режима ROMmon, можно снова запустить маршрутизатор путем ввода в командной строке символа "**i**" или введя команду **reset** для перезагрузки устройства. В этом случае загрузка произойдет из нового образа Cisco IOS, находящегося во Flash-памяти.

Проверка файловой системы

Для тестирования файловой системы маршрутизатора могут быть использованы несколько команд. Одной из таких команд является команда **show version**, которая служит для проверки текущего образа системы и объема доступной Flash-памяти. Команда **show version** также указывает источник, из которого была выполнена загрузка маршрутизатора, и отображает значение регистра конфигурации. Значение поля загрузки регистра конфигурации позволяет определить, откуда маршрутизатор может загрузить образ Cisco IOS. Если текущий образ и установка загрузочного поля регистра конфигурации не согласуются друг с другом, то причиной этого может быть повреждение или отсутствие файла образа операционной системы Cisco IOS во Flash-памяти или наличие в стартовой конфигурации команд **boot system**.

В примере 16.15 показано применение команды **show version**.

Пример 16.15. Тестирование файловой системы маршрутизатора

```
HMH# show version
Cisco Internetwork Operating System Software
IOS (tm) 1700 Software (C1700-BNSY-L), Version 12.2(11)P, RELEASE
SOFTWARE (fc1)

! Часть выводимой устройством информации опущена

System image file is "flash:c1700-bnsy-l.122-11.p", booted via flash
Cisco 171 (68360) processor (revision C) with 3584K/512K bytes of
memory.
Processor board ID 12014633, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
2 serial(sync/async) network interface(s)
System/IO memory with parity disabled
2048K bytes of DRAM onboard 2048K bytes of DRAM on SIMM
```

```
System running from FLASH
8K bytes of non-volatile configuration memory.
6144K bytes of processor board PCMCIA flash (Read ONLY)
Configuration register is 0x2102
HMH#
```

Для тестирования файловой системы, идентификации образа Cisco IOS или образов во Flash-памяти, а также количества доступной Flash-памяти может быть использована команда **show flash**. Команда **show flash** часто используется для того, чтобы проверить наличие достаточного количества памяти для сохранения нового образа IOS Cisco. В примере 16.16 приведен тот же вывод, что и в примере 16.15, но полученный с помощью команды **show flash**.

Пример 16.16. Выводимая командой show flash информация

```
Router# show flash
4096 bytes of flash memory on embedded flash (in XX).
file offset length name
0 0x40 1204637 xk09140z
[903848/2097152 bytes free]
```

Как уже говорилось, файл конфигурации может содержать команды **boot system**. Они могут быть использованы для задания желательного источника загрузочного образа программного обеспечения IOS Cisco. Для указания резервной последовательности для обнаружения и загрузки образа программного обеспечения Cisco IOS могут быть использованы несколько команд **boot system**. Эти команды **boot system** обрабатываются в порядке их расположения в файле конфигурации.

Резюме

В этой главе были рассмотрены следующие ключевые темы:

- выбор стандартного источника для загрузки программного обеспечения Cisco IOS зависит от аппаратной платформы, однако чаще всего для поиска источника маршрутизатор просматривает память NVRAM в поисках команд конфигурирования;
- для отображения версии операционной системы Cisco IOS, работающей в настоящий момент в маршрутизаторе, используется команда **show version**;
- для задания резервной последовательности загрузки операционной системы Cisco IOS можно ввести несколько команд **boot system**. Маршрутизаторы могут загружать операционную систему из Flash-памяти, с TFTP-сервера и из памяти ROM;
- проверить, достаточно ли доступного объема памяти для загрузки программного обеспечения Cisco IOS, можно с помощью команды **show flash**;

- при использовании программного обеспечения Cisco IOS версии 11.2 или более поздних используются специальные соглашения об именах файлов. Эти имена состоят из трех частей:
  - кода аппаратной платформы, для которой предназначена данная версия программного обеспечения;
  - кода специальных функций данной версии;
  - кода местоположения данной версии системы и указание на то, является ли она сжатой;
- копия программного обеспечения может быть скопирована на сетевой сервер. Эта копия может быть использована в качестве резервной, а также для проверки того, что копия во Flash-памяти совпадает с первоначальным файлом;
- при необходимости загрузки резервной версии Cisco IOS следует использовать вариацию команды **copy** — команду **copy tftp flash** для загрузки образа, ранее размещенного на TFTP-сервере.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Ключевые термины

Процедура начальной самозагрузки (bootstrap) представляет собой последовательность действий, выполняемых устройством после включения питания, в частности, в такую процедуру может входить установка IP-адресов Ethernet-интерфейсов маршрутизатора, которая влияет на дальнейшую загрузку системы (например, загрузка операционной системы выполняется по сети).

Flash-память (Flash memory) — специализированный тип памяти EEPROM (Electrically Erasable Programmable Read-Only Memory — электронно-перепрограммируемая постоянная память), содержимое которой может быть стерто и перепрограммировано заново блоками, в отличие от обычной побайтовой записи. Во многих современных персональных компьютерах BIOS-функции (Basic Input/Output System — базовая система ввода/вывода) хранятся во Flash-памяти, что позволяет при необходимости обновлять их. Такая микросхема BIOS иногда называется Flash-BIOS (Flash BIOS). Flash-память также широко используется в модемах, поскольку она позволяет производителям модемов поддерживать новые протоколы по мере того, как они становятся стандартами.

Энергонезависимая оперативная память (NonVolatile Random-Access Memory — NVRAM) представляет собой память RAM (Random-Access Memory — оперативная память), содержимое которой сохраняется при отключении питания.

Оперативная память (random-access memory — RAM) — это память, которая функционирует только при включенном питании, ее содержимое может записываться и считываться микропроцессором.

Протокол удаленного копирования (Remote Copy Protocol — RCP) представляет собой механизм, который позволяет копировать файлы как с удаленного сервера на локальный узел, так и в обратном направлении.

Простой протокол передачи файлов (Trivial File Transfer Protocol — TFTP) — упрощенная версия протокола FTP, позволяющая передавать по сети файлы от одного компьютера на другой, обычно без какой-либо аутентификации клиента (например, запроса имени пользователя и пароля).

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. Какое из приведенных ниже действий правильно указывает, как маршрутизатор должен загрузить программное обеспечение Cisco IOS?
   а) Задать резервные источники, которые маршрутизатор будет последовательно использовать, начиная с памяти NVRAM.
   б) Сконфигурировать образ Cisco IOS для того местоположения, где он будет выполнять процедуру начальной самозагрузки.
   в) Вручную загрузить стандартный образ системы посредством виртуального терминала.
   г) Вручную загрузить стандартный образ системы с использованием сетевого сервера.
2. Какое из приведенных ниже действий не является опцией загрузки операционной системы Cisco IOS, которая может быть установлена в загрузочном поле конфигурационного регистра?
   а) Программное обеспечение Cisco IOS загружается в режиме монитора ROM.
   б) Программное обеспечение Cisco IOS автоматически загружается из оперативной памяти ROM.
   в) Программное обеспечение Cisco IOS автоматически загружается с сервера TFTP.
   г) Команды загрузки **`boot system`** ищутся в памяти NVRAM.

3. В каком из приведенных ответов правильно указана информация, отображаемая после выполнения команды **`show version`**?

   а) Подробная статистика о каждой странице памяти маршрутизатора.

   б) Имя образа системы.

   в) Имена и размеры всех файлов, находящихся во Flash-памяти.

   г) Состояние всех сконфигурированных сетевых протоколов.

4. Какая из приведенных ниже команд используется для того, чтобы узнать текущее значение конфигурационного регистра?

   а) **`show register.`**

   б) **`show running-config.`**

   в) **`show version.`**

   г) **`show startup-config.`**

5. В каком из приведенных ответов правильно указана информация, **не** предоставляемая именем файла образа операционной системы Cisco IOS?

   а) Функции образа операционной системы.

   б) Платформа, для которой предназначен этот образ.

   в) Где запускается этот образ.

   г) Размер образа.

6. Какое из приведенных действий не является частью стандартной рекомендуемой процедуры загрузки образа программного обеспечения Cisco IOS во Flash-память с TFTP-сервера? (Действия перечислены в правильном порядке.)

   а) Создание резервной копии текущего образа программного обеспечения на сервере TFTP.

   б) Ввод команды **`copy flash tftp`** для начала загрузки нового образа системы с сервера.

   в) Ответ на запрос процедуры о согласии пользователя стереть содержимое Flash-памяти.

   г) Отображение на дисплее ряда символов “V”, указывающих на успешный результат проверки контрольной суммы.

7. Каким будет начальное действие устройства, если конфигурационный регистр при загрузке содержит значение 0x2101?

   а) Устройство переходит в режим начальной настройки (Setup mode).

   б) Устройство пытается загрузиться с TFTP-сервера.

   в) Устройство пытается загрузиться из памяти ROM.

   г) Устройство пытается загрузиться из Flash-памяти.

8. В каком из приведенных ниже компонентов содержится ограниченная версия программного обеспечения Cisco IOS для маршрутизатора?

а) Память ROM.

б) Flash-память.

в) Сервер TFTP.

г) Набор микросхем для начальной загрузки (Bootstrap).

9. Каким будет начальное действие, если в конфигурационном регистре при загрузке содержится значение 0x2102?

а) Устройство пытается загрузиться из Flash-памяти.

б) Устройство пытается загрузиться с TFTP-сервера.

в) Устройство пытается загрузиться из памяти ROM.

г) Устройство ищет команды **`boot system`**.

10. Какая из приведенных последовательностей загрузки используется маршрутизатором как стандартная процедура поиска программного обеспечения Cisco IOS?

а) Flash-память, память NVRAM, сервер TFTP.

б) Память NVRAM, сервер TFTP, Flash-память.

в) Память NVRAM, Flash-память, сервер TFTP.

г) Flash-память, сервер TFTP, память ROM.

11. Что из приведенного ниже не отображается на экране при выполнении команды операционной системы Cisco IOS **`show version`**?

а) Статистика для сконфигурированных интерфейсов.

б) Тип платформы, на которой работает программное обеспечение Cisco IOS.

в) Текущее значение конфигурационного регистра.

г) Версия программного обеспечения Cisco IOS.

12. Какое из приведенных выражений правильно описывает подготовку TFTP-сервера к копированию программного обеспечения во Flash-память?

а) TFTP-сервер должен представлять собой подсоединенный маршрутизатор или узел, такой, как рабочая станция UNIX или переносной компьютер.

б) TFTP-сервер должен быть подсоединен к сети Ethernet.

в) Должно быть задано имя маршрутизатора, содержащего Flash-память.

г) Должна присутствовать Flash-память.

13. Для чего создается резервная копия образа операционной системы Cisco IOS?

а) Для проверки того, что во Flash-памяти находится та же копия, которая загружена в память ROM.

б) Для создания резервной копии текущего образа перед копированием нового образа операционной системы на новый маршрутизатор.

в) Для создания резервной копии текущего образа в качестве части операций, выполняемых при восстановлении системы после системного сбоя.

г) Для создания резервной копии текущего образа перед переходом на новую версию Cisco IOS.

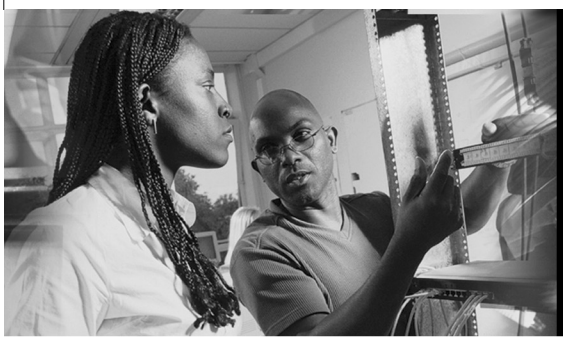
14. Какую из приведенных команд необходимо выполнить в том случае, когда требуется обновить существующую версию операционной системы Cisco IOS путем загрузки нового образа с TFTP-сервера?

а) `boot system tftp 131.21.11.3.`

б) `copy tftp flash.`

в) `show flash.`

г) `tftp ios.exe.`



ГЛАВА 17

Маршрутизация и протоколы маршрутизации

В этой главе...

- рассмотрены основные принципы маршрутизации;
- описаны различия между маршрутизируемыми сетевыми протоколами и протоколами маршрутизации;
- описаны внутренние и внешние протоколы маршрутизации;
- представлено сравнение статических и динамических маршрутов;
- рассказано, как создавать статические маршруты;
- описан процесс конфигурирования стандартных маршрутов;
- описаны некоторые методы поиска ошибок в сконфигурированных статических маршрутах;
- разъяснена необходимость в динамических протоколах маршрутизации;
- описана дистанционно-векторная маршрутизация;
- описана маршрутизация с учетом состояния каналов;
- рассмотрен вопрос выбора протокола маршрутизации в зависимости от конкретной ситуации.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

маршрутизация, с. 758,
статическая маршрутизация, с. 759,
тупиковая сеть, с. 759,
административное расстояние, с. 761,
динамическая маршрутизация, с. 768,
распределение нагрузки, с. 769,
метрика, с. 770,
маршрутизируемый протокол, с. 772,
протокол маршрутизации, с. 772,
автономная система, с. 773,
дистанционно-векторный протокол, с. 774,
протокол с учетом состояния канала, с. 774,
сбалансированный гибридный протокол, с. 774,
анонсы состояния канала, с. 777,
топологическая база данных, с. 778,
алгоритм выбора кратчайшего пути, с. 778,
таблица маршрутизации, с. 778,
протокол внутреннего шлюза, с. 790,
протокол внешнего шлюза, с. 790.

В этой главе подробно рассматриваются вопросы использования маршрутизаторов и операции, выполняемые основными функциями сетевого (третьего) уровня эталонной модели OSI (Open System Interconnection reference model). Кроме того, в главе рассмотрены различия между сетевыми (маршрутизируемыми) протоколами и протоколами маршрутизации, а также различные способы определения маршрутизатором расстояния между двумя сетевыми узлами. В заключение подробно рассматриваются различные типы протоколов маршрутизации: дистанционно-векторный, по состоянию канала и гибридный, а также решение ими типичных задач маршрутизации.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Введение в статическую маршрутизацию

Маршрутизация представляет собой выбор направлений передачи данных от одной сети другой. Эти направления, также называемые маршрутами, могут предоставляться динамически другими маршрутизаторами. Однако они могут также назначаться маршрутизатору статически. В данном разделе рассматривается назначение маршрутов вручную сетевым администратором.

Основы маршрутизации

Маршрутизация представляет собой процесс, который используется маршрутизатором для пересылки пакета в сеть получателя. Маршрутизатор принимает решения, основываясь на IP-адресе получателя пакета. Для того чтобы переслать пакет в требуемом направлении, все устройства на пути его следования используют IP-адрес получателя. Этот адрес позволяет пакету достичь требуемого пункта назначения. Для принятия правильного решения маршрутизаторы должны знать направления к удаленным сетям. При использовании динамической маршрутизации это направление к удаленным сетям маршрутизатор узнает от других маршрутизаторов сети. При использовании статической маршрутизации информация об удаленных сетях задается вручную сетевым администратором.

Поскольку статические маршруты конфигурируются вручную, любые изменения сетевой топологии требуют участия сетевого администратора для добавления и удаления статических маршрутов в соответствии с этими изменениями. В крупных сетях такая ручная поддержка таблиц маршрутизации может потребовать огромных затрат времени сетевого администратора. В небольших сетях, в которых изменения незначительны, поддержка статических маршрутов особых затрат не требует. Статическая маршрутизация не обладает возможностями масштабирования, имеющимися у динамической маршрутизации, из-за дополнительных требований к настройке и необходимости вмешательства администратора. Однако и в крупных сетях часто конфигурируются статические маршруты для специальных целей в комбинации с

протоколом динамической маршрутизации. Несмотря на то что динамические протоколы маршрутизации могут автоматически определять маршруты, для этого они все же должны быть сначала активизированы и сконфигурированы сетевым администратором. В последующих разделах будут рассмотрены различные подходы к маршрутизации.

Дополнительная информация: сравнение статических и динамических маршрутов

Информация статических маршрутов вводится в конфигурацию маршрутизатора вручную сетевым администратором. В каждом случае, когда изменение топологии объединенной сети требует обновления статических маршрутов, это обновление должно выполняться вручную сетевым администратором.

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

Для чего нужны статические маршруты?

Статическая маршрутизация имеет несколько полезных приложений. При динамической маршрутизации имеется тенденция к распространению всей информации об объединенной сети. Однако по соображениям безопасности иногда требуется скрыть некоторые части сети. *Статическая маршрутизация* (*static routing*) позволяет пользователю указать, какая информация может распространяться относительно таких скрытых сетей с ограниченным доступом.

Если доступ к сети может быть получен только по одному маршруту, то одного статического маршрута может оказаться вполне достаточно. Такой тип сети носит название *тупиковой сети (stub network*). Тупиковая сеть представляет собой зону протокола OSPF, в которой имеется стандартный маршрут, маршруты между зонами и внутренние маршруты зоны, однако нет внешних маршрутов. Как показано на рис. 17.1, конфигурирование статического маршрута к тупиковой сети позволяет уменьшить служебную нагрузку динамической маршрутизации (объем пересылки анонсов маршрутизации).

Принцип действия статических маршрутов

Функционирование статических маршрутов может быть описано тремя положениями.

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

Поскольку статический маршрут конфигурируется вручную, для его установки на маршрутизаторе сетевой администратор должен ввести соответствующую команду **`ip route`**. Эта команда имеет следующий синтаксис:

```
Router(config)# ip route prefix mask { ip-address | interface-type
interface-number}[ distance ]
```

На рис. 17.2 сетевому администратору маршрутизатора *Hoboken* требуется сконфигурировать статический маршрут к сетям 172.16.1.0/24 и 172.16.5.0/24, подсоединенным к другим маршрутизаторам.

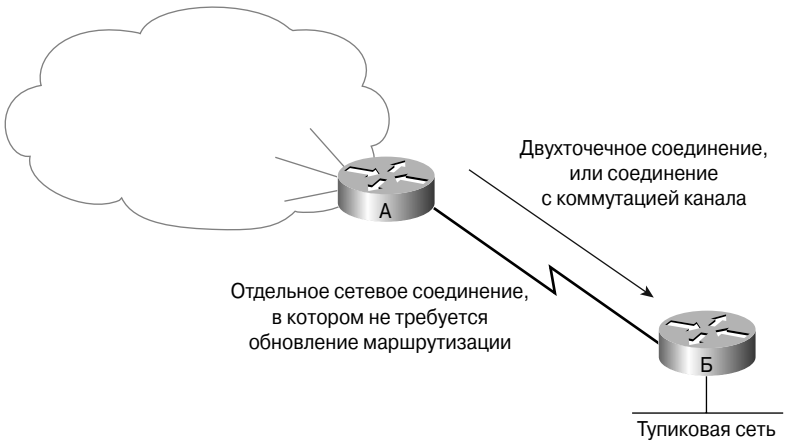


Рис. 17.1. Принцип действия статического маршрута

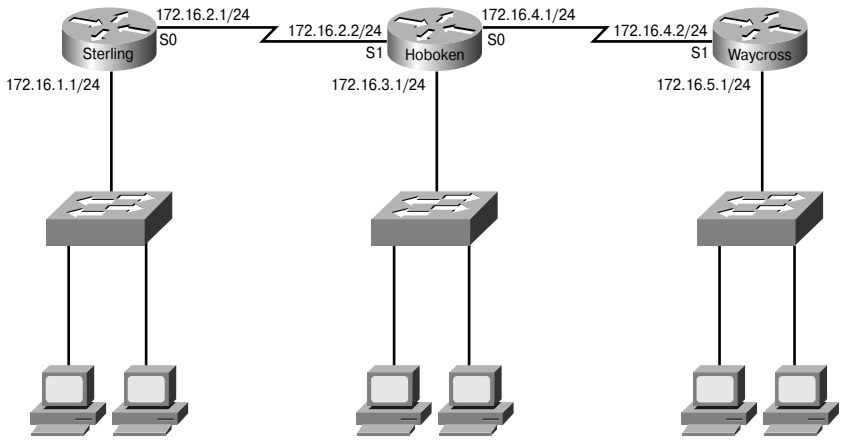


Рис. 17.2. Статические маршруты

Для решения этой задачи сетевой администратор может ввести одну или две команды. В примере 17.1 для этого указывается выходной интерфейс (Serial 0). В примере 17.2 указывается IP-адрес смежного (соседнего) маршрутизатора (172.16.2.2). Любая из этих команд задает статический маршрут в таблице маршрутизации маршрутизатора *Hoboken*.

Пример 17.1. Статический маршрут с использованием интерфейса

```
Sterling(config)# ip route 172.16.3.0 255.255.255.0 s0
```

Пример 17.2. Статический маршрут с использованием IP-адреса маршрутизатора следующего перехода

```
Sterling(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.2
```

Единственным различием между этими двумя командами является *административное расстояние (administrative distance*), назначаемое маршруту при его занесении в таблицу маршрутизации. Под административным расстоянием понимается необязательный параметр, который характеризует надежность маршрута. Меньшему значению административного расстояния соответствует менее надежный маршрут. Такое утверждение означает, что маршрут с меньшим административным расстоянием будет установлен в таблицу маршрутизации прежде, чем маршрут с бо́льшим административным расстоянием. Стандартно при использовании адреса следующего перехода административное расстояние устанавливается равным 1. При задании выходного интерфейса для административного расстояния устанавливается значение 0. В табл. 17.1 приведены административные расстояния для каждого поддерживаемого протокола. Маршрутам с меньшим административным расстоянием отдается предпочтение по сравнению с аналогичными маршрутами с большим административным расстоянием. Если требуется установить административное расстояние, отличающееся от стандартного, то следует ввести значение в интервале от 0 до 255 после адреса следующего перехода или указания выходного интерфейса, как показано ниже.

```
ip route 172.16.3.0 255.255.255.0 192.168.2.1 255
```

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

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

Таблица 17.1. Административные расстояния в операционной системе Cisco IOS

Источник маршрута	Стандартное значение административного расстояния
Подсоединенный интерфейс	0
Статический маршрут	1
Суммарный маршрут протокола EIGRP (Enhanced Interior Gateway Routing Protocol)	5
Протокол BGP (External Border Gateway Protocol)	20
Внутрениий маршрут протокола EIGRP	90
Протокол IGRP	100
Протокол OSPF	110
Протокол IS-IS (Intermediate System-to-Intermediate System)	115
Протокол RIP (Routing Information Protocol)	120
Протокол EGP (Exterior Gateway Protocol)	140
Внешние маршруты протокола EIGRP	170
Внутренние маршруты BGP	200
Неизвестен	255

Конфигурирование статических маршрутов

В этом разделе описаны действия, которые необходимо выполнить для конфигурирования статических маршрутов, и приведен Пример простой сети, в которой требуется сконфигурировать статические маршруты. Чтобы сконфигурировать статические маршруты, необходимо выполнить описанные ниже действия.

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

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

192.168.0.0/24

192.168.1.0/24

192.168.2.0/24

192.168.3.0/24

Этап 2. Войти в режим глобального конфигурирования.

Этап 3. Ввести команду **`ip route`** с адресом сети-получателя и маской подсети, за которыми следует адрес следующего транзитного узла (о нем говорилось на этапе 1). Указание административного расстояния не является обязательным.

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

Этап 5. Выйти из режима глобального конфигурирования.

Этап 6. Сохранить активную конфигурацию в памяти NVRAM с помощью команд **`copy running-config startup-config`** и **`write memory`**[1].

В сети, которая показана на рис. 17.3, представлена простая структура с тремя маршрутизаторами. Маршрутизатор *Hoboken* должен быть сконфигурирован таким образом, чтобы он обеспечивал доступ к сетям с адресами 172.16.1.0 и 172.16.5.0. В обеих сетях маска подсети имеет вид 255.255.255.0.

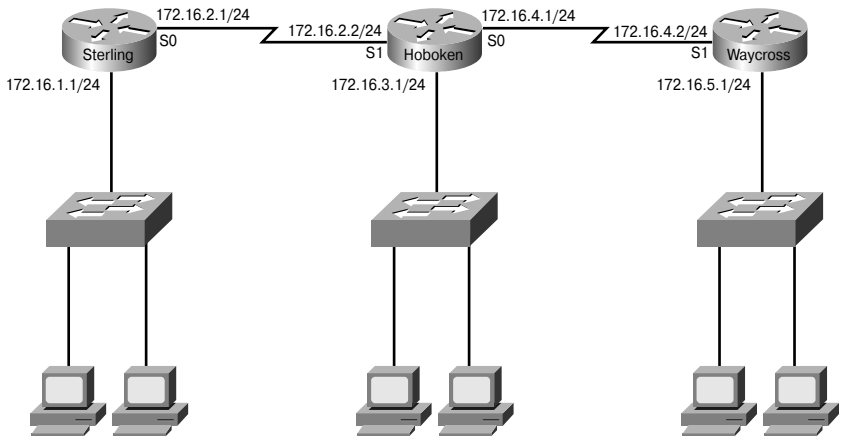


Рис. 17.3. Функционирование статических маршрутов

Пакеты, у которых получателем является сеть 172.16.1.0, требуется направлять на маршрутизатор *Sterling*. Пакеты, у которых получателем является сеть 172.16.5.0, требуется направлять на маршрутизатор *Waycross*. Для этого необходимо сконфигурировать статические маршруты с использованием выходных интерфейсов маршрутизатора S0 и S1, как показано в примере 17.3.

[1] *Эта команда считается устаревшей; в операционной системе версии 12.0 и выше рекомендуется применять первую команду. — Прим. ред.*

Пример 17.3. Задание выходных интерфейсов IP-маршрутов

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0
```

Оба статических маршрута конфигурируются с использованием локального интерфейса в качестве шлюза к сетям-получателям, как показано на рис. 17.4. Поскольку административное расстояние не указано, при занесении маршрутов в таблицу маршрутизации оно стандартно принимается равным нулю. Следует обратить внимание на то, что административное расстояние, равное нулю, также присуще непосредственно подсоединенной сети.

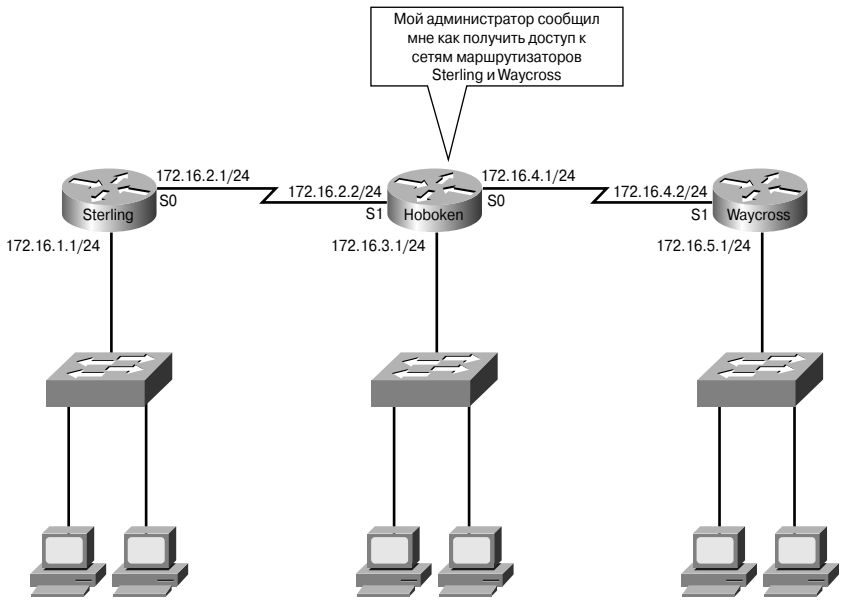


Рис. 17.4. Статические маршруты, сконфигурированные сетевым администратором

Те же статические маршруты могут быть сконфигурированы с использованием в качестве шлюза адреса следующего перехода. Первый маршрут к сети 172.16.1.0 проходит через шлюз 172.16.2.1. У сети 172.16.5.0 шлюз имеет адрес 172.16.4.2. В примере 17.4 показано, как сконфигурировать статические маршруты с использованием адреса интерфейса следующего транзитного перехода; в него включены комментарии (которым предшествует символ "!"), которые не будут отображены в файле конфигурации. Поскольку административное расстояние явным образом не задано, стандартно оно устанавливается равным единице.

Пример 17.4. Статические маршруты с использованием адреса следующего транзитного перехода и комментариями

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

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

Дополнительная информация: использование стандартных маршрутов

На рис. 17.5 показано использование стандартного маршрута, т.е. позиции в таблице маршрутизации, которая указывает адрес следующего перехода в том случае, когда такой переход явно не указан в таблице маршрутизации. Стандартные маршруты могут быть установлены как часть процесса конфигурирования статических маршрутов.

В данном примере у маршрутизаторов компании “X” имеется информация о топологии сети этой компании, однако отсутствует информация о топологии других сетей. Поддержка информации о топологии всех других сетей, к которым можно получить доступ через среду Internet, не является необходимой, а во многих случаях она просто невозможна.

Вместо того чтобы хранить информацию обо всех сетях, каждый маршрутизатор компании “X” имеет стандартный маршрут, который используется для получения доступа к неизвестным сетям-получателям путем непосредственной пересылки пакетов в среду Internet.

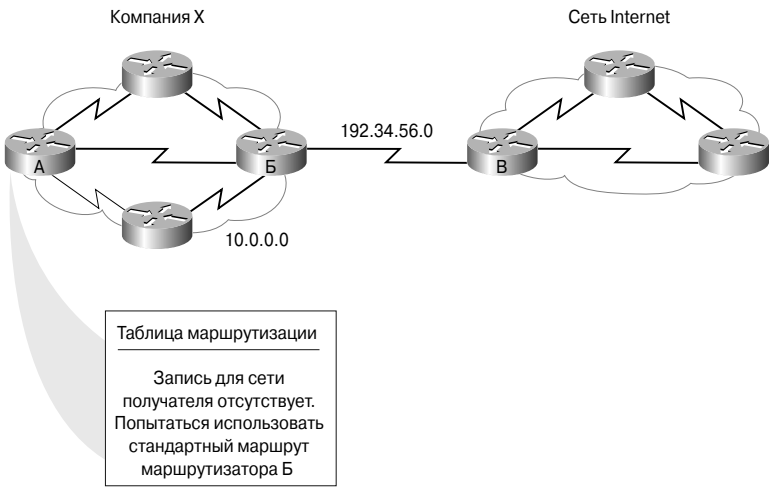


Рис. 17.5. Конфигурирование статического маршрута с использованием адреса следующего транзитного перехода

Конфигурирование пересылки пакетов по стандартному маршруту

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

```
ip route 0.0.0.0 0.0.0.0 [ next-hop-address | outgoing interface]
```

ВНИМАНИЕ!

Операция логического "И" (AND) над маской 0.0.0.0 и IP-адресом пакета всегда дает результатом сеть 0.0.0.0. Если для пакета в таблице маршрутизации не находится точного соответствия сети-получателя, он направляется в сеть с адресом 0.0.0.0.

Для конфигурирования маршрутов по умолчанию необходимо выполнить описанные ниже действия.

Этап 1. Войти в режим глобальной конфигурации.

Этап 2. Ввести в командной строке команду **`ip route`** с адресом 0.0.0.0 для сети-получателя и значением 0.0.0.0 для маски подсети. Шлюзом стандартного маршрута может быть либо локальный интерфейс маршрутизатора, через который осуществляется связь с внешними сетями, либо адрес маршрутизатора следующего перехода. В большинстве случаев предпочтительнее задавать IP-адрес маршрутизатора следующего перехода.

Этап 3. Выйти из режима глобального конфигурирования.

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

На рис. 17.2 было показано конфигурирование статических маршрутов для маршрутизатора *Hoboken* к маршрутизатору *Sterling* сети 172.16.5.0 и маршрутизатору *Waycross* сети 172.16.1.0. Теперь требуется, чтобы пакеты для этих сетей могли быть отправлены с маршрутизатора *Hoboken* по стандартному маршруту. Однако при текущей конфигурации маршрутизаторы *Sterling* и *Waycross* не обладают информацией о том, как вернуть пакеты в сеть, к которой они непосредственно не подсоединены. На каждом из этих маршрутизаторов (*Sterling* и *Waycross*) могут быть сконфигурированы статические маршруты к сетям-получателям, с которыми они не имеют непосредственного соединения, однако в крупной сети такое решение не позволяет масштабировать ее.

Маршрутизатор *Sterling* подсоединяется ко всем сетям, которые с ним непосредственно не соединены, через интерфейс s0. Маршрутизатор *Waycross* также имеет только одно соединение со всеми непосредственно к нему не подсоединенными сетями. Это соединение осуществляется через последовательный интерфейс Serial 1. Как показано на рис. 17.6, указание стандартного маршрута для маршрутизаторов *Sterling* и *Waycross* позволяет им осуществлять маршрутизацию всех пакетов, направляемых в сети, которые непосредственно к этим маршрутизаторам не подсоединены. В примерах 17.5 и 17.6 приведены команды, которые требуется выполнить для конфигурирования стандартных маршрутов для маршрутизаторов *Waycross* и *Sterling* соответственно.

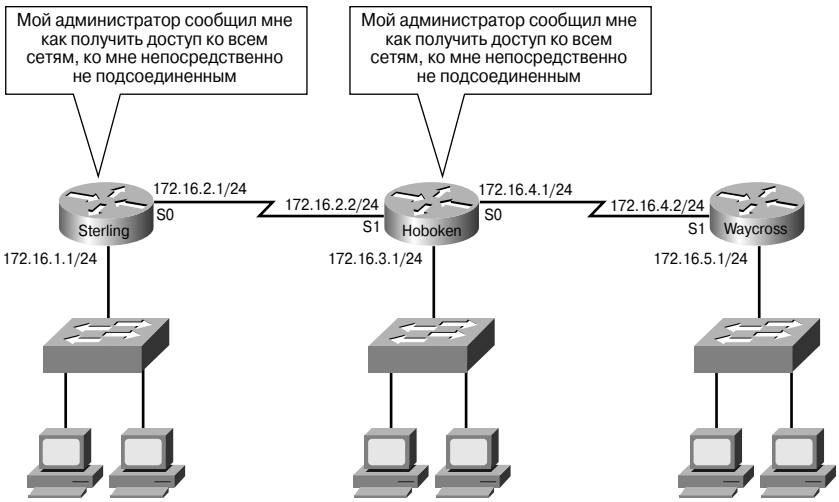


Рис. 17.6. Статический маршрут для маршрутизатора Waycross

Пример 17.5. Стандартный маршрут для маршрутизатора Waycross

```
Waycross(config)# ip route 0.0.0.0 0.0.0.0 s1
```

Пример 17.6. Стандартный маршрут для маршрутизатора Sterling

```
Sterling(config)# ip route 0.0.0.0 0.0.0.0 s0
```

Проверка статических маршрутов

После того как статические маршруты сконфигурированы, важно проверить, что они находятся в таблице маршрутизации и пересылка пакетов по ним осуществляется требуемым образом. Для просмотра активной конфигурации в памяти NVRAM и проверки правильности ввода статических маршрутов используется команда **show**

running-config. Для проверки наличия маршрута в таблице маршрутизации используется команда **show ip route**.

Для тестирования конфигурации статических маршрутов следует выполнить описанные ниже действия.

Этап 1. В привилегированном режиме ввести команду **show running-config** для просмотра активной конфигурации.

Этап 2. Проверить правильность строк статических маршрутов. Если маршрут введен неправильно, следует вернуться в режим глобального конфигурирования, удалить неверный маршрут и ввести правильный.

Этап 3. Ввести команду **show ip route**.

Этап 4. Проверить, что сконфигурированный маршрут находится в таблице маршрутизации.

Устранение ошибок в конфигурации статических маршрутов

Знание средств и процедур, используемых для поиска ошибок в статической маршрутизации, столь же важно, как и во всех других аспектах работы с сетями. Для проверки состояния и конфигурации интерфейса, который будет использоваться в качестве шлюза для маршрута, служит команда **show interfaces**. Команда **ping** позволяет проверить наличие сквозного соединения между конечными точками маршрута. Если после выполнения команды **ping** эхо-ответ не поступает, следует использовать команду **traceroute** для выяснения того, на каком маршрутизаторе, находящемся на пути следования пакета, последний теряется.

Процесс маршрутизации должен выполняться на каждом маршрутизаторе, через который проходит пакет, в противном случае этот пакет будет отброшен. Во многих случаях пакеты достигают пункта назначения, однако последний маршрутизатор удаленной сети не знает маршрута, по которому следует отправить ответное сообщение.

Для поиска и устранения ошибок в конфигурировании статических маршрутов необходимо выполнить перечисленные ниже действия.

Этап 1. Удостовериться в том, что доступен канал, который будет использоваться в качестве шлюза для маршрута.

Этап 2. Ввести команду **show interfaces** и удостовериться в активности интерфейса и канального протокола.

Этап 3. Проверить правильность IP-адреса, используемого на интерфейсе.

Этап 4. Выполнить команду **ping** для IP-адреса интерфейса удаленного маршрутизатора, непосредственно подсоединенного к шлюзу маршрута. Если результат выполнения этой команды окажется отрицательным, то проблема не связана с маршрутизацией. Возможно, интерфейсы одного или обоих непосредственно подсоединенных маршрутизаторов сконфигурированы неправильно или в канале существуют физические проблемы. В этом случае следует снова выполнить действия этапа 1,

чтобы найти и устранить ошибки.

Этап 5. Если команда **`ping`** не срабатывает на маршрутизаторе, расположенном на дальнем конце, необходимо выполнить команду **`traceroute`** для определения того узла на маршруте, на котором теряется пакет.

Этап 6. Подсоединиться к маршрутизатору, на котором не сработала трассировка маршрута, с помощью команды **`traceroute`**. После этого следует повторить действия этапа 1.

Этап 7. Если команда **`ping`** сработала успешно, нужно выполнить ее для маршрутизатора на дальнем конце маршрута. Если результат будет успешным, то полное сквозное соединение установлено, и тест статического маршрута можно считать законченным.

Практическое задание 17.1.6. Использование статических маршрутов
В этой лабораторной работе требуется сконфигурировать статические маршруты между маршрутизаторами, для того чтобы стала возможной передача данных между ними без использования протоколов динамической маршрутизации.

Обзор динамической маршрутизации

Администратор сети выбирает динамический протокол маршрутизации, исходя из множества предпосылок. Прежде всего во внимание принимаются такие характеристики, как размер сети, доступная полоса пропускания соединений, аппаратные возможности процессоров маршрутизирующих устройств, модели и типы маршрутизаторов, а также типы протоколов, которые используются в сетях. В этом разделе основное внимание уделено отличиям разных протоколов маршрутизации и тому, как они влияют на принимаемое сетевым администратором решение.

Дополнительная информация: динамическая маршрутизация

Динамическая маршрутизация (dynamic routing) необходима для того, чтобы сети могли обновлять свои таблицы маршрутизации и быстро адаптироваться к изменениям в топологии и состоянии соединений. Показанная на рис. 17.7 сеть по-разному адаптируется к изменениям топологии, в зависимости от того, какой тип маршрутизации используется: динамическая или статическая.

Статическая маршрутизация позволяет переслать пакет из одной сети в другую на основе вручную заданных маршрутов. В данном примере маршрутизатор А всегда пересылает потоки данных, предназначенные маршрутизатору В, через маршрутизатор Г. Маршрутизатор обращается к своей таблице маршрутизации и в соответствии с находящейся там информацией о статическом маршруте направляет пакет на узел пункта назначения.

Если маршрут от маршрутизатора А к маршрутизатору Г по какой-либо причине становится недоступным, то маршрутизатор А не может передать пакет маршрутизатору Г по нему. Соответственно, до повторного ручного конфигурирования маршрутизатора А на передачу пакетов через маршрутизатор Б связь с сетью-получателем будет невозможной. Динамическая маршрутизация обеспечивает большую гибкость. В соответствии с таблицей маршрутизации, созданной на маршрутизаторе А, пакет может быть доставлен к пункту назначения по более предпочтительному маршруту через маршрутизатор Г.

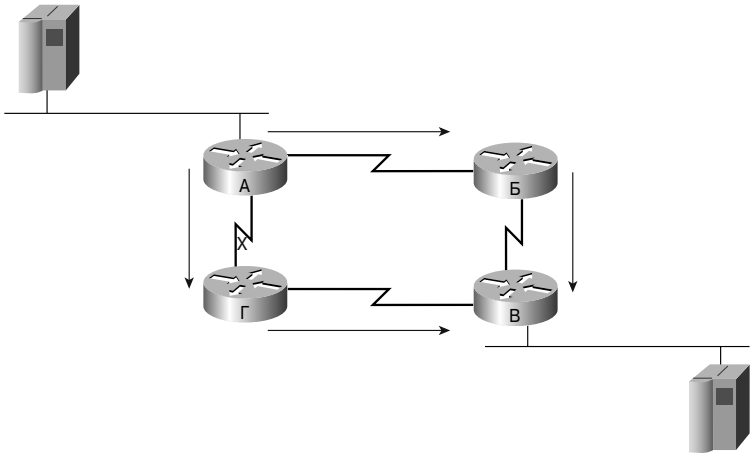


Рис. 17.7. Динамический маршрут

Однако при этом остается доступным и второй путь к пункту назначения — через маршрутизатор Б. Когда маршрутизатор А узнает о том, что канал к маршрутизатору Г вышел из строя, он обновит свою таблицу маршрутизации, делая маршрут через маршрутизатор Б предпочтительным маршрутом к пункту назначения. В этом случае маршрутизаторы продолжают пересылку пакетов по такому каналу.

После того как маршрут между маршрутизаторами А и Г восстановлен, маршрутизатор А снова обновляет свою таблицу маршрутизации, отдавая предпочтение маршруту к получателю против часовой стрелки, т.е. через маршрутизаторы Г и В. Протоколы динамической маршрутизации могут также для повышения эффективности работы сети направлять потоки данных одного и того же сеанса по нескольким маршрутам. Этот механизм представляет собой *распределение нагрузки (load sharing*) между несколькими каналами и устройствами.

Операции динамической маршрутизации

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

- поддержки таблицы маршрутизации в актуальном состоянии;
- своевременного распространения информации в виде анонсов и обновлений маршрутов среди остальных маршрутизаторов (рис. 17.8).

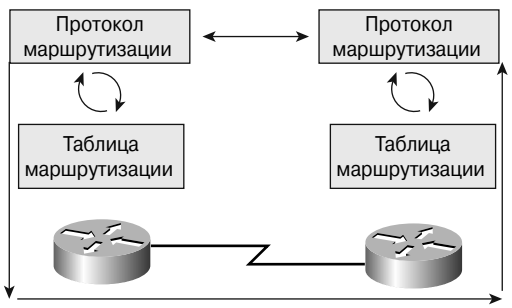


Рис. 17.8. Протоколы маршрутизации поддерживают информацию о маршрутах

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

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

Определение длины сетевых маршрутов с помощью различных метрик

При обновлении алгоритмом маршрутизации таблицы маршрутизации первичной задачей устройства является выбор наилучшего маршрута для включения его в таблицу. Каждый алгоритм маршрутизации использует свой собственный способ выбора наилучшего маршрута. Для этого он генерирует определенное значение, называемое *метрикой (metric*), для каждого маршрута в сети. Обычно чем меньше значение метрики, тем лучше маршрут, как показано на рис. 17.9.

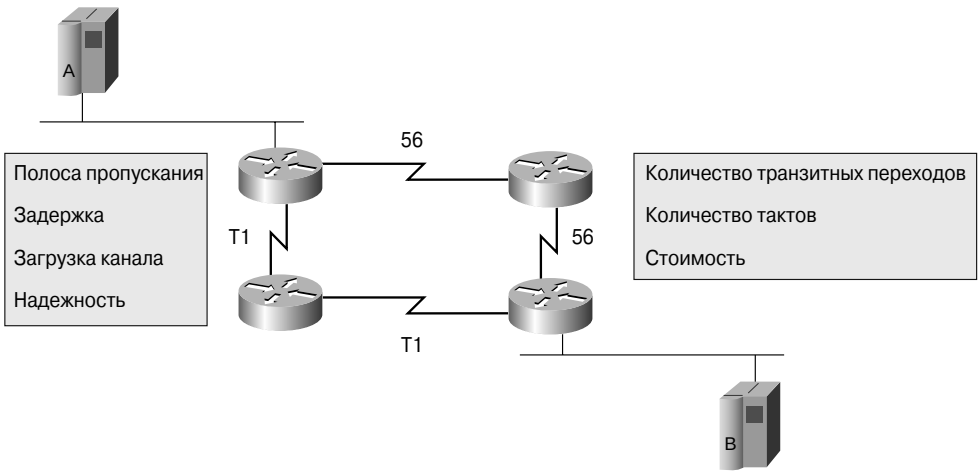


Рис. 17.9. Метрики, используемые для определения наилучшего маршрута

Могут использоваться простые метрики, которые вычисляются на основе одной характеристики, такой, например, как количество переходов на маршруте, или более сложные метрики, использующие несколько параметров маршрутов. Ниже перечислены наиболее часто используемые в метриках характеристики.

- **Полоса пропускания (Bandwidth**) описывает пропускную способность канала (обычно канал Ethernet со скоростью 10 Мбит/с предпочтительнее выделенной линии со скоростью 64 Кбит/с).
- **Задержка (Delay**) представляет собой время, требуемое пакету для прохождения по каналу от отправителя до получателя.
- **Назрузка (Load**) — это степень использования сетевых ресурсов на маршрутизаторе или канале.
- **Надежность (Reliability**) обычно характеризует уровень ошибок в сетевом канале.
- **Количество переходов (Hop count)** — это число маршрутизаторов, через которые должен пройти пакет до поступления в пункт назначения.

- **Стоимость (Cost)** представляет собой произвольное значение, обычно вычисляемое на основе ширины полосы пропускания, финансовых затрат или других характеристик, выбираемых сетевым администратором.

Введение в протоколы маршрутизации

В этом разделе приведен краткий обзор некоторых наиболее часто используемых протоколов маршрутизации и их важнейшие характеристики.

Протоколы маршрутизации отличаются от маршрутизируемых протоколов как по своим функциям, так и по задачам, которые перед ними ставятся. Протокол маршрутизации — это средство коммуникации между маршрутизаторами, которое позволяет устройствам совместно использовать информацию о сетях и определять расстояние до разных узлов и сетей. Информация, которую один маршрутизатор получает от другого (посредством протокола маршрутизации), используется для построения и поддержания в актуальном состоянии таблицы маршрутизации.

К наиболее распространенным протоколам маршрутизации локальных сетей можно отнести следующие:

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

Маршрутизируемые протоколы (часто их называют протоколами передачи данных) используются для доставки пользовательской информации. Маршрутизируемый протокол содержит достаточное количество информации в адресе сетевого уровня, которую позволит доставить от одного узла другому в рамках используемой схемы адресации.

К наиболее распространенным маршрутизируемым протоколам сетей можно отнести следующие:

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

По причине внешней похожести двух терминов — *маршрутизируемые протоколы* и *протоколы маршрутизации* — часто возникает путаница (рис. 17.10). Ниже подробно объяснены различия между этими терминами.

- *Маршрутизируемый (routed protocol)*, *или сетевой, протокол — это* любой сетевой протокол, предоставляющий в своем адресе сетевого уровня достаточно информации для пересылки пакета от одного узла другому на основе используемой схемы адресации. Маршрутизируемые протоколы определяют форматы полей внутри пакета. Пакеты обычно передаются от одной конечной системы другой. Для пересылки пакетов маршрутизируемый протокол использует

таблицу маршрутизации. Примером такого протокола может служить протокол Internet (Internet Protocol — IP).

- *Протокол маршрутизации (routing protocol)* — это протокол, который обеспечивает работу маршрутизируемого протокола, предоставляя механизмы совместного использования информации о маршрутах. Для этого между маршрутизаторами передаются сообщения протоколов маршрутизации. Протокол маршрутизации позволяет маршрутизаторам осуществлять связь друг с другом для поддержки и обновления таблиц маршрутизации. Ниже перечислены протоколы маршрутизации, используемые стеком протоколов TCP/IP:
  - протокол маршрутной информации (Routing Information Protocol — RIP);
  - протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP);
  - усовершенствованный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP);
  - протокол обнаружения первого кратчайшего пути (Open Shortest Path First — OSPF).

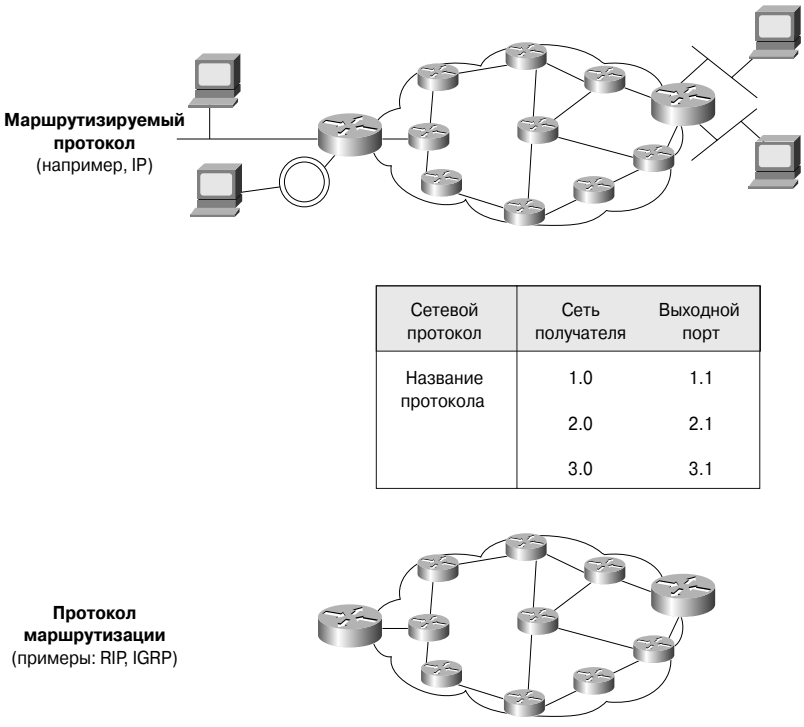


Рис. 17.10. Маршрутизаторы и протоколы маршрутизации

Автономные системы

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

Американский реестр Internet-номеров (American Registry of Internet Numbers — ARIN), провайдер службы или сетевой администратор присваивает номер (идентификатор) каждой автономной системе. Идентификатор автономной системы представляет собой шестнадцатибитовое число. Некоторые протоколы маршрутизации, такие, как фирменные протоколы IGRP и EIGRP корпорации Cisco, используют такое понятие, как "номер автономной системы" в своей конфигурации; в действительности же нет никакой необходимости устанавливать туда реальный номер. Этот параметр представляет собой просто идентификатор процесса. Для двух указанных протоколов маршрутизации нет необходимости использовать номер системы, который получен от реестра ARIN, или частный номер автономной системы.

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

Назначение протоколов маршрутизации и цели использования автономных систем

Целью использования протокола маршрутизации является построение и поддержка таблицы маршрутизации. В этой таблице содержатся информация об известных маршрутизатору сетях и соответствующие порты, ведущие к этим сетям. Маршрутизаторы используют протоколы маршрутизации для управления информацией, полученной от других маршрутизаторов, и информацией, получаемой из конфигурации своих собственных интерфейсов.

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

Основой динамической маршрутизации является алгоритм маршрутизации. При любом изменении топологии сети, связанном с ее увеличением, реконфигурацией или выходом из строя устройств, информация о сети должна быть обновлена. Она должна точно и последовательно отражать текущее состояние новой топологии сети.

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

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

Идентификация класса протокола маршрутизации

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

- дистанционно-векторный протокол;
- протокол с учетом состояния канала.

Дистанционно-векторный протокол (distance vector routing protocol) определяет направление, или вектор, и расстояние до нужного узла объединенной сети. *Протокол с учетом состояния канала (link-state routing protocol*), также называемый алгоритмом выбора кратчайшего пути (shortest path first — SPF), воссоздает топологию всей сети. *Сбалансированный гибридный протокол (balanced hybrid routing protocol*) соединяет в себе определенные черты обоих алгоритмов: дистанционно-векторного и с учетом состояния канала.

Особенности дистанционно-векторных протоколов

При использовании дистанционно-векторных алгоритмов между маршрутизаторами они периодически пересылают копии таблиц маршрутизации друг другу. В таких регулярных обновлениях маршрутизаторы сообщают друг другу об изменениях в топологии сети. Дистанционно-векторные алгоритмы маршрутизации также называются алгоритмами Беллмана-Форда (Bellman-Ford).

На рис. 17.11 каждый маршрутизатор получает таблицу маршрутизации от соседних маршрутизаторов. В частности, маршрутизатор Б получает информацию от маршрутизатора А. Маршрутизатор Б добавляет значение вектора расстояния, количество переходов, что увеличивает результирующий вектор расстояния. После этого маршрутизатор Б передает свою новую таблицу маршрутизации своему соседу, маршрутизатору В. Такой пошаговый процесс происходит на всех соседних маршрутизаторах.

В дистанционно-векторном алгоритме накапливаются расстояния в сети, что позволяет поддерживать базу данных, содержащую информацию о топологии сети. Однако дистанционно-векторные алгоритмы не предоставляют маршрутизаторам точную топологию всей сети, поскольку каждому маршрутизатору известны только соседние с ним маршрутизаторы.

Каждый маршрутизатор, использующий дистанционно-векторную маршрутизацию, начинает свою работу с определения соседних маршрутизаторов. На рис. 17.12 проиллюстрировано формирование вектора расстояния. Для каждого интерфейса, ведущего к непосредственно подсоединенной сети, вектор расстояния устанавливается

равным нулю. По мере того, как процесс расчета вектора расстояния продолжается, маршрутизаторы находят наилучший маршрут к сетям-получателям на основе информации, которую они получают от своих соседей. Например, маршрутизатор А узнает о других сетях на основе информации, которую он получает от маршрутизатора Б. В каждой из позиций таблицы маршрутизации есть суммарный вектор расстояния, который показывает, на каком расстоянии находится соответствующая удаленная сеть.

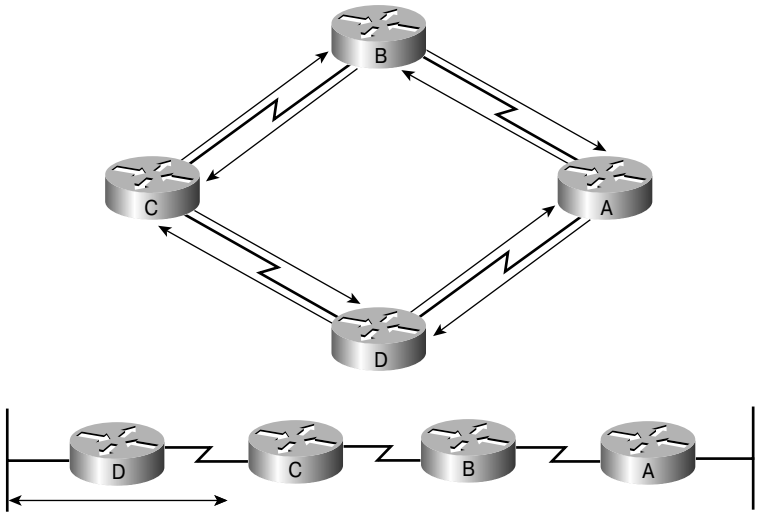


Рис. 17.11. Концепция дистанционно-векторной маршрутизации

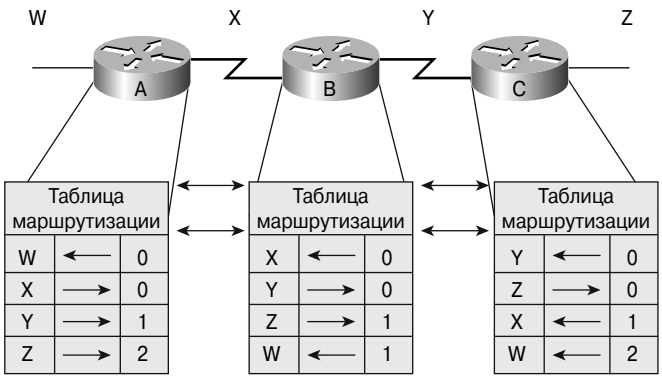


Рис. 17.12. Процесс построения структуры сети в дистанционно-векторном протоколе маршрутизации

Обновление таблицы маршрутизации происходит при изменении топологии сети. По мере формирования векторов расстояния изменения топологии заносятся в таблицы маршрутизации последующих маршрутизаторов, как показано на рис. 17.13. Дистанционно-векторные алгоритмы требуют, чтобы каждый маршрутизатор пересылал всю таблицу маршрутизации каждому из своих соседей. В этой таблице содержатся общая оценка маршрута, определяемая метрикой, и логический адрес первого маршрутизатора на пути к каждой сети, имеющейся в таблице. Значение метрики составляется из нескольких компонентов, как показано на рис. 17.14.

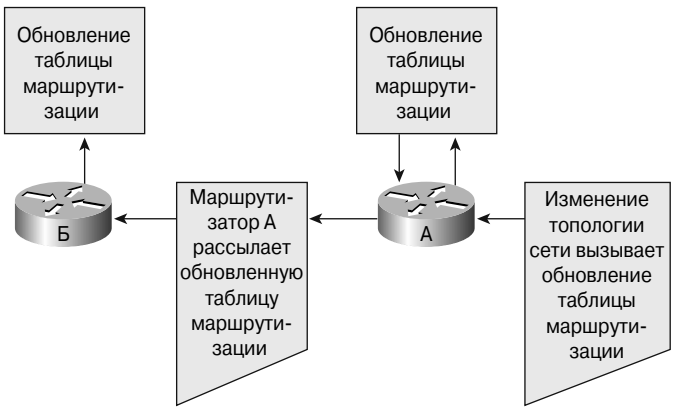


Рис. 17.13. Обработка изменений топологии дистанционно-векторным протоколом маршрутизации

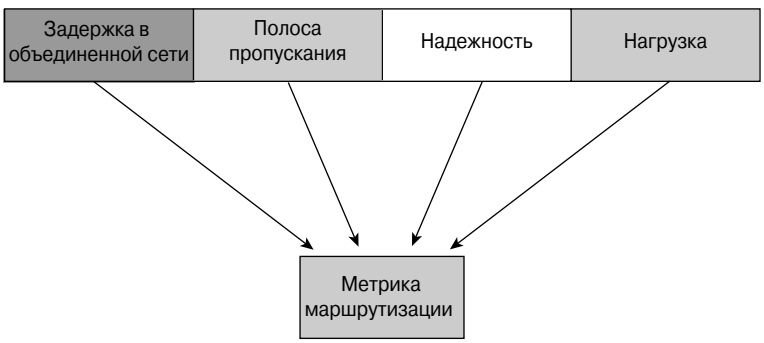


Рис. 17.14. Компоненты метрики дистанционно-векторного протокола

Обновления маршрутов

Каждый маршрутизатор получает таблицу маршрутизации от соседних, непосредственно подсоединенных к нему маршрутизаторов. Например, как показано на рис. 17.13, маршрутизатор Б получает информацию от маршрутизатора А. Маршрутизатор Б добавляет свое значение к вектору расстояния (например, количество переходов) и передает новую таблицу маршрутизации соседнему маршрутизатору.

Подобный пошаговый процесс происходит между всеми соседними маршрутизаторами.

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

Основы маршрутизации по состоянию канала

Вторым базовым алгоритмом маршрутизации является алгоритм выбора маршрута по состоянию канала. Такие алгоритмы известны как алгоритмы Дейкстры (Dijkstra) или как алгоритмы выбора кратчайшего пути (Shortest Path First — SPF). Они поддерживают сложную базу топологической информации. В то время, как дистанционно-векторные алгоритмы не содержат определенной информации об удаленных сетях и удаленных маршрутизаторах, алгоритмы с использованием состояния канала поддерживают полную информацию об удаленных маршрутизаторах и их соединениях друг с другом. При маршрутизации по состоянию канала используются следующие компоненты:

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

Такая концепция маршрутизации на основе состояния канала была реализована в протоколе маршрутизации, называемом протоколом выбора первого кратчайшего пути (Open Shortest Path First — OSPF). Основные положения и операции протокола состояния канала связи OSPF описаны в документе RFC 1583.

На рис. 17.15 проиллюстрированы основные концепции маршрутизации на основе состояния канала.

Процесс обнаружения сетей для маршрутизации по состоянию канала

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

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

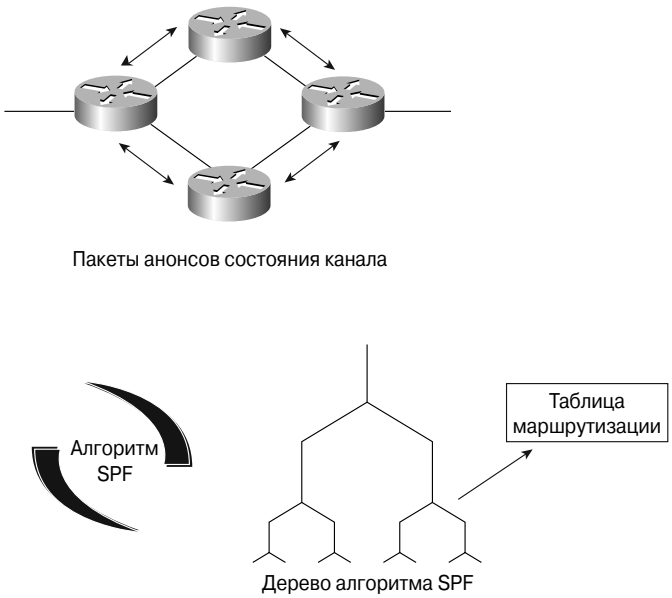


Рис. 17.15. Концепции маршрутизации на основе состояния канала

Обмен информацией о маршрутах в протоколах с учетом состояния каналов

Для создания общей картины всей сети в протоколах с учетом состояния каналов используются специализированные механизмы обнаружения сетей. Такая подробная информация совместно используется всеми маршрутизаторами объединенной сети. Информацию о топологии можно сравнить с наличием нескольких идентичных карт города. На рис. 17.16 четыре сети (W, X, Y и Z) соединены между собой с помощью трех маршрутизаторов, на которых работает протокол с маршрутизацией по состоянию канала. Для обнаружения сетей в протоколе маршрутизации по состоянию канала используются перечисленные ниже процессы.

1. Маршрутизаторы обмениваются друг с другом LSA-сообщениями. Каждый маршрутизатор начинает построение своей таблицы маршрутизации с непосредственно подсоединенных к нему сетей, от которых он получает информацию непосредственно, “из первых рук”.

2. Каждый маршрутизатор параллельно с остальными создает топологическую базу данных, состоящую из информации, полученной из всех LSA-сообщений объединенной сети.
3. Алгоритм SPF вычисляет доступность сетей. Маршрутизатор строит логическую топологию в виде дерева, корнем которого является он сам, а ветвями — все возможные маршруты ко всем сетям, входящим в объединенную сеть протокола состояния канала. Позже маршруты сортируются с использованием алгоритма выбора кратчайшего пути (Shortest Path First — SPF).
4. Маршрутизатор заносит наилучшие маршруты и ведущие к ним порты в свою таблицу маршрутизации. Маршрутизатор также поддерживает другие базы данных топологических элементов и информации о состоянии каналов.

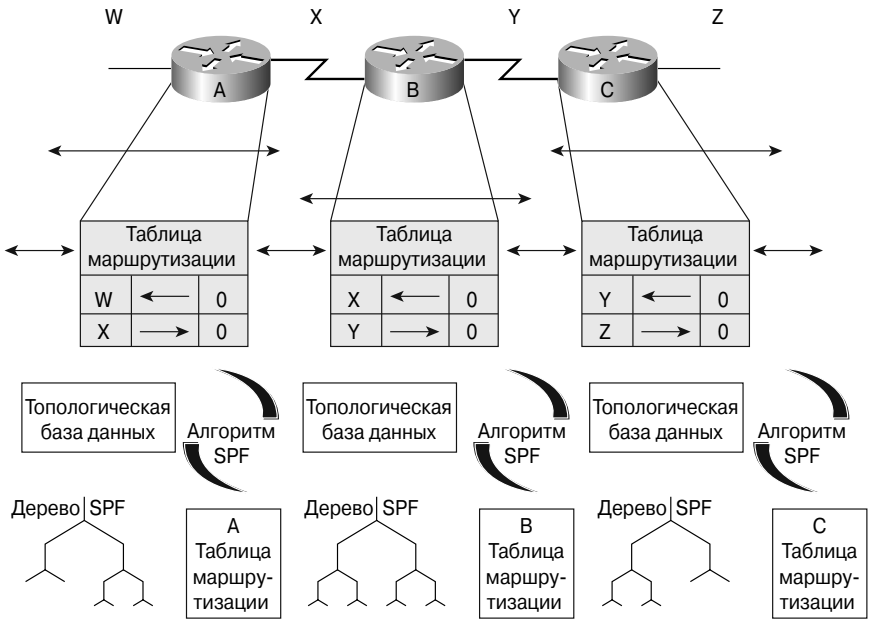


Рис. 17.16. Вычисление кратчайшего пути алгоритмом состояния канала

Если маршрутизатор узнает об изменении состояния канала, он рассылает эту информацию всем остальным маршрутизаторам объединенной сети с тем, чтобы они могли ее использовать для маршрутизации. Для того чтобы закончилась конвергенция, каждый маршрутизатор поддерживает информацию о соседних маршрутизаторах, их именах, состоянии интерфейсов и стоимости каналов к соседним устройствам. Маршрутизатор создает пакет LSA, в котором содержится перечисленная информация наряду с информацией о новых соседях, изменениях в стоимостях каналов и о каналах, которые перестали функционировать. Затем этот пакет LSA направляется всем остальным маршрутизаторам. На рис. 17.17 проиллюстрирован

Пример изменений в топологии сети и реакция на них протокола с учетом состояния канала.

При получении маршрутизатором пакета LSA его база данных обновляется в соответствии с последней полученной информацией. Накопленные данные используются для создания карты объединенной сети, а алгоритм SPF вычисляет кратчайшие пути к другим сетям. При получении каждого пакета LSA, содержащего изменения, алгоритм SPF заново вычисляет наилучшие маршруты и обновляет свою таблицу маршрутизации. При определении наилучшего маршрута для использования при маршрутизации пакетов каждый маршрутизатор принимает во внимание изменения топологии объединенной сети.

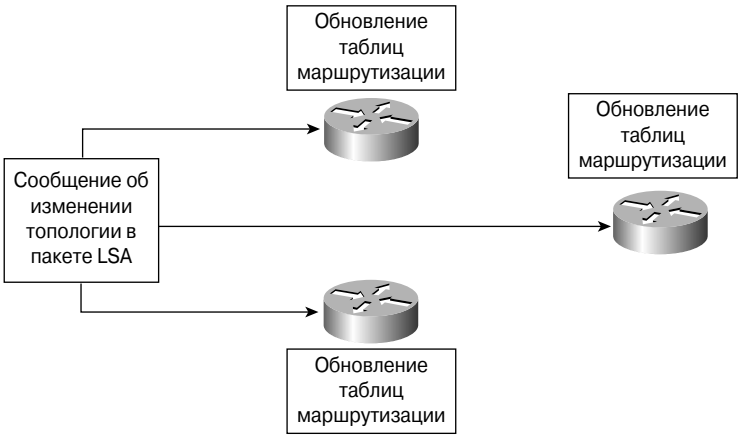


Рис. 17.17. Изменения в топологии сети и реакция протокола с учетом состояния канала

Три проблемы в протоколах состояния канала

При использовании протоколов состояния канала возникают три основные проблемы:

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

Маршрутизаторы, на которых работают протоколы с учетом состояния канала, требуют большего объема памяти и выполняют больший объем обработки данных, чем при использовании дистанционно-векторного протокола маршрутизации. Как показано на рис. 17.18, маршрутизаторы должны иметь достаточно памяти для сохранения большого объема информации в различных базах данных, поддержки топологического дерева и таблицы маршрутизации. Первоначальные потоки маршрутных данных о состоянии каналов занимают большую часть полосы пропускания,

поскольку в первоначальной фазе обнаружения сетей все маршрутизаторы, использующие протоколы с маршрутизацией по состоянию канала, рассылают друг другу пакеты LSA. Эта рассылка в значительной степени заполняет сеть и временно уменьшает полосу пропускания, доступную для передачи данных пользователей. После этого временного переполнения протоколы состояния канала обычно требуют лишь минимальной полосы пропускания для рассылки нечастых или вызванных особыми изменениями в сети пакетов LSA, отражающих эти изменения.

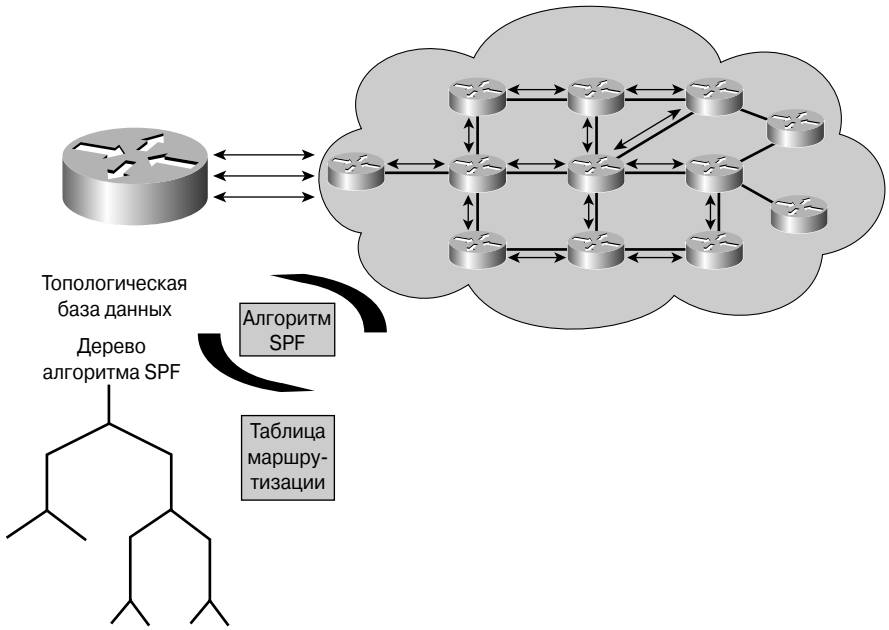


Рис. 17.18. Проблемы протоколов состояния канала

Дополнительная информация: функции гибридных протоколов маршрутизации

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

Как и протоколы состояния канала связи, сбалансированные гибридные протоколы обладают быстрой сходимостью. Однако они отличаются от дистанционно-векторных протоколов и от протоколов с учетом состояния канала связи тем, что они в меньшей степени используют полосу пропускания, память и создают меньшую нагрузку на процессор для обработки служебной информации. Примером гибридного протокола может служить усовершенствованный протокол внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP).

Обзор протоколов маршрутизации

В текущем разделе основное внимание уделено особенностям протоколов маршрутизации. Основные темы этого раздела включают в себя:

- механизм определения пути маршрутизатором;
- конфигурирование процесса маршрутизации;
- примеры протоколов маршрутизации;
- сравнение протоколов внешнего и внутреннего шлюзов.

Дополнительная информация: механизм определения маршрута

Определение маршрутов для потоков данных, проходящих по сетевой среде, осуществляется на сетевом (третьем) уровне модели OSI. Функция определения маршрута позволяет маршрутизатору оценить различные маршруты к месту назначения пакета и выбрать оптимальный способ его обработки. При оценке различных маршрутов службы маршрутизации используют информацию о сетевой топологии. Такая информация может быть задана сетевым администратором или собрана маршрутизатором динамически в процессе работы сети.

Сетевой уровень обеспечивает негарантированную сквозную доставку пакетов в объединенных сетях. Для пересылки пакетов от отправителя получателю все устройства, которые работают на сетевом уровне, используют таблицу маршрутизации протокола IP. После того как маршрутизатор определил маршрут, происходит пересылка пакета. Маршрутизатор пересылает принятый на одном из своих интерфейсов пакет на какой-либо другой интерфейс или порт, в соответствии с выбранным для пакета оптимальным маршрутом.

Маршрутизация представляет собой процесс, который используется маршрутизатором для пересылки пакета в сеть получателя. Маршрутизатор принимает решения, основываясь на IP-адресе получателя пакета. Чтобы переслать пакет в требуемом направлении, все устройства на пути следования потока данных используют IP-адрес получателя. Этот адрес позволяет пакету достичь требуемого пункта назначения. Для принятия правильного решения маршрутизаторы должны “знать” направления к удаленным сетям. При использовании динамической маршрутизации это направление к удаленным сетям маршрутизатор получает от других маршрутизаторов в сети. При использовании статической маршрутизации информация об удаленных сетях задается вручную сетевым администратором.

Поскольку статические маршруты конфигурируются вручную, любые изменения сетевой топологии требуют участия сетевого администратора для добавления и удаления статических маршрутов в соответствии с этими изменениями. В крупных сетях такая поддержка таблиц маршрутизации вручную может потребовать огромных затрат времени сетевого администратора. В небольших сетях, в которых изменения незначительны, поддержка статических маршрутов особых затрат не требует. Статическая маршрутизация не обладает возможностями масштабирования, имеющимися у динамической маршрутизации из-за дополнительного требования: для изменения маршрутов необходимо вмешательство администратора. Однако и в крупных сетях часто конфигурируются статические маршруты для специальных целей в комбинации с протоколом динамической маршрутизации. Хотя динамические протоколы маршрутизации могут автоматически определять маршруты, для этого они все же должны быть сначала активизированы и сконфигурированы сетевым администратором.

В следующих разделах рассматриваются различные подходы к маршрутизации:

- процесс выбора маршрута от отправителя к получателю для пакета (маршрутизация);
- адресация;
- выбор маршрута и коммутация пакета;
- маршрутизируемые протоколы и протоколы маршрутизации.

Каким образом маршрутизаторы пересылают пакеты от отправителя получателю

Чтобы сеть работала эффективно, в ней должна существовать связная картина доступных маршрутов между маршрутизаторами. Как показано на рис. 17.19, каждый канал между маршрутизаторами имеет номер, который маршрутизаторы используют в качестве сетевого адреса. Эти адреса должны предоставлять информацию, которая будет использоваться для передачи пакета от отправителя получателю. Используя указанные адреса, на сетевом уровне можно установить соединения для передачи данных между независимыми сетями.

Согласованность адресов третьего уровня во всей объединенной сети также повышает эффективность использования полосы пропускания за счет предотвращения излишнего широковещания. Широковещание вызывает ненужное увеличение объема служебных данных и напрасные затраты мощности всех устройств и каналов, для которых эти данные не предназначены. За счет использования согласованной сквозной адресации для представления маршрута в среде передачи сетевой уровень может определить путь к сети назначения пакета без излишней нагрузки на устройства и каналы объединенной сети, вызываемой широковещанием.

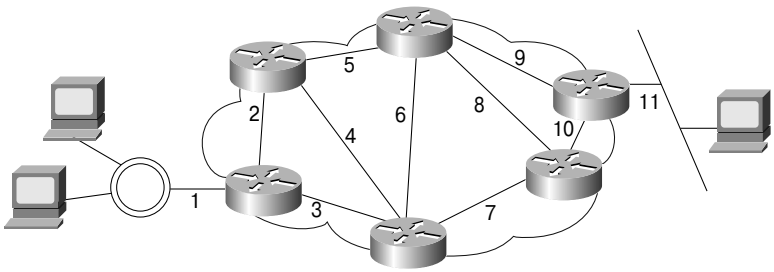


Рис. 17.19. Сетевые адреса

Адресация сетей и их узлов

Маршрутизатор использует адрес сети для нахождения сети-получателя для пакета в объединенной сети. На рис. 17.20 показаны три адреса сетей, указывающих сегменты, подсоединенные к маршрутизатору.

Большинство схем протокольной адресации использует ту или иную форму адреса узла. В некоторых протоколах сетевого уровня сетевой администратор назначает адреса узлов сети в соответствии с заранее определенным планом адресации. В других протоколах сетевого уровня назначение узлам адресов происходит полностью или частично динамическим путем. На рис. 17.20 три узла совместно используют адрес сети 1.

Операции протоколов сетевого уровня

Предположим, приложению узла требуется отправить пакет получателю, находящемуся в другой сети. Такой узел направляет фрейм канального уровня маршрутизатору, используя адрес одного из интерфейсов маршрутизатора. Процесс сетевого уровня (т.е. служба) маршрутизатора анализирует заголовок третьего уровня входящего пакета для определения адреса сети-получателя, а затем просматривает свою таблицу маршрутизации, в которой указаны связи сетей с выходными интерфейсами (рис. 17.21). После этого пакет вновь инкапсулируется во фрейм канального уровня, соответствующий выбранному интерфейсу, и устанавливается в очередь для отправки по выбранному маршруту на следующий транзитный переход.

Указанный выше процесс происходит при каждой пересылке пакета на другой маршрутизатор. Когда пакет поступает на маршрутизатор, непосредственно подсоединенный к локальной сети получателя, он инкапсулируется во фрейм канального уровня, соответствующий типу этой сети.

Сеть	Узел
1	1 2 3
2	1
3	1

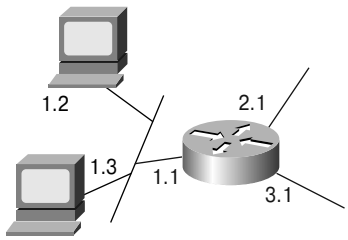


Рис. 17.20. Адреса сетей и их узлов

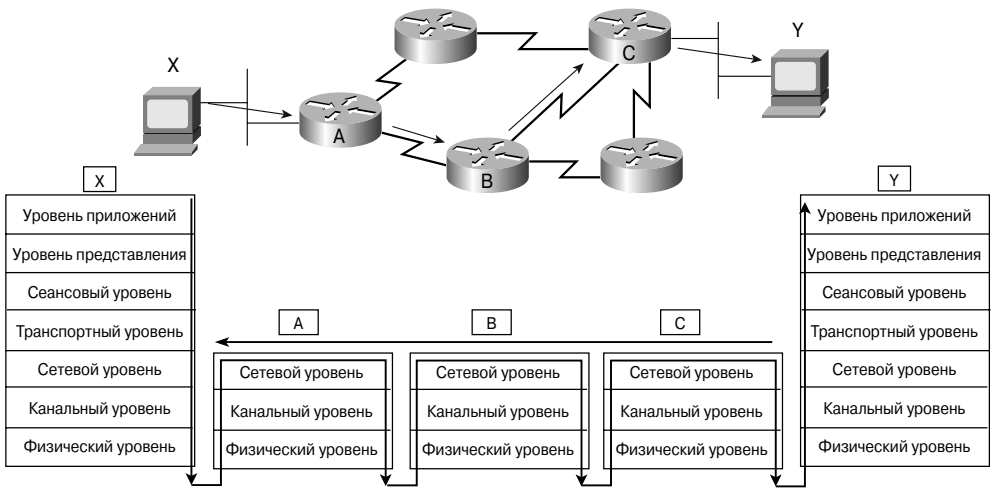


Рис. 17.21. Службы маршрутизаторов

Многопротокольная маршрутизация

Маршрутизаторы могут поддерживать несколько независимых протоколов маршрутизации и соответствующих таблиц маршрутизации. Эта функция позволяет устройству доставлять пакеты нескольких сетевых протоколов по одним и тем же каналам передачи данных (рис. 17.22).

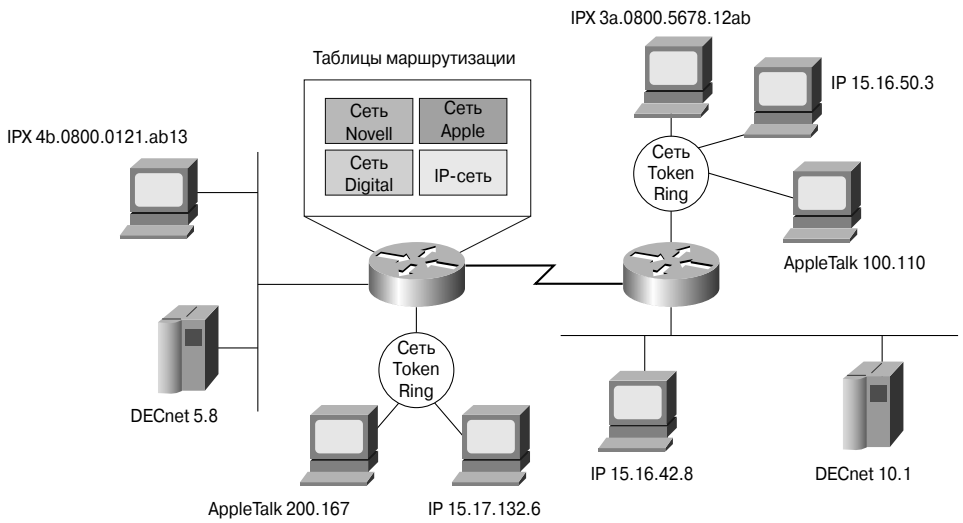


Рис. 17.22. Пересылка маршрутизатором данных нескольких протоколов

Выбор маршрута и коммутация пакетов

Маршрутизатор обычно пересылает пакет из одного канала передачи данных в другой, используя две основные функции:

- функцию определения маршрута;
- функцию коммутации.

На рис. 17.23 показано, как маршрутизаторы используют адресацию для выполнения функций маршрутизации и коммутации. Маршрутизатор использует сетевую часть адреса для выбора маршрута, по которому пакет будет передаваться следующему маршрутизатору. Функция коммутации позволяет маршрутизатору принять пакет на одном из интерфейсов и переслать его далее через другой интерфейс. Функция определения маршрута позволяет маршрутизатору выбрать наиболее подходящий интерфейс для пересылки пакета. Узловая часть адреса используется последним маршрутизатором (маршрутизатором, подсоединенным к сети получателя) для доставки пакета требуемому получателю.

Презентация: механизм определения маршрута
В этой видеопрезентации проиллюстрирован принцип работы механизма определения маршрутов и механизма доставки пакетов из одного соединения передачи данных в другое.

Сеть получателя	Направление пересылки и порт маршрутизатора
1.0	← 1.1
2.0	→ 2.1
3.0	→ 3.1

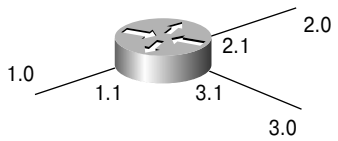


Рис. 17.23. Использование маршрутизатором схемы адресации для выполнения функций маршрутизации и коммутации

Конфигурирование службы маршрутизации

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

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

```
Router(config)#router protocol {process-id | autonomous-system},
```

где

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

Команда **`network`** является необходимой, поскольку она позволяет процессу маршрутизации идентифицировать интерфейсы, которые принимают участие в отправке и получении сообщений обновления маршрутов. Команда **`network`** имеет следующий синтаксис:

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

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

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

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

На Internet-уровне стека протоколов TCP/IP маршрутизатор может использовать протокол IP-маршрутизации для осуществления маршрутизации путем реализации конкретного алгоритма. Примеры протоколов IP-маршрутизации приведены на рис. 17.24:

- **протокол маршрутной информации (Routing Information Protocol — RIP)** — дистанционно-векторный протокол внутренней маршрутизации;
- **протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP)** — дистанционно-векторный протокол маршрутизации, разработанный корпорацией Cisco;
- **протокол выбора первого кратчайшего маршрута (Open Shortest Path First — OSPF)** — протокол внутренней маршрутизации по состоянию канала;
- **усовершенствованный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — IGRP)** — гибридный протокол маршрутизации, разработанный корпорацией Cisco;
- **протокол граничного шлюза (Border Gateway Protocol — BGP)** — протокол внешней маршрутизации.

Рис. 17.24. Протоколы маршрутизации

Примеры протоколов маршрутизации

На Internet-уровне стека протоколов TCP/IP маршрутизатор использует одну из реализаций алгоритма маршрутизации — так называемый протокол маршрутизации.

Протокол RIP был первоначально описан в документе RFC 1058. Ниже перечислены его важнейшие характеристики.

- RIP является дистанционно-векторным протоколом.
- В качестве метрики в этом протоколе используется количество переходов. Если это количество переходов превышает 15, пакет отбрасывается.
- Стандартно обновления маршрутов широковещательно рассылаются каждые 30 секунд.

IGRP представляет собой дистанционно-векторный протокол, разработанный корпорацией Cisco. Он рассылает обновления маршрутов с 90-секундными интервалами, объявляя (анонсируя) маршруты для отдельных автономных систем. Этот протокол имеет следующие характеристики и функции:

- содержит средства многофункционального автоматического анализа неопределенных и сложных топологий;
- предоставляет гибкость при работе с сегментами, имеющими различную ширину полосы пропускания и величину задержки;
- имеет средства масштабирования для работы с крупными сетями.

Стандартно протокол IGRP использует две характеристики в метрике: ширину полосы пропускания и задержку. Он может быть сконфигурирован для использования комбинации переменных в качестве сложной составной метрики. Возможные типы конфигурирования допускают использование следующих параметров:

- ширины полосы пропускания;
- величины задержки;
- нагрузки;
- надежности.

Протокол OSPF представляет собой протокол маршрутизации с учетом состояния каналов. Он используется в стеке IP-протоколов. Протоколы с учетом состояния каналов поддерживают подробную информацию о сетевой топологии, которая позволяет им, выполнив определенные вычисления, предотвращать появление в сети кольцевых маршрутов. При использовании протокола OSPF передается также маска подсети, что позволяет выполнять такие функции, как использование масок переменной длины (Variable-Length Subnet Mask — VLSM) и суммирование или агрегирование (summarization) маршрутов.

Протокол EIGRP представляет собой гибридный протокол маршрутизации, разработанный корпорацией Cisco. Этот протокол имеет общие характеристики как с дистанционно-векторными протоколами, так и с протоколами состояния канала. Протокол EIGRP вычисляет наилучший маршрут к каждой сети и подсети

и предоставляет альтернативные маршруты, которые могут быть использованы в том случае, если текущий маршрут становится недоступным. При осуществлении маршрутизации этот протокол также передает маску подсети для каждой позиции. По этой причине он легко поддерживает такие функции, как VLSM и суммирование маршрутов.

Протокол BGP представляет собой протокол внешней (по отношению к локальной сети) маршрутизации. Он предназначен для обработки маршрутов между автономными системами. Протокол BGP может быть использован между провайдерами ISP или между компаниями и Internet-провайдерами.

Сравнение протоколов IGP и EGP

Протокол внутреннего шлюза (interior gateway protocol — IGP) предназначен для использования в сети, управляемой или администрируемой отдельной организацией. Такой протокол служит для нахождения наилучшего маршрута в одной сети. Иными словами, метрика и характер ее использования являются наиболее важными элементами протокола IGP.

Протокол внешнего шлюза (exterior gateway protocol — EGP) предназначен для осуществления маршрутизации между сетями, управляемыми различными организациями. Как правило, протоколы класса используются для маршрутизации между провайдерами служб Internet (Internet Service Providers — ISP) или между отдельной компанией и Internet-провайдером. Например, компания может использовать протокол BGP, который является одним из протоколов EGP, для связи одного из своих маршрутизаторов с маршрутизатором провайдера ISP. Перед запуском EGP-протокола стека IP-протоколов необходимо указать следующие информационные компоненты:

- перечень соседних маршрутизаторов для обмена с ними информацией маршрутизации;
- список сетей, которые будут анонсированы как непосредственно достижимые;
- номер автономной системы локального маршрутизатора.

Протокол EGP должен изолировать автономные системы. Поскольку в каждой автономной системе используются свои собственные правила, в объединенной сети должен функционировать общий для всех систем протокол, который позволит осуществлять связь между ними. На рис. 17.25 приведен Пример автономной системы.

Каждая автономная система имеет шестнадцатибитовый идентификационный номер, который присваивается ей Американским реестром Internet-номеров (American Registry of Internet Numbers — ARIN) или местным представителем этой организации. Протоколы маршрутизации, такие, как IGRP и EIGRP, требуют, чтобы каждая система имела свой собственный уникальный номер.

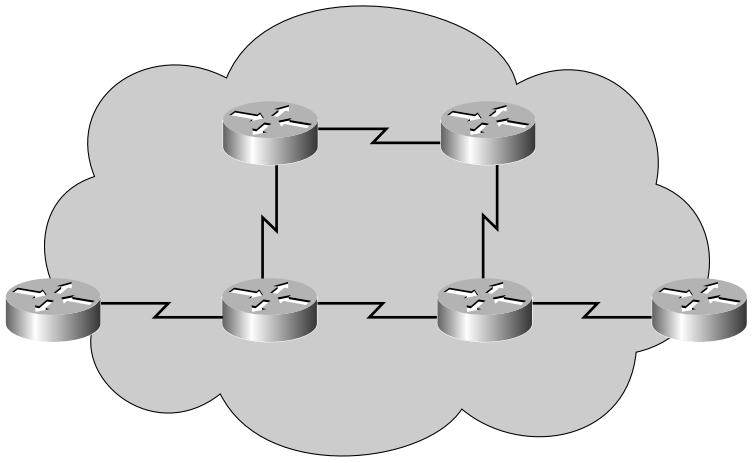


Рис. 17.25. Автономная система

Интерактивная презентация: сравнение протоколов IGP и EGP
В этой презентации проиллюстрированы отличия между двумя классами протоколов маршрутизации.

Резюме

В этой главе были рассмотрены следующие ключевые темы:

- маршрутизатор может переслать пакет только в том случае, когда он знает маршрут к сети-получателю;
- статические маршруты конфигурируются вручную сетевым администратором;
- стандартные маршруты представляют собой специальные статические маршруты, ведущие к стандартным шлюзам сети;
- статические и стандартные маршруты конфигурируются с помощью команды **`ip route`**;
- конфигурация статических и стандартных маршрутов может быть протестирована с помощью команд **`show ip route`**, **`ping`** и **`traceroute`**;
- существуют три типа протоколов маршрутизации:
  - дистанционно-векторные;
  - протоколы с учетом состояния каналов;
  - сбалансированные гибридные;
- под автономной системой (AS) понимается набор сетей, находящихся под общим административным управлением и использующих общую стратегию маршрутизации.

Обратите внимание на относящиеся к данной главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Ключевые термины

Автономная система (Autonomous System — AS) — это набор сетей, находящихся в одном административном домене.

Административное расстояние (Administrative Distance — AD) — это величина, характеризующая надежность источника информации о маршрутизации. Эта величина выражается числом в диапазоне от 0 до 255. Чем больше ее значение, тем менее доверительна полученная информация.

Алгоритм выбора кратчайшего маршрута (Shortest Path First — SPF algorithm) — это выполняемые над базой данных вычисления, результатом которых является построение дерева SPF.

Динамическая маршрутизация (dynamic routing) представляет собой разновидность маршрутизации, в которой автоматически учитываются изменения сетевой топологии и характера потоков данных. Также называется адаптивной маршрутизацией. Для осуществления такой маршрутизации между маршрутизаторами должен функционировать протокол маршрутизации.

Дистанционно-векторный протокол маршрутизации (distance vector routing protocol) относится к классу алгоритмов маршрутизации, последовательно анализирующих переходы на маршруте для построения связующего дерева кратчайшего пути. В дистанционно-векторных протоколах требуется, чтобы каждый маршрутизатор при каждом обновлении маршрутизации рассылал полностью свою таблицу маршрутизации, но только своим соседям. Алгоритмы дистанционно-векторной маршрутизации подвержены проблеме образования кольцевых маршрутов, однако в вычислительном отношении они проще алгоритмов маршрутизации по состоянию канала. Такие алгоритмы также называются алгоритмами маршрутизации Беллмана-Форда (Bellman-Ford).

Маршрутизация (routing) представляет собой процесс нахождения маршрута к узлу-получателю. В крупных сетях маршрутизация является весьма сложным процессом, поскольку на пути следования пакета к конечному узлу-получателю может находиться большое количество промежуточных узлов.

Маршрутизируемый протокол (routed protocol) — это протокол, данные которого маршрутизируются маршрутизатором. Маршрутизатор должен быть способен интерпретировать информацию о логической адресации объединенной сети, которая указана в заголовке пакета такого маршрутизируемого протокола. Примерами маршрутизируемых или сетевых протоколов могут служить протоколы AppleTalk, IPX и IP.

Метрика (metric) — это числовое значение, вырабатываемое каким-либо алгоритмом для каждого маршрута в сети. Обычно чем меньше метрика, тем предпочтительнее маршрут.

Протокол внешнего шлюза (Exterior Gateway Protocol — EGP) — это протокол маршрутизации, предназначенный для использования между сетями, управляемыми различными организациями.

Протокол внутреннего шлюза (Interior Gateway Protocol — IGP) — это протокол маршрутизации, предназначенный для использования в сети, управляемой или администрируемой одной организацией.

Протокол маршрутизации (routing protocol) — это протокол, осуществляющий реализацию какого-либо алгоритма маршрутизации. Примерами протоколов маршрутизации могут служить протоколы IGRP, OSPF и RIP.

Протокол маршрутизации по состоянию канала (link-state routing protocol) — это алгоритм маршрутизации, в котором каждый маршрутизатор выполняет широковещательную или многоадресатную рассылку информации о стоимости маршрута к каждому из своих соседей всех остальных узлов сети. Алгоритмы состояния канала создают связную картину всей сети, поэтому они практически не подвержены проблеме возникновения циклических маршрутов. Однако такое поведение достигается ценой большего объема и сложности вычислений и бо́льшего объема служебных сообщений, чем у дистанционно-векторных протоколов.

Распределение нагрузки (load sharing). Под распределением нагрузки понимается направление данных одного и того же сеанса связи по нескольким маршрутам в сети для повышения эффективности системы передачи информации.

Сбалансированный гибридный протокол маршрутизации (balanced hybrid routing protocol) — это протокол маршрутизации, использующий элементы дистанционно-векторного протокола и протокола маршрутизации по состоянию канала.

Сообщения о состоянии канала (link-state advertisement — LSA) представляют собой небольшие пакеты, содержащие информацию о маршрутизации, которые рассылаются между маршрутизаторами.

Статическая маршрутизация (static routing) — это процесс определения и конфигурирования маршрутов вручную.

Таблица маршрутизации (routing table) — это список известных устройству маршрутов и соответствующих им интерфейсов.

Топологическая база данных (topological database) — это совокупность информации, полученной из сообщений LSA.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Какое из выражений наилучшим образом описывает одну из функций третьего (сетевого) уровня эталонной модели OSI?
   а) Этот уровень отвечает за надежность связи между узлами сети.
   б) Этот уровень отвечает за физическую адресацию и анализ сетевой топологии.
   в) Этот уровень определяет наилучший маршрут для передачи данных по сети.
   г) Этот уровень управляет обменом данными между уровнями представления двух систем.
2. Какая функция позволяет маршрутизаторам оценивать доступные маршруты к пункту назначения и выбирать предпочтительный способ обработки пакетов?
   а) Функция взаимодействия.
   б) Функция определения маршрута.
   в) Протокол интерфейса SDLC.
   г) Функция обработки протокола Frame Relay.
3. Каким образом сетевой уровень направляет пакеты от отправителя получателю?
   а) Путем анализа таблицы IP-маршрутизации.
   б) Посредством использования ответов протокола ARP.
   в) Путем ссылки на имя сервера.
   г) Путем ссылки на мост.
4. Какие две части сетевого адреса используют маршрутизаторы для пересылки данных по сети?
   а) Адрес сети и адрес узла.
   б) Адрес сети и MAC-адрес.
   в) Адрес узла и MAC-адрес.
   г) MAC-адрес и маску подсети.
5. Какое из приведенных ниже утверждений наилучшим образом описывает сетевой (маршрутизируемый) протокол?
   а) Адрес этого протокола предоставляет достаточно информации для пересылок пакета между узлами.
   б) Этот протокол предоставляет информацию, необходимую для передачи пакетов данных следующему верхнему уровню.
   в) Этот протокол позволяет маршрутизаторам обмениваться информацией друг с другом для поддержки и обновления адресных таблиц.
   г) Он позволяет маршрутизаторам логически связывать между собой MAC-адрес и IP-адрес.

6. Какое из приведенных ниже утверждений наилучшим образом описывает протокол маршрутизации?

а) Этот протокол осуществляет маршрутизацию путем реализации некоторого алгоритма.

б) Этот протокол задает способ логического связывания между собой IP- и MAC-адресов.

в) Этот протокол определяет формат полей пакета данных и их использования.

г) Этот протокол позволяет пересылать пакеты от одного узла другому.

7. В чем состоит преимущество дистанционно-векторных алгоритмов?

а) Для них маловероятно бесконечное накапливание количества переходов (зацикливание в кольцевом маршруте).

б) Эти алгоритмы легко реализуются в крупных сетях.

в) Для дистанционно-векторных алгоритмов не характерно образование петель в маршрутизации.

г) Эти протоколы просты в вычислительном отношении.

8. Какое из приведенных ниже утверждений наилучшим образом описывает алгоритм маршрутизации по состоянию канала?

а) Этот алгоритм полностью воссоздает точную топологию всей объединенной сети.

б) Этот алгоритм требует большого объема вычислений.

в) Этот алгоритм определяет расстояние и направление ко всем каналам объединенной сети.

г) Этот алгоритм использует небольшое количество служебной информации и уменьшает общий объем передаваемых по сети данных.

9. Какова причина возникновения кольцевых маршрутов (петель) маршрутизации?

а) Медленная конвергенция после изменения топологии объединенной сети.

б) Искусственное создание расщепления горизонта.

в) Сегменты сети последовательно выходят из строя и тем самым каскадно выводят из строя и другие сегменты.

г) Сетевым администратором не были установлены и инициированы стандартные маршруты.

10. Какое из приведенных ниже утверждений наилучшим образом характеризует сбалансированную гибридную маршрутизацию?

а) Этот тип маршрутизации определяет наилучшие маршруты с использованием дистанционно-векторного алгоритма, однако изменения топологии вызывают обновления таблиц маршрутизации.

б) Этот тип маршрутизации использует дистанционно-векторную маршрутизацию для определения наилучших маршрутов в периоды большой загрузки сети.

в) Этот тип маршрутизации использует информацию о топологии сети для определения наилучших маршрутов, однако часто обновляет таблицы маршрутизации.

г) Этот тип маршрутизации использует информацию о топологии сети для определения наилучших маршрутов, однако использует вектор расстояния для обхода бездействующих сетевых каналов.

11. Как называется сеть, которая имеет только один маршрут к вышестоящему маршрутизатору?

а) Статическая.

б) Динамическая.

в) Модульная.

г) Тупиковая.

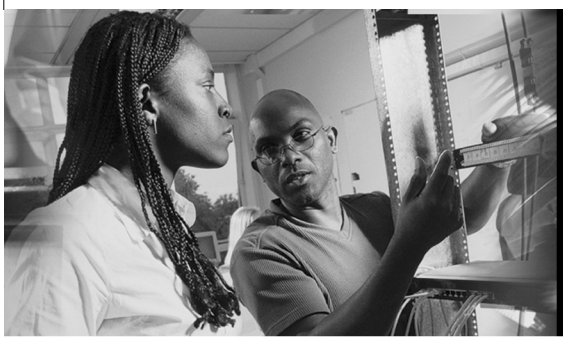
12. Какое из приведенных ниже определений наилучшим образом описывает стандартный маршрут?

а) Стандартным называется маршрут для срочной передачи данных, устанавливаемый сетевым администратором.

б) Стандартным называется маршрут, используемый в тех случаях, когда часть сети выходит из строя.

в) Стандартным называется маршрут, используемый в тех случаях, когда сеть-получатель не присутствует явным образом в таблице маршрутизации.

г) Стандартным называется заранее установленный кратчайший маршрут.



ГЛАВА 18

Дистанционно-векторные протоколы маршрутизации

В этой главе...

- описаны этапы первоначального конфигурирования маршрутизатора;
- даны характеристики протокола RIP;
- рассмотрен процесс конфигурирования протокола RIP, основные этапы и команды;
- описаны характеристики протокола IGRP;
- рассмотрен процесс конфигурирования протокола IGRP;
- описан механизм распределения нагрузки по нескольким маршрутам и тестирование его работы;
- рассказано, почему и как возникают кольцевые маршруты в дистанционно-векторных протоколах маршрутизации;
- описаны механизмы дистанционно-векторных протоколов маршрутизации, которые позволяют поддерживать информацию о маршрутах в актуальном состоянии;
- указано, для чего используется команда **`ip classless`**;
- рассмотрены методы и технологии поиска и устранения неисправностей в службах RIP-маршрутизации.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

таблица маршрутизации, с. 799,
смежное устройство, с. 799,
конвергенция, с. 800,
зацикливание, с. 801,
метрика, с. 802,
расщепление горизонта, с. 803,
мгновенные обновления, с. 805,
протокол маршрутной информации, с. 807,
обновления маршрутизации, с. 807,
протокол маршрутизации внутреннего шлюза, с. 826,
внутренний маршрут, с. 830,
системный маршрут, с. 830,
внешний маршрут, с. 830,
удаление маршрута, с. 804,
таймер обновления, с. 831,
таймер действительности маршрута, с. 831,
таймер удержания информации, с. 831,
таймер сброса маршрута, с. 831.

Теперь, когда в предыдущей главе мы рассмотрели основные положения, относящиеся к протоколам маршрутизации, можно рассмотреть процесс конфигурирования протоколов IP-маршрутизации. Как известно, в маршрутизаторе можно сконфигурировать один или более протоколов IP-маршрутизации. В этой главе мы рассмотрим первоначальное конфигурирование в маршрутизаторе протокола маршрутной информации (Routing Information Protocol — RIP) и протокола маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP); кроме того, будут рассмотрены методы мониторинга протоколов IP-маршрутизации.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Дополнительная информация: первоначальное конфигурирование маршрутизатора

После тестирования аппаратного обеспечения и загрузки образа программного обеспечения Cisco IOS маршрутизатор находит и выполняет директивы файла конфигурации. В этих директивах задаются установки атрибутов для конкретного маршрутизатора, функции протоколов и адреса интерфейсов. Следует помнить о том, что если маршрутизатор не может найти правильный файл стартовой конфигурации, то он входит в режим первоначального конфигурирования, называемый также режимом начальной установки или диалогом конфигурирования системы.

В таком режиме установки пользователю предлагается ответить на вопросы в режиме интерактивного диалога конфигурирования системы. В диалоге вводится базовая информация о конфигурации системы, которая позволяет маршрутизатору создать минимальный, но достаточный для работы конфигурационный файл. В режиме установки вводится следующая информация:

- используемые интерфейсы;
- глобальные параметры устройства;
- параметры интерфейсов;
- обзор сценария установки;
- указание маршрутизатору, следует ли в дальнейшем использовать эту конфигурацию.

После ввода указанной выше информации в режиме установки маршрутизатор использует ее в качестве текущей конфигурации. Маршрутизатор также сохраняет эту конфигурацию в энергонезависимой памяти (NonVolatile Random-Access Memory — NVRAM) в качестве новой стартовой конфигурации, после чего устройство будет готово к работе. Для внесения дополнительных изменений, касающихся протоколов и интерфейсов, следует войти в привилегированный режим и ввести команду **`configure`**.

Дистанционно-векторная маршрутизация

В этом разделе обсуждаются дистанционно-векторные протоколы, их достоинства и недостатки, а также способы решения проблем, которые могут возникнуть при использовании дистанционно-векторной маршрутизации. Алгоритмы, основанные на использовании вектора расстояния, периодически рассылают между маршрутизаторами копии их таблиц маршрутизации. В этих периодических обновлениях содержится информация об изменениях в топологии сети.

Анонсы маршрутов в дистанционно-векторных протоколах

В сетях, использующих дистанционно-векторную маршрутизацию, *таблица маршрутизации (routing table*) может обновляться как периодически, так и при изменении топологии соединений.

При обновлении таблиц маршрутизации от протокола маршрутизации требуется достаточная эффективность. По мере обнаружения новых сетей обновления маршрутизации систематически передаются от одного маршрутизатора другому. На рис. 18.1 показано, как дистанционно-векторные протоколы обрабатывают изменения топологии.

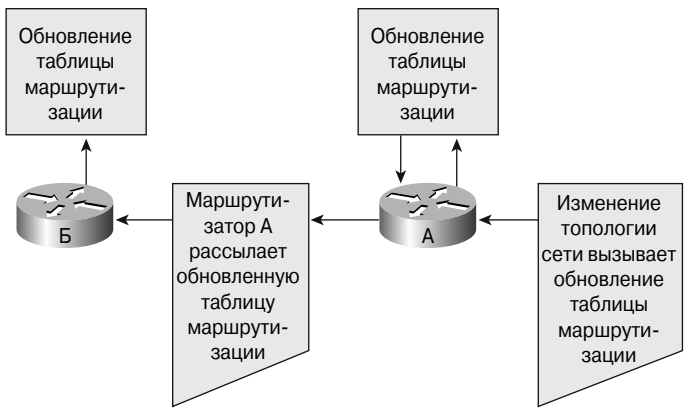


Рис. 18.1. Отслеживание изменений топологии сети в дистанционно-векторных алгоритмах маршрутизации

Дистанционно-векторные алгоритмы требуют, чтобы каждый маршрутизатор рассылал копию своей таблицы маршрутизации *смежным устройствам (adjacent neighbors)*. Смежное устройство — это маршрутизатор следующего перехода на подключенном к устройству канале.

В таблицах маршрутизации содержится информация об общей стоимости маршрута, определяемой используемой метрикой, и логический адрес анонсирующего сеть маршрутизатора для маршрута к каждой сети.

Как возникают маршрутные петли при дистанционно-векторной маршрутизации

Маршрутные петли могут возникать в том случае, если для протокола маршрутизации характерна медленная *конвергенция (convergence*) после изменений в сети или для топологии сети в маршрутизаторах возникло несоответствие между записями таблиц маршрутизации. На рис. 18.2 показаны петли маршрутизации.

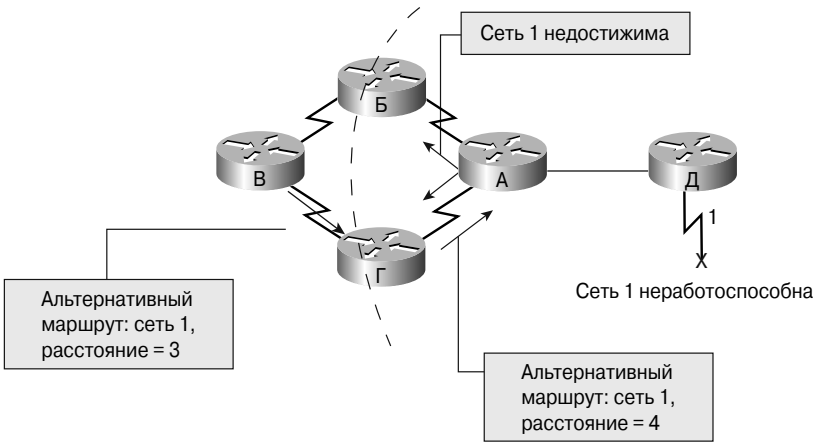


Рис. 18.2. Петли маршрутизации

Образование петель маршрутизации происходит описанным ниже образом (рис. 18.2).

1. Перед выходом из строя сети 1 все маршрутизаторы имеют согласованные и корректные таблицы маршрутизации. В этом случае говорят, что в сети произошла конвергенция. До конца этого примера предполагается, что для маршрутизатора В наилучший маршрут к сети 1 проходит через маршрутизатор Б, а расстояние от маршрутизатора В до сети 1 равно трем переходам.
2. Если сеть 1 выходит из строя, то маршрутизатор Д пересылает сообщение об обновлении маршрутов маршрутизатору А. После его получения маршрутизатор А прекращает отправку пакетов в сеть 1, однако маршрутизаторы Б, В и Г продолжают, поскольку они еще не информированы о сбое в сети 1. Когда маршрутизатор А отправляет свое сообщение об обновлении, маршрутизаторы Б и Г прекращают отправку пакетов в сеть 1. Однако в этот момент маршрутизатор В еще не получил сообщение об обновлении. Для него сеть 1 попрежнему считается достижимой через маршрутизатор Б.

3. Предположим, что маршрутизатор В отправляет периодическое обновление маршрутов маршрутизатору Г, указывая маршрут к сети 1 через маршрутизатор Б. Маршрутизатор Г изменяет свою таблицу маршрутизации для того, чтобы учесть такую некорректную информацию, и посылает эту информацию маршрутизатору А. Маршрутизатор А отправляет эту же информацию маршрутизаторам Б и Д, и т.д. Теперь любой пакет, предназначенный для сети 1, движется по кольцевому маршруту (петле) от маршрутизатора Б к маршрутизатору Б, далее к А и Г и вновь к маршрутизатору В.

Презентация: векторы расстояния
В этой презентации показано, как дистанционно-векторные протоколы маршрутизации рассылают анонсы маршрутов.

Максимальное количество транзитных переходов

Некорректные сведения о сети 1 продолжают циркулировать по кольцевому маршруту до тех пор, пока какой-либо другой процесс не прекратит рассылку. При таком состоянии сети, называемом *зацикливанием (count to infinity*), пакеты продолжают непрерывно двигаться по сети, несмотря на то что сеть-получатель вышла из строя. Пока маршрутизаторы увеличивают количество переходов потенциально до бесконечности, неверная информация допускает существование петли (рис. 18.3).

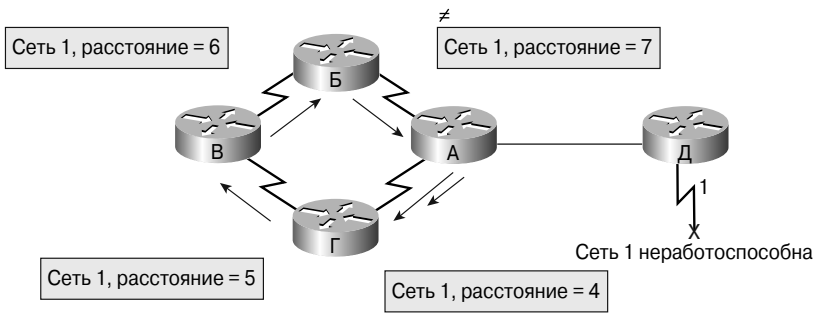


Рис. 18.3. Зацикливание

Если не будут предприняты какие-либо контрмеры для остановки этого процесса, то вектор расстояния или метрика, отражающая количество переходов, будут возрастать при каждом прохождении пакета через очередной маршрутизатор. Метрики маршрутов и их использование подробно описаны в главе 17, "Маршрутизация и протоколы маршрутизации". Таким образом, пакеты движутся по петле вследствие того, что в таблицах маршрутизации содержится ошибочная информация.

Дистанционно-векторные алгоритмы маршрутизации обладают способностью самокоррекции, однако для устранения петли в маршрутизации и проблемы зацикливания требуются специальные меры. Для того чтобы избежать проблемы зацикливания, в дистанционно-векторных протоколах бесконечность определяется

как конечное максимальное число. Такое число обычно называют *метрикой маршрутизации*. Метрика в самом простейшем случае может быть просто количеством переходов. Описанный подход проиллюстрирован на рис. 18.4.

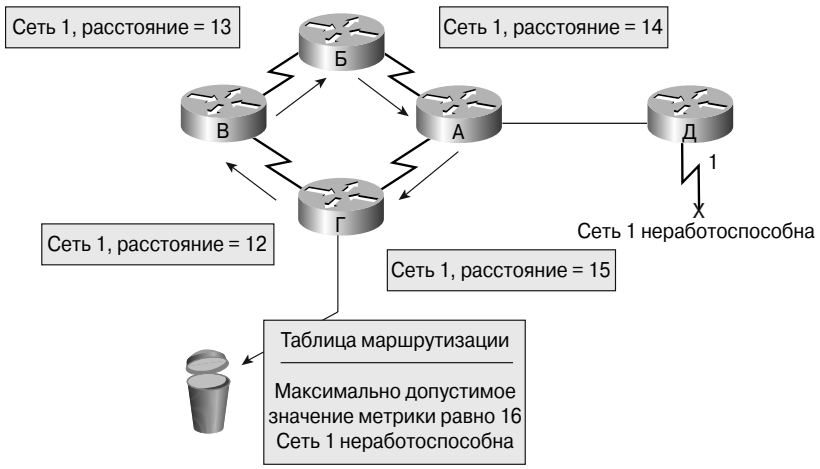


Рис. 18.4. Задание максимального значения метрики

При замене бесконечности некоторым максимальным числом протокол маршрутизации позволяет петле существовать лишь до того момента, пока метрика не превысит максимального допустимого значения. На рис. 18.4 показано, что значение метрики достигло шестнадцати; поскольку вектор расстояния превысил стандартный максимум в 15 транзитных переходов, пакет маршрутизатором отбрасывается. В любом случае, когда значение метрики превышает максимально допустимое, сеть 1 рассматривается как недостижимая.

Теперь попробуем разобраться в том, что происходит с другими IP-пакетами, которые не являются сообщениями протоколов маршрутизации в кольцевом маршруте (т.е. когда возникает петля). Вполне очевидно, что пакеты будут перебрасываться от одного маршрутизатора другому по кругу. В протоколе IP есть свой собственный механизм предотвращения бесконечной циркуляции пакетов по кругу — поле TTL (Time-To-Live — время существования пакета). Перед тем как IP-пакет будет передан узлом, в это поле согласно стандарту может быть установлено значение между 1 и 255. Такое значение не зависит от типа операционной системы и стандартно программными средствами заносится число между 32 и 128. Когда такой пакет поступает в маршрутизатор, устройство уменьшает значение в поле (зачастую его называют просто счетчиком TTL) на единицу. Когда значение TTL достигает нуля, маршрутизаторы обязаны отбросить такой IP-пакет и переслать отправителю соответствующее информационное ICMP-сообщение. Протокол ICMP и его различные сообщения подробно описаны в главе 19, “Сообщения об ошибках и управляющие сообщения протокола TCP/IP”. Такой механизм устраняет возможность бесконечной циркуляции IP-пакетов в сети и помогает решить проблему кольцевых маршрутов.

Предотвращение петель в маршрутизации с помощью расщепления горизонта

Другой возможный источник петли в маршрутизации возникает в том случае, когда маршрутизатору переслана неверная информация, противоречащая правильной, которую он первоначально распространил. Как показано на рис. 18.5, при этом происходит описанный ниже процесс, который и создает проблему петли маршрутизации.

1. Маршрутизатор А посылает маршрутизаторам Б и Г обновление, в котором указывается, что сеть 1 неработоспособна.
2. Однако маршрутизатор В передает маршрутизатору Б другое сообщение, в котором указывается, что сеть 1 доступна через маршрутизатор Г с расстоянием, равным четырем переходам. Такое действие не нарушает правил расщепления горизонта.
3. После получения последнего сообщения маршрутизатор Б неправильно заключает, что у маршрутизатора В по-прежнему имеется действительный маршрут к сети 1, хотя он гораздо менее предпочтителен для метрики. Маршрутизатор Б отсылает сообщения об обновлении маршрутизатору А, извещая его о новом маршруте к сети 1.
4. Получив его, устройство А делает вывод о том, что оно может переслать информацию в сеть 1 через маршрутизатор Б. В свою очередь маршрутизатор Б заключает, что он может посылать информацию в сеть 1 через маршрутизатор В, а маршрутизатор В решает, что он может послать информацию в сеть 1 через маршрутизатор Г. В такой ситуации любой пакет будет двигаться по кольцевому маршруту (петле) между этими маршрутизаторами.
5. Расщепление горизонта пытается предотвратить такую ситуацию. Согласно этому методу, при поступлении сообщения об обновлении маршрутов для сети 1 от маршрутизатора А маршрутизаторы Б и Г не могут посылать информацию о сети 1 в обратном направлении, т.е. маршрутизатору А, как показано на рис. 18.5. Таким образом, *расщепление горизонта (split horizon*) не позволяет распространять неверную информацию маршрутизации и уменьшает объем передаваемых служебных сообщений.

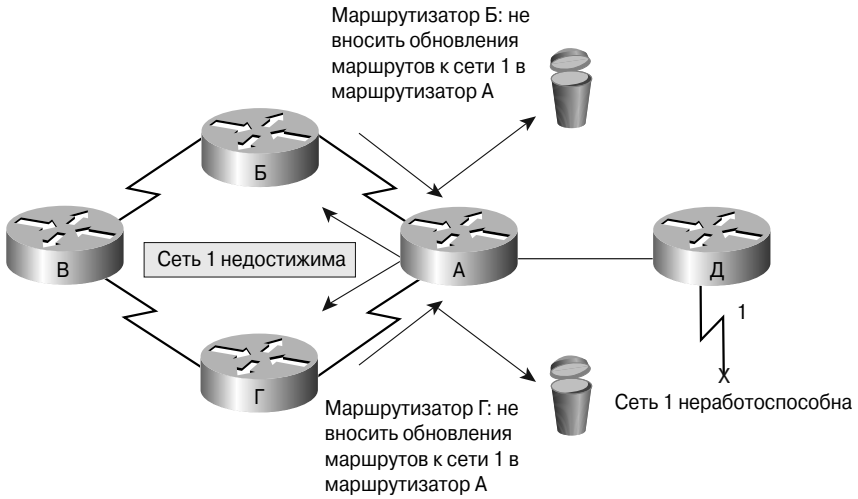


Рис. 18.5. Расщепление горизонта

Удаление маршрута в обратном направлении

Удаление маршрута в обратном направлении (route poisoning) используется различными дистанционно-векторными протоколами для предотвращения больших петель маршрутизации и предоставления явной информации о маршрутах в тех случаях, когда подсеть или сеть недостижимы. Такое удаление маршрута обычно осуществляется путем установки количества переходов на единицу большим, чем максимальное значение. Этот механизм является альтернативным способом предотвращения петель маршрутизации. Такой подход может быть сформулирован так, как указано ниже.

После получения информации о маршруте через какой-либо интерфейс следует объявить его недостижимым через этот же интерфейс. Лучше явно уведомить маршрутизатор о том, что маршрут следует игнорировать, чем пустить все на самотек.

Предположим, на всех маршрутизаторах на рис. 18.6 включен механизм обратного удаления машрутов. После получения информации маршрутизатором One о сети A от маршрутизатора Two устройство One объявляет сеть A недостижимой через свои каналы к маршрутизаторам Two и Three. Если маршрутизатор Three имеет какой-либо маршрут к сети A через маршрутизатор One, он удаляет этот маршрут, поскольку получил сообщение о недостижимости этой сети. Например, протокол EIGRP использует оба правила для предотвращения петель маршрутизации.

Протокол EIGRP использует расщепление горизонта и объявляет маршрут недостижимым:

- когда два маршрутизатора находятся в режиме загрузки (впервые обмениваются топологическими таблицами);
- при рассылке анонсов изменений в топологической таблице;
- при отправке запроса.

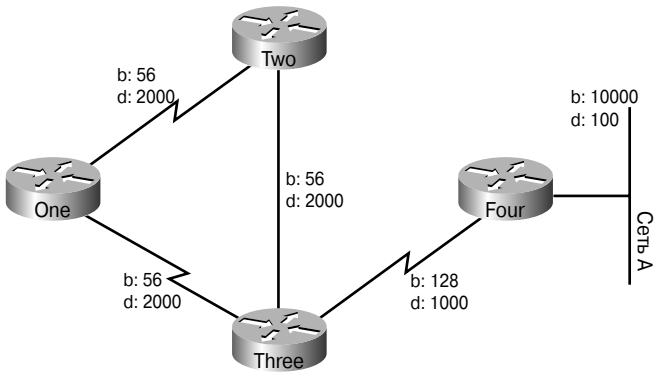


Рис. 18.6. Удаление маршрута в обратном направлении

Использование описываемого механизма вместе с мгновенной рассылкой анонсов (event triggered update) ускоряет конвергенцию сети, поскольку соседним маршрутизаторам не требуется в течение 30 секунд ожидать обновлений до удаления маршрута. Использование механизма удаления маршрута в обратном направлении приводит к анонсированию протоколом маршрутизации бесконечной метрики для неработоспособных маршрутов. Этот механизм не нарушает правила расщепления горизонта. Расщепление горизонта совместно с механизмом удаления маршрута, по существу, является методом исключения некорректных маршрутов. Одновременно оба механизма вводятся на каналах, через которые в обычном случае правило расщепления горизонта позволяет проходить нежелательной информации о маршрутах. В любом случае результатом является тот факт, что неработоспособные маршруты анонсируются с бесконечной метрикой.

Предотвращение петель маршрутизации посредством мгновенных обновлений

Новые копии таблиц маршрутизации обычно регулярно рассылаются соседним маршрутизаторам. Протокол рассылает сообщения обновлений каждые 30 секунд. Однако *мгновенные обновления (triggered update*) рассылаются немедленно в ответ на какое-либо изменение в таблице маршрутизации. Маршрутизатор, который обнаружил изменение в топологии, немедленно рассылает сообщение-обновление смежным маршрутизаторам. Такие маршрутизаторы в свою очередь также генерируют мгновенные обновления, оповещая о переменах своих соседей. При выходе какого-либо маршрута из строя сообщение отправляется, не дожидаясь истечения времени таймера обновления. Использование мгновенных обновлений в сочетании с механизмами удаления маршрутов гарантирует, что все маршрутизаторы будут оповещены об отказавших маршрутах до истечения времени любого таймера хранения информации.

Мгновенное обновление, таким образом, представляет собой анонс, который рассылается до истечения времени таймера обновления. Маршрутизатор также немедленно отправляет сообщение обновления на все свои остальные интерфейсы, не дожидаясь истечения времени таймера. Такой принцип работы приводит к рассылке обновленной информации о состоянии маршрута и сбрасывает таймеры на соседних маршрутизаторах. Эта волна обновлений передается по всей сети. Принцип описанной рассылки проиллюстрирован на рис. 18.7.

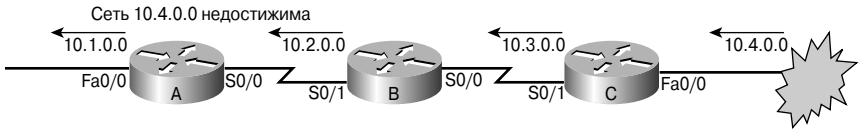


Рис. 18.7. Мгновенные обновления

Маршрутизатор B генерирует мгновенное обновление, извещая о том, что сеть 10.4.0.0 недостижима. После получения этой информации маршрутизатор B извещает остальные маршрутизаторы о выходе из строя сети 10.4.0.0 через интерфейс S0/1. В свою очередь, маршрутизатор A отправляет это сообщение об обновлении через интерфейс Fa0/0.

Предотвращение петель маршрутизации с помощью таймеров удержания информации

Зацикливания можно избежать путем использования таймеров удержания информации (holddown timer). Правильная последовательность действий при этом описана ниже.

1. Когда маршрутизатор получает от соседнего устройства обновление маршрутов, указывающее, что ранее доступная сеть стала неработающей, он помечает этот маршрут как недоступный и запускает таймер.
2. Если до истечения времени таймера от того же соседнего устройства поступает новое сообщение-обновление, в котором указывается, что вышедшая из строя сеть вновь доступна, то маршрутизатор помечает сеть как доступную и отключает таймер удержания информации.
3. Если же новое обновление поступает от другого соседнего маршрутизатора, и указанная в нем метрика лучше первоначально зарегистрированной для данной сети, то маршрутизатор помечает сеть как доступную и отключает таймер.

Если до истечения времени таймера удержания информации от иного соседнего маршрутизатора поступает новое обновление и указанная в нем метрика для данной сети хуже первоначально зарегистрированной, сообщение обновления игнорируется. В такой ситуации игнорирование сообщений об обновлениях предоставляет больше времени для распространения по всей сети информации об изменениях в топологии сети, как показано на рис. 18.8.

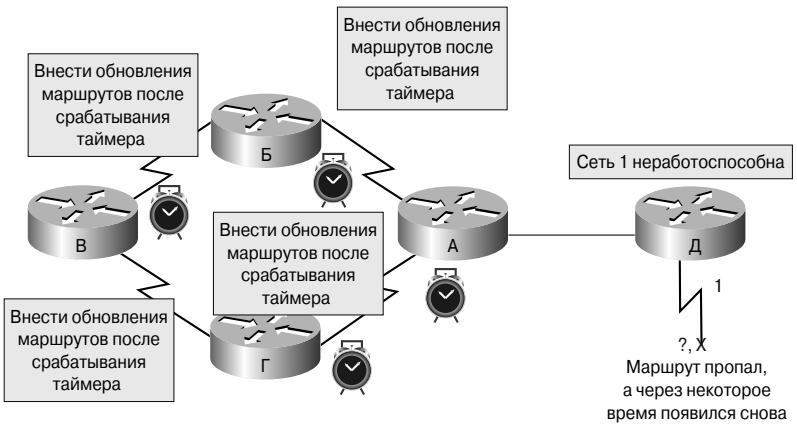


Рис. 18.8. Таймеры удержания информации

Презентация: таймеры удержания информации
В этой презентации проиллюстрирован принцип работы таймеров удержания информации при рассылке обновлений маршрутов.

Протокол RIP

Протокол маршрутной информации (Routing Information Protocol — RIP) был первоначально определен в документе RFC 1058 в 1988 году. Наиболее существенны его следующие характеристики:

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

Следует обратить внимание на то, что на рис. 18.9 маршрут с полосой пропускания 19,2 Кбит/с (через верхние маршрутизаторы) включает в себя два перехода. Нижний альтернативный маршрут (использующий линию T1) включает четыре перехода. Поскольку выбор маршрута в протоколе RIP основывается исключительно на количестве переходов, в данном случае выбирается маршрут с пропускной способностью 19,2 Кбит/с вместо гораздо более быстрых линий T1.

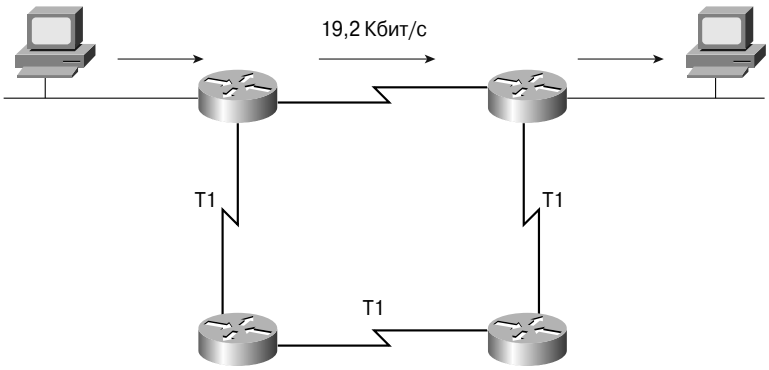


Рис. 18.9. Протокол RIP использует в качестве метрики количество переходов

Процесс маршрутизации протокола RIP

Протокол RIP с течением времени претерпел значительную эволюцию: от основанного на классах протокола маршрутизации RIP первой версии (RIP-1) к бесклассовому протоколу RIP второй версии (RIP-2). Усовершенствования протокола RIP-2 включают в себя:

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

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

Конфигурирование протокола RIP

Команда **`router rip`** включает RIP в качестве протокола маршрутизации. После этого выполняется команда **`network`** для указания протоколу сетей, которые непосредственно подсоединены к маршрутизатору и должны быть им анонсированы. Процесс маршрутизации после выполнения указанных двух действий логически

связывает эти интерфейсы с сетевыми адресами и начинает использовать протокол RIP на интерфейсах маршрутизатора.

Как и большинство других протоколов, RIP рассылает регулярные сообщения об обновлении маршрутов, а реализация корпорации Cisco данного протокола использует мгновенные анонсы (их называют как event-triggered, так и event-driven) в тех случаях, когда изменяется топология сети. Изменения в топологии сети запускают рассылку обновлений также и в протоколе IGRP, вне зависимости от значения таймера удержания информации. Без такого механизма мгновенной рассылки обновлений как протокол RIP, так и IGRP не будут работать с максимальной эффективностью, поскольку мгновенные обновления значительно ускоряют конвергенцию таблиц маршрутизации и, следовательно, снижают риск образования петель маршрутизации.

При получении маршрутизатором сообщения об обновлении, содержащего изменения, он обновляет свою таблицу маршрутизации для отображения в ней нового маршрута. Значение метрики при этом увеличивается на единицу, а интерфейс оптравителя обновления указывается в качестве следующего транзитного перехода на маршруте. Маршрутизаторы RIP записывают только наилучший маршрут к пункту назначения, однако могут поддерживать и несколько маршрутов, если они имеют одинаковое значение метрики.

После обновления таблицы маршрутизации вследствие изменения топологии сети маршрутизатор сразу начинает рассылать сообщения об обновлении маршрутов, для того чтобы проинформировать другие маршрутизаторы о произошедших изменениях. Обновления рассылаются независимо от обычных регулярных сообщений RIP-маршрутизаторов. Если обновление пересылается через интерфейс другой суперсети с несовпадающим суммарным адресом, то протокол RIP анонсирует только сети, основанные на классах или сети главного класса. Иными словами, информация о подсетях не суммируется к одному агрегированному адресу и передается в виде отдельных записей, если анонс пересылается через интерфейс, адрес которого принадлежит той же суперсети. Классовые протоколы маршрутизации, например, RIP версии 1, в анонсах маршрутизации не пересылают информацию о масках подсетей.

Для включения на маршрутизаторе протокола RIP используются команды режима глобального конфигурирования, описанные в табл. 18.1.

Таблица 18.1. Команды для включения протокола RIP

Команда	Назначение
`Router(config)#router rip`	Включает процесс RIP-маршрутизации, после чего устройство переходит в режим конфигурирования маршрутизации
`Router(config-router)#network` *network-number*	Связывает сеть с процессом RIP-маршрутизации

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

```
BHM(config)#router rip
! Включение протокола маршрутизации RIP
BHM(config-router)#network 1.0.0.0
! Указание непосредственно подключенной к устройству сети
BHM(config-router)#network 2.0.0.0
! Указание непосредственно подключенной к устройству сети
```

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

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

Практическое задание 18.2.2. Конфигурирование протокола RIP в маршрутизаторе
В этом практическом задании необходимо реализовать схему IP-адресации с использованием блока адресов сетей класса C и сконфигурировать процесс маршрутизации протокола RIP в маршрутизаторах.

Использование команды ip classless

Иногда маршрутизатор получает пакеты, предназначенные неизвестной подсети некоторой сети, которая входит в непосредственно подсоединенные сети устройства. Для пересылки этих пакетов по наилучшему маршруту используется команда глобального конфигурирования **ip classless**. Такая команда стандартно включена в конфигурации всех операционных систем Cisco IOS, начиная с версии 11.3 и выше. Для отключения этой функции используется форма данной команды с ключевым словом **no**.

В случае, когда функция отключена и пакет пересылается в подсеть сети, к которой нет стандартного маршрута, пакет маршрутизатором отбрасывается. Такой принцип работы проиллюстрирован на рис. 18.10: если маршрутизатор пересылает пакет в сеть 128.20.4.1 и стандартный маршрут отсутствует, то пакет отбрасывается.

Команда **ip classless** воздействует только на операцию пересылки пакета, выполняемую операционной системой IOS. Она не влияет на построение таблицы маршрутизации. Описанный характер воздействия команды выражает сущность бесклассовой маршрутизации. Если известна часть крупной сети, а подсеть получателя, для которой предназначен пакет, неизвестна, то пакет отбрасывается.

В описываемом правиле больше всего сбивает с толку то, что маршрутизатор использует стандартный маршрут только в том случае, когда в таблице маршрутизации отсутствует пункт назначения главной сети. Стандартно маршрутизатор предполагает, что все подсети непосредственно подсоединенной сети в таблице маршрутизации

присутствуют. Если маршрутизатор получает пакет с неизвестным адресом получателя, находящегося в неизвестной подсети подсоединенной сети, то он предполагает, что такая подсеть не существует. Поэтому устройство отбрасывает пакет даже в том случае, если существует стандартный маршрут. Конфигурирование в маршрутизаторе команды **`ip classless`** решает эту проблему за счет указания маршрутизатору игнорировать основанные на классах границы сетей в его таблице маршрутизации и просто выбирать стандартный маршрут, как показано на рис. 18.11.

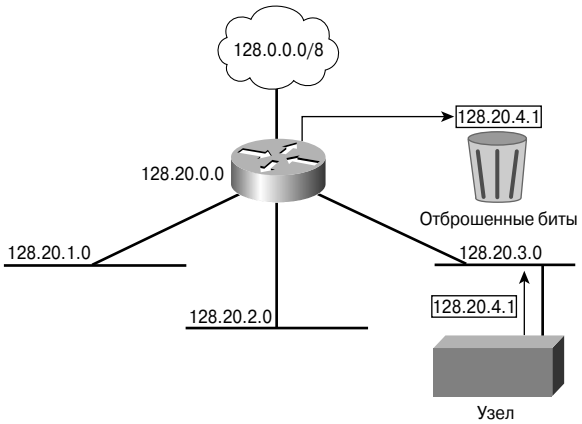


Рис. 18.10. Результат использования команды ***`no ip classless`***

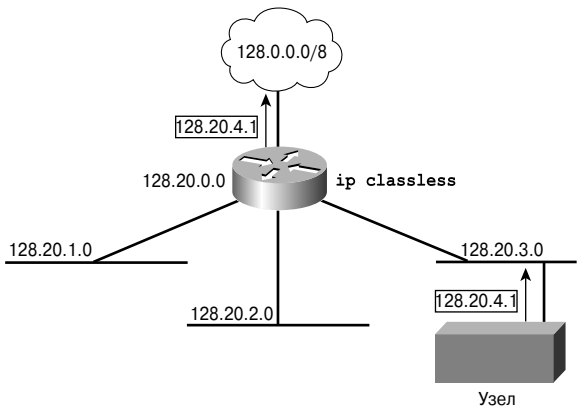


Рис. 18.11. Бесклассовая IP-маршрутизация

Общие вопросы конфигурирования протокола RIP

При получении информации о сети RIP-маршрутизаторы полагаются на соседние маршрутизаторы. Протокол RIP использует дистанционно-векторный алгоритм, а всем протоколам дистанционно-векторной маршрутизации свойственны проблемы, приводящие к медленной конвергенции.

Некоторые проблемы связаны с возникновением петель маршрутизации, приводящих к зацикливанию. Обе проблемы приводят к несогласованности информации о маршрутах, вызванной распространением по сети сообщений об устаревших маршрутах.

Для предотвращения появления петель маршрутизации и зацикливания пакетов протокол RIP использует следующие методы:

- расщепление горизонта;
- удаление маршрутов в обратном направлении;
- таймеры удержания информации;
- мгновенные сообщения.

Некоторые из перечисленных методов требуют дополнительного конфигурирования, другие — не всегда или вообще не требуют. Максимальное число переходов, допускаемое протоколом RIP, равно пятнадцати. Любая сеть-получатель, находящаяся на расстоянии, большем, чем 15 переходов, помечается как недостижимая. Установка максимально допустимого количества переходов в протоколе RIP значительно ограничивает возможности его использования в крупных объединенных сетях, однако предотвращает проблему зацикливания пакетов и кольцевых маршрутов, возникающую при появлении петель маршрутизации.

Использование метода расщепления горизонта основано на том, что, как правило, нет необходимости в отправке информации о маршруте в обратном направлении, т.е. в том направлении, по которому этот маршрут поступил. В некоторых конфигурациях сетей может оказаться необходимым отключение механизма расщепления горизонта: отключение производится для каждого отдельного интерфейса.

Для отключения механизма используется команда **`split horizon`** совместно с ключевым словом **`no`**:

```
Router(config-if)# no ip split-horizon
```

Еще одним механизмом, который может потребовать внесения некоторых изменений, является использование таймера удержания информации. Такой таймер позволяет предотвратить зацикливание пакетов, однако увеличивает время конвергенции. Стандартно время удержания в протоколе RIP составляет 180 секунд. В течение этого времени не разрешается обновление внутренних маршрутов, однако при этом действительные альтернативные маршруты также не будут устанавливаться. Для ускорения конвергенции время таймера удержания может быть уменьшено, однако такое уменьшение требует осторожности. Идеальным решением является установка этого периода удержания чуть бо́льшим максимального времени обновления маршрутов в данной объединенной сети. На рис. 18.12 показана образовавшаяся из четырех маршрутизаторов петля. Если время обновления для каждого маршрутизатора составляет 30 секунд, то общее время обхода петли равно 120-ти секундам. Соответственно, для таймера удержания информации следует сконфигурировать период, несколько бо́льший 120-ти секунд.

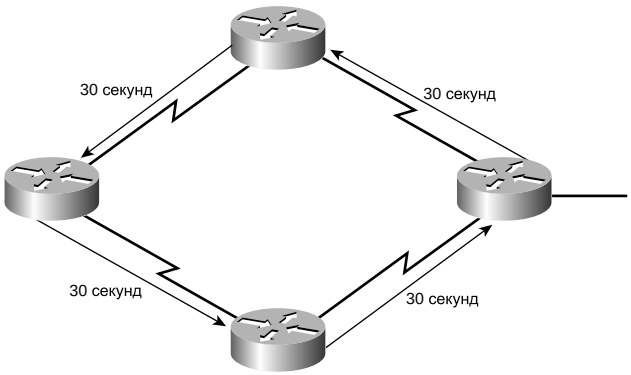


Рис. 18.12. Определение периода таймера удержания

Для изменения периода таймера удержания информации используется команда **timers basic** *update invalid holddown flush* [*sleep-time*], в которой все значения указываются в секундах. Например, таймерам можно указать следующие значения:

```
Router (config-router)# timers basic 30 90 100 300
```

Дополнительным параметром, влияющим на скорость конвергенции и допускающим конфигурирование, является интервал рассылки сообщений обновления маршрутов. Стандартно обновления IP-протокола RIP рассылаются программным обеспечением Cisco IOS каждые 30 секунд. Это время может быть увеличено для экономии полосы пропускания или уменьшено для сокращения времени конвергенции.

Как уже говорилось, еще одной проблемой, возникающей при использовании протоколов маршрутизации, являются нежелательные анонсы обновлений маршрутизации с некоторых интерфейсов. При использовании команды **network** протокол RIP рассылает информацию о маршруте к указанной в ней сети со всех интерфейсов в диапазоне адресов этой сети. Для управления набором интерфейсов, которые обмениваются сообщениями обновлений, сетевой администратор может отключить для отдельных интерфейсов отправку таких сообщений с помощью команды **passive-interface**. Протокол маршрутизации RIP в таком случае будет принимать обновления маршрутов через интерфейс, но не будет их рассылать.

Известно, что протокол RIP использует механизм широковещательной рассылки, тем не менее, сетевому администратору может потребоваться конфигурирование протокола RIP для обмена информацией маршрутизации по нешироковещательной сети, такой, например, как сеть протокола Frame Relay. В сетях такого типа протоколу RIP необходимо предоставить информацию о соседних RIP-маршрутизаторах. Для указания соседнего маршрутизатора, с которым требуется обмениваться информацией маршрутизации, используется следующая команда:

```
GAD(config-router)neighbor ip address
```

Стандартно программное обеспечение получает пакеты протоколов RIP-1 и RIP-2, однако рассылает только пакеты протокола RIP-1. Сетевой администратор может сконфигурировать маршрутизатор на получение и отправку только пакетов протокола RIP первой версии или рассылку только пакетов протокола RIP версии 2. Для того чтобы сконфигурировать маршрутизатор на отправку и получение пакетов только одной версии протокола RIP, следует использовать команды режима конфигурирования маршрутизатора, описанные в табл. 18.2.

Таблица 18.2. Указание используемой версии протокола RIP

Команда	Назначение
`(config-router)#version {1 | 2}`	Указывает программному обеспечению на необходимость получения и отправки только пакетов версии RIP-1 или версии RIP-2
`(config-if)#ip rip send version 1`	Конфигурирует интерфейс для отправки только пакетов версии RIP-1
`(config-if)#ip rip send version 2`	Конфигурирует интерфейс для отправки только пакетов версии RIP-2
`(config-if)#ip rip send version 1 2`	Конфигурирует интерфейс для отправки пакетов версии RIP-1 или версии RIP-2

Для управления процессом обработки полученных на некотором интерфейсе пакетов используются команды, описанные в табл. 18.3.

Таблица 18.3. Управление обработкой пакетов

Команда	Назначение
`(config-if)#ip rip receive version 1`	Конфигурирует интерфейс для получения только пакетов версии RIP-1
`(config-if)#ip rip receive version 2`	Конфигурирует интерфейс для получения только пакетов версии RIP-2
`(config-if)#ip rip receive version 1 2`	Конфигурирует интерфейс для получения пакетов версии RIP-1 или версии RIP-2

Тестирование конфигурации протокола RIP

Для проверки правильности созданной конфигурации протокола RIP могут быть использованы несколько команд. Двумя наиболее часто используемыми командами являются **`show ip route`** и **`show ip protocols`**.

При вводе команды **`show ip protocols`** отображается информация обо всех протоколах IP-маршрутизации, сконфигурированных на маршрутизаторе (пример 18.1). Такие сведения могут быть использованы для тестирования большей части, если даже не всей RIP-конфигурации. Ниже перечислены основные тестируемые параметры конфигурации.

- Включен ли на требуемых интерфейсах протокол RIP?
- Соответствующие ли интерфейсы принимают и пересылают обновления маршрутизации протокола RIP?
- Правильная ли версия обновлений маршрутизации протокола RIP используется?
- Анонсирует ли маршрутизатор требуемые сети?

Пример 18.1. Выводимая командой `show ip protocols` информация

```
GAD# show ip protocols
Routing Protocol is "rip“
! В строке выше указано, что протокол RIP запущен
Sending updates every 30 seconds, next due in 5 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Redistributing: rip
Default version control: send version 1, receive any version
! В строке выше указана версия протокола RIP
 Interface Send Recv Triggered RIP Key-chain
! В строках ниже указаны интерфейсы протокола RIP
FastEthernet0/0 1 1 2
Serial0/0 1 1 2
Routing for Networks:
192.168.1.0
192.168.2.0
! В строках выше указаны анонсируемые сети
Routing Information Sources:
Gateway Distance Last Update
192.168.2.2 120 00:00:11
Distance: (default is 120)
```

Команда **`show ip route`** может быть использована для проверки того, что маршруты, полученные по протоколу RIP, заносятся в таблицу маршрутизации, как показано в примере 18.2. Рекомендуется просмотреть вывод по этой команде и найти маршруты протокола RIP, которые обозначены символом “R”. Следует помнить о том, что для конвергенции требуется некоторое время, поэтому маршруты появляются в таблице маршрутизации по истечении некоторого промежутка времени.

Пример 18.2. Выводимая командой `show ip route` информация

```
GAD# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
```

```
P - periodic downloaded static route
Gateway of last resort is not set
C 192.168.1.0/24 is directly connected, FastEthernet0/0
C 192.168.2.0/24 is directly connected, Serial0/0
R 192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:07, Serial0/0
! В последней строке указан маршрут протокола RIP
```

Последняя строка вывода, начинающаяся символом *R*, указывает, что информация о сети 192.168.3.0 была получена посредством протокола RIP. В эту сеть можно попасть через интерфейс 192.168.2.2 смежного маршрутизатора (маршрутизатора следующего перехода), который подсоединен как удаленный узел к последовательному порту **Serial 0/0** данного маршрутизатора.

Для проверки правильности конфигурирования протокола RIP могут быть также использованы команды:

- **show interface** *interface*;
- **show ip interface** *interface*;
- **show running-config**.

Перечисленные выше команды полезны в тех случаях, когда необходимо получить информацию о конкретном интерфейсе. При выполнении команды **show interface** отображается вся информация об отдельном интерфейсе, в частности, активен ли он, а также какой тип протокола, IP-адрес или тип инкапсуляции могут быть сконфигурированы на нем. В целом перечисленные выше команды предоставляют администратору всю доступную конфигурационную информацию о конкретном интерфейсе. Команда **show running-config** используется для отображения текущей конфигурации маршрутизатора и всех его интерфейсов. Отметим, что маршрутизаторы корпорации Cisco используют каждый протокол отдельно от других. По этой причине ключевое слово **ip** в команде **show ip interface** необходимо для того, чтобы была выведена информация о протоколе IP, касающаяся данного интерфейса.

Устранение ошибок анонсов протокола RIP

Большинство ошибок в RIP-конфигурации связано с выполнением некорректных команд **network**, с разрывами в сетях или с расщеплением горизонта. Первичным инструментом для обнаружения ошибок, связанных с обновлениями протокола RIP, является команда **debug ip rip**.

При выполнении команды **debug ip rip** отображаются обновления маршрутизации протокола RIP по мере их отправки или получения. На рис. 18.13 и в примере 18.3 проиллюстрирован маршрутизатор, выполняющий команду **debug ip rip** и получающий обновления маршрутизации.

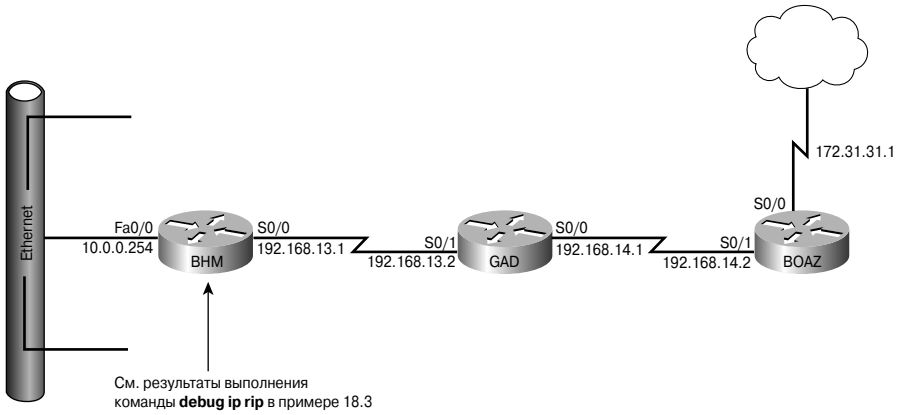


Рис. 18.13. Отладка сети протокола RIP

Пример 18.3. Выводимая командой `debug ip rip` информация

```
BHM# debug ip rip
RIP event debugging is on
BHM#
00:45:36 RIP:received v1 update from 192.168.13.2 on Serial0/0
00:45:36 192.168.14.0 in 1 hop
00:45:36 172.31.0.0 in 2 hops
00:45:36 172.29.0.0 in 15 hops
00:45:36 RIP sending v1 update to 255.255.255.255 via Serial0/0
  (192.168.13.1)
00:45:36 network 10.0.0.0, metric 1
00:45:36 RIP sending v1 update to 255.255.255.255 via
  FastEthernet0/0 (10.0.0.254)
00:45:36 network 192.168.13.0 metric 1
00:45:33 network 192.168.14.0 metric 2
00:45:33 network 172.31.0.0 metric 3
00:45:36 network 172.29.0.0 metric 16
```

Маршрутизатор пересылает информацию об обновлении маршрутизации с двух RIP-интерфейсов. Приведенный выше пример показывает, что маршрутизатор использует версию RIP-1 и широковещательно рассылает сообщения об обновлении (адрес 255.255.255.255). Номер сети в скобках представляет собой адрес сети-отправителя, инкапсулированный в IP-заголовок RIP-обновления.

В приведенном выше примере работы команды **`debug ip rip`** можно заметить некоторые возникшие проблемы. В частности, имеются проблемы, связанные с отсутствием непрерывности в подсетях или дублирующиеся сети. О наличии этих проблем говорит то, что протокол маршрутизации анонсирует сетевой маршрут, метрика которого меньше метрики, характерной для этой сети.

В примере 18.4 приведена соответствующая такому случаю информация команды **`debug ip rip`**.

Пример 18.4. Выводимая командой `debug ip rip` информация о некорректной маршрутизации

```
BMH# debug ip rip
RIP event debugging is on
BHM#
7w2d: RIP: received v1 update from 192.168.13.2 on serial0/0
7w2d:         192.168.14.0 1 hop
7w2d:         172.31.0.0 in 2 hops
7w2d: RIP: sending v1 update to 255.255.255.255 via Serial0/0
(192.168.13.1)
7w2d:         network 172.31.0.0 metric 1
7w2d: RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0
(10.0.0.254)
7w2d:         192.168.13.0 metric 1
7w2d:         192.168.14.0 metric 2
```

Для обнаружения и устранения ошибок в протоколе RIP могут быть дополнительно использованы приведенные ниже команды.

- Команда **`show ip rip database`** используется для отображения содержимого частной базы данных в том случае, когда включены мгновенные расширения протокола RIP.
- Команда **`show ip protocols {summary}`** служит для отображения информации, относящейся к IP-протоколу маршрутизации.
- Команда **`show ip route`** используется для отображения таблицы IP-маршрутизации на маршрутизаторе.
- Команда **`debug ip rip {events}`** служит для отображения в интерфейсе командной строки информации протокола RIP, которая обрабатывается маршрутизатором.
- Команда **`show ip interface brief`** используется для отображения общей IP-информации и состояния в привилегированном EXEC-режиме. Параметр **`brief`** является необязательным; при его включении отображается краткая информация о состоянии IP-протокола и конфигурации.

Все перечисленные выше команды предоставляют информацию, которая может оказаться полезной при проверке конфигурации маршрутизатора.

Практическое задание 18.2.6. Поиск и устранение неисправностей в работе протокола RIP

В этой лабораторной работе требуется создать схему IP-адресации, используя адреса класса B, и сконфигурировать в маршрутизаторах протокол RIP. После завершения первой части задания следует понаблюдать за процессом маршрутизации с помощью команды **`debug ip rip`** и просмотреть маршруты с помощью команды **`show ip route`**.

Отключение рассылки анонсов маршрутизации через интерфейс

С помощью команды **passive-interface** можно предотвратить рассылку обновлений маршрутизации через конкретный интерфейс маршрутизатора. Отключение пересылки через интерфейс сообщений об обновлении маршрутизации не позволяет другим системам данной сети динамически получать информацию о маршрутах. Как показано на рис. 18.14, в маршрутизаторе Д используется команда **passive-interface** для предотвращения рассылки сообщений об обновлении маршрутизации.

```
RouterE (config-router)# passive-interface Fa0/0
```

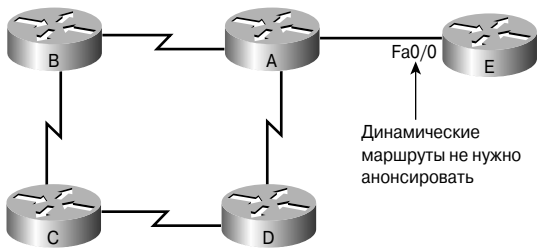


Рис. 18.14. Конфигурирование пассивного режима работы интерфейса

Для протоколов RIP и IGRP команда **passive-interface** прекращает рассылку маршрутизатором сообщений об обновлениях соседним маршрутизаторам, однако он не прекращает получать и использовать обновления от соседних устройств. Зачастую интерфейс, в котором выключена рассылка, называют пассивным, поскольку интерфейс не участвует активно в процессе маршрутизации, но, тем не менее, продолжает пассивно принимать сообщения от смежных маршрутизаторов.

Практическое задание 18.2.7. Отключение анонсов маршрутизации для заданного интерфейса

В этой лабораторной работе необходимо отключить анонсы маршрутизации для определенного интерфейса, чтобы ограничить число анонсируемых маршрутов, и проследить, какие будут получены результаты. Для выполнения работы необходимо использовать команду **passive-interface** и сконфигурировать стандартный маршрут.

Распределение нагрузки в протоколе RIP

Под распределением нагрузки понимается использование механизма, который позволяет маршрутизатору воспользоваться наличием нескольких маршрутов к требуемой точке назначения. Такие маршруты задаются либо статически, либо могут быть получены в результате работы протокола динамической маршрутизации, такого, например, как протокол RIP.

Протокол RIP способен осуществлять распределение нагрузки по нескольким маршрутам с равной стоимостью, число которых не должно превышать шести. Для протокола RIP количество одновременно используемых маршрутов с равной метрикой может быть указано с помощью команды **maximum-paths** *num_path*. Стандартно количество маршрутов для перераспределения нагрузки в большинстве протоколов маршрутизации не должно превышать четырех. Протокол RIP осуществляет балансировку нагрузки по циклическому принципу (round robin), который подразумевает, что по очереди используется сначала первый, потом второй, затем третий и так далее параллельный канал, и по достижении последнего процедура повторяется. Для многих интерфейсов стандартно включен механизм быстрой коммутации пакетов (Fast Switching), о чем свидетельствует команда **ip route-cache** в их конфигурации. В таком случае балансирование, или распределение, нагрузки происходит на основе IP-адресов получателей. Это утверждение означает, что при наличии, например, двух каналов все пакеты для IP-адреса одного получателя будут направлены по первому каналу, для другого получателя — по второму, для третьего — снова по первому и т.д. для каждого потока пакетов[1]. Если в конфигурации устройства ввести команду **no ip route-cache**, то в действие вступит программный механизм коммутации, который зачастую называют коммутацией с помощью программного процесса (process switching), и поведение устройства в таком случае будет отличаться. Подробнее этот механизм описан ниже в текущей главе.

На рис. 18.15 приведен пример распределения нагрузки по четырем маршрутам с равной метрикой. Маршрутизатор начинает работу, установив указатель на интерфейс, подсоединенный к маршрутизатору 1. После этого указатель циклически указывает на остальные интерфейсы и маршруты, например, 2-3-4, потом опять 1-2-3-4-1, и т.д.

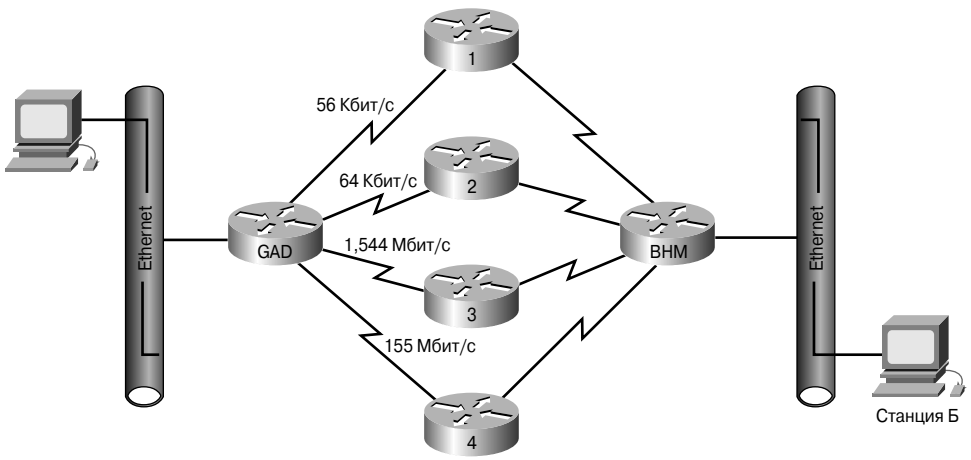


Рис. 18.15. Распределение нагрузки с помощью протокола RIP

[1] *Этот механизм называют* потоковой *балансировкой нагрузки (per flow load balancing). — Прим. ред.*

Поскольку метрикой протокола RIP является количество переходов, скорость каналов при этом не учитывается. Поэтому канал со скоростью 56 Кбит/с обрабатывает столько же данных, передаваемых между двумя сетями, сколько и канал со скоростью 155 Мбит/с.

Маршруты с равными стоимостями обычно можно найти с помощью команды **show ip route**. В примере 18.5 проиллюстрирована информация, которую дает команда **show ip route** для конкретной подсети с несколькими маршрутами.

Пример 18.5. Тестирование маршрутов с равными стоимостями с помощью команды show ip route

```
RouterC# show ip route 192.168.2.0
Routing entry for 192.168.2.0/24
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 192.168.4.2 on FastEthernet0/0, 00:00:18 ago
Routing Descriptor Blocks:
192.168.4.1, from 192.168.4.1, 00:02:45 ago, via FastEthernet0/0
Route metric is 1, traffic share count is 1
* 192.168.4.2, from 192.168.4.2, 00:00:18 ago, via FastEthernet0/0
Route metric is 1, traffic share count is 1
```

Отметим, что в приведенном выше выводе имеются два описательных блока. Каждый из них описывает один маршрут. Перед началом одного из блоков стоит символ “*”, указывающий, что блок соответствует активному маршруту, который используется для новых потоков данных.

Распределение нагрузки по нескольким маршрутам

Под распределением нагрузки понимается способность маршрутизатора передавать пакеты одного сеанса одному и тому же IP-получателю по нескольким маршрутам. Распределение нагрузки позволяет маршрутизатору воспользоваться преимуществами, вытекающими из наличия нескольких маршрутов к пункту назначения. Равноправные маршруты создаются статически сетевым администратором или могут быть получены посредством протоколов динамической маршрутизации, таких, как RIP, EIGRP, OSPF и IGRP. На рис. 18.16 проиллюстрировано распределение нагрузки.

Когда маршрутизатор узнает о наличии нескольких маршрутов к какой-либо сети при посредстве процессов маршрутизации или через протоколы маршрутизации, он заносит маршрут с минимальным административным расстоянием в свою таблицу маршрутизации. Иногда маршрутизатору приходится выбирать один из нескольких маршрутов, предоставляемых одним и тем же процессом маршрутизации и имеющих одно и то же административное расстояние. В таком случае маршрутизатор выбирает маршрут к пункту назначения, имеющий минимальную стоимость или метрику. Каждый процесс маршрутизации вычисляет стоимость присущим ему способом и поэтому иногда для того, чтобы сделать возможным распределение нагрузки, стоимости приходится задавать вручную.

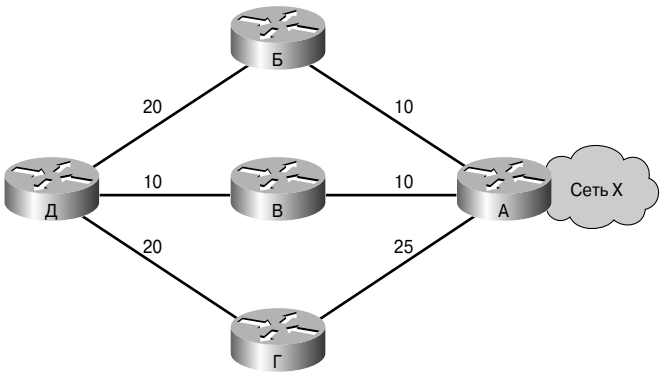


Рис. 18.16. Распределение нагрузки

Распределение нагрузки, как правило, может осуществляться только для маршрутов с одними и теми же административным расстоянием и стоимостью маршрута к пункту назначения. Программное обеспечение Cisco IOS ограничивает количество различных маршрутов для распределения нагрузки шестью маршрутами таблицы маршрутизации с равными метриками, однако некоторые протоколы внутреннего шлюза (Interior Gateway Protocol — IGP) устанавливают свои собственные ограничения. Например, протокол EIGRP позволяет использовать до четырех маршрутов с равными оценками.

Стандартно большинство протоколов IP-маршрутизации допускает установку в таблице маршрутизации максимум четырех параллельных маршрутов. Для статических маршрутов это ограничение всегда равно шести. Исключением является протокол внешней маршрутизации — протокол граничного шлюза (Border Gateway Protocol (BGP), который стандартно допускает существование только одного маршрута к пункту назначения.

Таким образом, максимальное количество маршрутов для распределения нагрузки находится в диапазоне от одного до шести. Для изменения стандартного количества параллельных маршрутов в таблице маршрутизации используется приведенная ниже команда режима конфигурирования маршрутизатора.

```
Router (config-router)# maximum-paths maximum
```

Количество неравных по величине пропускания каналов, на которых протокол IGRP может распределять нагрузку, достигает шести. В сетях протокола RIP распределение нагрузки может осуществляться только для каналов с одинаковым числом переходов, в то время как протокол IGRP для перераспределения нагрузки использует ширину полосы пропускания каналов.

На рис. 18.16 показаны три способа получения доступа к сети X:

- маршрут от маршрутизатора Д к маршрутизатору Б и далее к маршрутизатору А с метрикой 30;

- маршрут от маршрутизатора Д к маршрутизатору В и далее к маршрутизатору А с метрикой 20;
- маршрут от маршрутизатора Д к маршрутизатору Г и далее к маршрутизатору А с метрикой 45.

Маршрутизатор Д выбирает второй маршрут. Если два или более маршрута имеют равные метрики, то становится возможным распределение нагрузки.

При использовании IP-маршрутизации программное обеспечение Cisco IOS предлагает два способа распределения нагрузки:

- попакетное распределение нагрузки;
- распределение нагрузки по пунктам назначения.

Если включена коммутация посредством программного процесса (process switching), то маршрутизатор циклически использует разные маршруты для каждого нового пакета. Если же включена быстрая коммутация (Fast Switching), то в качестве адреса пункта назначения кэшируется только один из альтернативных маршрутов, поэтому все пакеты в потоке, связанном с конкретным узлом, отправляются по одному и тому же маршруту. Пакеты, исходящие из другого узла той же сети, могут быть отправлены по альтернативному маршруту; в этом случае происходит перераспределение потоков данных на основе адресов пунктов назначения (т.е. по потокам).

Практическое задание: распределение нагрузки по нескольким маршрутам
В этой лабораторной работе требуется сконфигурировать распределение нагрузки по нескольким маршрутам с помощью протокола RIP и проверить работу этого механизма.

Интеграция статических маршрутов в протокол RIP

Статические маршруты представляют собой определенные администратором пути, по которым принудительно направляются пакеты в указанный в них пункт назначения. Такие маршруты приобретают большое значение в том случае, когда программное обеспечение Cisco IOS не может определить маршрут к конкретному пункту назначения. Они также полезны для указания стандартного маршрута (иногда называемого "шлюзом последней надежды"), по которому направляются все пакеты, для которых отсутствует какой-либо определенный маршрут.

Маршрутизатор, на котором функционирует протокол RIP, может узнать адрес стандартной сети через обновление маршрутизации, полученное от другого маршрутизатора, на котором также работает протокол RIP. Альтернативной возможностью является самостоятельная генерация маршрутизатором стандартного маршрута.

Статические маршруты могут быть удалены с помощью команды глобального конфигурирования **`no ip route`**. Динамические маршруты могут быть заменены статическими сетевым администратором путем их явного указания за счет меньшего административного расстояния. Каждому протоколу динамической маршрутизации присуще стандартное значение административного расстояния, которое позволяет

использовать статический маршрут в качестве резервного вместо динамического маршрута в случае неработоспособности последнего.

Статические маршруты, указывающие на некоторые интерфейсы, стандартно не анонсируются посредством протокола RIP, поскольку они считаются маршрутами, которые ведут к непосредственно подсоединенным сетям, но, тем не менее, не теряют свой статический характер. Если статический маршрут назначен интерфейсу, который не указан в команде **network**, то ни один протокол динамической маршрутизации не анонсирует такой маршрут, кроме того случая, когда для протокола в конфигурации маршрутизатора задана команда **redistribute static**.

Если какой-либо интерфейс выходит из строя, то все проходящие через него статические маршруты удаляются из таблицы IP-маршрутизации локального устройства. Кроме того, если программное обеспечение не может найти действительный адрес следующего транзитного перехода для адреса, указанного маршрутизатору в статическом маршруте, то такой статический маршрут удаляется из таблицы IP-маршрутизации.

Статические маршруты вводятся намеренно сетевым администратором с тем, чтобы маршрутизатору был известен конкретный (явный) маршрут к пункту назначения. Динамические маршруты становятся известными маршрутизатору с помощью различных протоколов маршрутизации. В этом случае не гарантируется, что маршрутизатору будет всегда известен маршрут к требуемому получателю.

Для конфигурирования статического маршрута используется приведенная ниже команда режима глобального конфигурирования.

```
Router (config)# ip route prefix mask {address | interface}
[distance] [tag tag] [permanent]
```

На рис. 18.17 в маршрутизаторе GAD сконфигурирован статический маршрут, который будет использован вместо RIP-маршрута в случае, если последний станет недействителен.

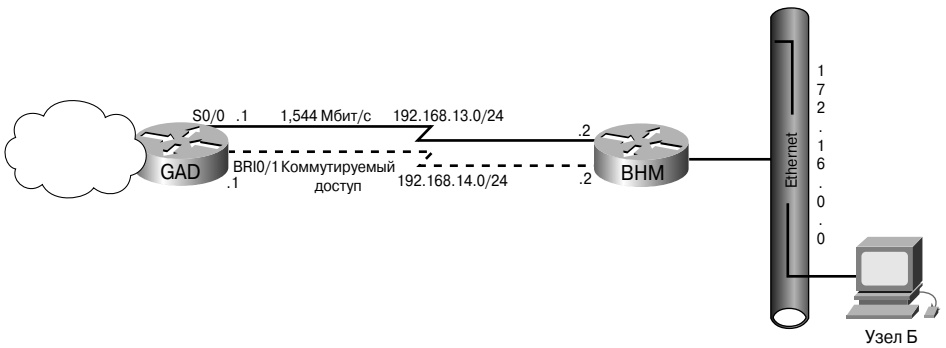


Рис. 18.17. Протокол RIP с плавающими статическими маршрутами

В примере 18.6 показан статический маршрут, добавляемый с административным расстоянием, равным 130-ти; такой маршрут называется плавающим статическим маршрутом (floating static). Плавающий статический маршрут задается путем объявления для него административного расстояния, равного 130-ти, которое превышает административное расстояние протокола RIP, равное 120-ти. Зачем необходимо менять расстояние для статического маршрута? Машрутизатор выберет наилучший маршрут на основании такого административного расстояния. Согласно принципу работы маршрутизации, устройство всегда предпочитает статические маршруты динамическим, поскольку у статических маршрутов административное расстояние всегда меньше. Для статических маршрутов стандартно расстояние равно 1. Сконфигурировав статический маршрут вручную с заданным административным расстоянием 130, администратор позволит устройству установить в таблицу маршрутизации маршрут протокола RIP, расстояние которого равно 120-ти. Если по причине отказа канала или соседнего устройства динамический маршрут будет удален из таблицы маршрутизации, устройство автоматически переключится на плавающий статический маршрут, который в данном случае будет резервным.

Следует помнить, что после того как администратор статически сконфигурирует маршрут к сети 172.16.0.0 через узел с адресом 192.168.14.2, такой маршрут не появится в таблице маршрутизации устройства. В ней будет присутствовать только динамический маршрут протокола маршрутизации RIP. Такое поведение — результат того, что администратор вручную установил административное расстояние для плавающего статического маршрута (130), которое больше стандартного расстояния протокола RIP. Только в том случае, когда динамический маршрут будет удален из таблицы (а такое может произойти тогда, когда, например, интерфейс **Serial 0/0** будет выключен или будет разорван подключенный к нему канал), статический маршрут появится в таблице маршрутизации устройства (пример 18.6).

Пример 18.6. Плавающий статический маршрут

```
GAD# configure terminal
GAD(config)# ip route 172.16.0.0 255.255.0.0 192.168.14.2 130
GAD(config)# ^z
GAD# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
             inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C        192.168.113.0/24 is directly connected, Serial0/0
C        192.168.14.0/24 is directly connected, BRI0/1
R        172.16.0.0/16 [120/1] via 192.168.13.2, 00:00:24, Serial0/0
```

Следует обратить внимание на то, о чем говорилось выше: статический маршрут отсутствует в таблице маршрутизации, поскольку для маршрута к требуемой сети-получателю указывается символ *R*, а не *S*[2]. Аналогично, если указать команду в режиме конфигурирования протокола маршрутизации **`redistribute static`**, на любом из соседних устройств можно увидеть такой статический маршрут; обозначен он будет символом *R*, поскольку был получен посредством анонсов протокола RIP. Без указанной команды статический маршрут будет доступен только на том устройстве, в котором он сконфигурирован.

Протокол IGRP

Как и RIP, протокол маршрутизации внутреннего шлюза (*Interior Gateway Routing Protocol — IGRP*) является дистанционно-векторным протоколом маршрутизации. Однако в отличие от протокола RIP, он не основан на стандартах, а является фирменным протоколом корпорации Cisco. Протокол IGRP прост в реализации, но вместе с тем является более развитым протоколом маршрутизации по сравнению с протоколом RIP и позволяет использовать большее количество параметров для определения наилучшего маршрута к пункту назначения. В этом разделе описано конфигурирование протокола IGRP, поиск и устранение ошибок, а также подробно рассмотрены следующие вопросы:

- функции протокола IGRP;
- метрики протокола IGRP;
- маршруты IGRP;
- функции обеспечения устойчивости протокола IGRP;
- конфигурирование IGRP;
- переход с протокола RIP на протокол IGRP;
- тестирование конфигурации IGRP;
- поиск и устранение ошибок в конфигурации протокола IGRP.

Функции протокола IGRP

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

---

[2] *Гораздо более надежным и все-таки первичным индикатором является адрес следующего транзитного перехода, 192.168.13.2, по которому также можно определить, что в данный момент не используется статический маршрут. — Прим. ред.*

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

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

Дистанционно-векторный протокол маршрутизации IGRP был разработан корпорацией Cisco. Этот протокол рассылает обновления маршрутизации с 90-секундными интервалами, анонсируя сети, принадлежащие конкретным автономным системам. Важнейшими характеристиками протокола IGRP являются следующие:

- протокол содержит разнообразные функции, позволяющие работать со сложными и запутанными топологиями сетей;
- он предоставляет высокий уровень гибкости, требуемый для работы с сегментами, имеющими различную ширину полосы пропускания и характеристики задержки;
- для протокола характерна высокая степень масштабируемости, позволяющая упростить работу в очень крупных сетях.

Стандартно в качестве метрики протокол маршрутизации IGRP использует ширину полосы пропускания и задержку. Кроме того, возможно иное конфигурирование протокола IGRP, при котором используется комбинация переменных параметров для вычисления сложной составной метрики.

В качестве параметров метрики могут выступать:

- ширина полосы пропускания;
- задержка;
- уровень загрузки канала;
- надежность канала.

ВНИМАНИЕ!

В некоторой литературе в качестве параметра метрики для протоколов IGRP и EIGRP ошибочно включают такой параметр, как MTU. Этот параметр никогда не использовался и не используется в качестве составной части метрики.

Презентация: сравнение протоколов маршрутизации RIP и IGRP
В этой презентации подробно описаны отличия двух указанных протоколов.

Презентация: обзор протокола маршрутизации IGRP
В этой презентации подробно описан процесс маршрутизации потоков данных протоколом IGRP.

Метрики протокола IGRP

С помощью команды **show ip protocols** отображаются параметры, фильтры и другая сетевая информация о протоколах маршрутизации, функционирующих в маршрутизаторе. Такая информация требуется для определения метрик K1-K5 и включает в себя максимальное количество переходов; она также используется для вычисления составной метрики протокола IGRP, которая вычисляется следующим образом:

метрика = [K1×полоса пропускания + K2×полоса пропускания/(256 – нагрузка) + + K3×задержка]×[K5/(надежность + K4)].

Параметр метрики K1 представляет ширину полосы пропускания, а параметр K3 — задержку. Стандартно значения параметров метрик K1 и K3 принимаются равными единице, а параметры K2, K4 и K5 устанавливаются равными нулю.

Стандартными значениями весов являются K1 = K3 = 1 и K2 = K4 = K5 = 0; в таком случае используется упрощенная формула расчета метрики протокола IGRP, в которой множитель [K5/(надежность + K4)] опущен. Композитная метрика рассчитывается по формуле:

метрика = полоса пропускания + задержка.

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

```
metric weights tos k1 k2 k3 k4 k5
```

Для нахождения ширины полосы пропускания необходимо выбрать наименьшее ее значение среди всех выходных интерфейсов и разделить это значение на 10 000 000. (Полоса пропускания выражается в Кбит/с с коэффициентом 10 000000.) Для вычисления задержки необходимо сложить ее значения для всех выходных интерфейсов и разделить это значение на 10 (задержка выражается в десятках долей микросекунды). Следует помнить о том, что наилучшим считается маршрут с наименьшей метрикой.

При выборе маршрута к пункту назначения такая составная метрика дает более точную характеристику маршрута, чем метрика протокола RIP, учитывающая только количество переходов. Маршрут с наименьшей метрикой принимается в качестве наилучшего.

Метрики протокола IGRP включают в себя следующие компоненты:

- **полосу пропускания (Bandwidth)** — выбирается наибольшее значение ширины полосы пропускания на маршруте;
- **задержку (Delay)** — кумулятивную задержку на интерфейсах при прохождении пакетов по маршруту;

- **надежность (Reliability)** — описывает надежность канала, ведущего к пункту назначения; эта величина определяется в процессе обмена тестовыми сообщениями (keepalives);
- **загрузку канала (Load)**, ведущего к пункту назначения; это значение выражается в битах в секунду.

Протокол IGRP использует составную метрику, которая вычисляется как функция полосы пропускания, задержки, загрузки и надежности канала. Стандартно в качестве параметров метрики используются только полоса пропускания и задержка, остальные параметры учитываются только в том случае, если их коэффициенты явно заданы в конфигурации. Значения задержки и полосы пропускания не измеряются в процессе работы устройством, а задаются в конфигурации командами **`delay`** и **`bandwidth`** определенного интерфейса. В примере 18.7 команда **`show ip route`** отображает в скобках значения метрик протокола IGRP. Первое значение представляет собой административное расстояние, а второе — вычисленное значение метрики. Канал с большей шириной полосы пропускания имеет меньшую метрику, аналогично маршрут с наименьшей задержкой также имеет меньшую метрику.

Пример 18.7. Результат выполнения команды `show ip route` (отображение значения метрик для маршрутов протокола IGRP)

```
RouterA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
            inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C        192.168.1.0/24 is directly connected, FastEthernet0/0
C        192.168.2.0/24 is directly connected, Serial0/0
I        192.168.3.0/24 [100/80135] via 192.168.2.2, 00:00:30,
           Serial0/0
```

Маршруты протокола IGRP

Протокол IGRP анонсирует три типа маршрутов:

- *внутренний (Interior route)* — представляет собой маршрут между подсетями сети, подсоединенной к интерфейсу маршрутизатора. Если сеть, подсоединенная к маршрутизатору, не имеет подсетей, то внутренние маршруты не анонсируются;

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

ВНИМАНИЕ!

На сегодняшний день протокол маршрутизации IGRP является устаревшим средством. Основной его недостаток состоит в том, что в нем отсутствует поддержка масок переменной длины (Variable-Length Subnet Mask — VLSM). Вместо того чтобы разрабатывать, например, протокол IGRP версии 2, для решения указанной проблемы корпорация Cisco на основе доказавшего свою ценность механизма IGRP создала новый протокол — EIGRP (Enhanced IGRP — усовершенствованный протокол IGRP).

Функции поддержки устойчивости сети протокола IGRP

Протокол IGRP имеет ряд функций, предназначенных для повышения устойчивости работы сети:

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

Таймеры удержания информации используются для предотвращения рассылки обновлений маршрутизации, содержащих маршруты, которые в действительности неработоспособны. Если маршрутизатор выходит из строя, то соседние маршрутизаторы определяют такое его состояние по отсутствию регулярных сообщений об изменении маршрутизации.

Использование механизма расщепления горизонта основано на предположении, что обычно нецелесообразно посылать информацию о маршруте в том же направлении, по которому она была получена. Использование этого механизма помогает предотвратить появление петель в маршрутизации.

Расщепление горизонта предотвращает появление кольцевых маршрутов между смежными маршрутизаторами, однако для предотвращения петель большей протяженности требуется использование другого механизма — удаления маршрутов. Строго говоря, увеличение метрики маршрутизации обычно указывает на появление петель маршрутизации. Удаление маршрутов в обратном направлении происходит посредством рассылки уведомлений для отмены маршрута и перевода его в состояние удержания. В протоколе IGRP такие сообщения рассылаются только в том случае, если метрика маршрута увеличилась в 1,1 раза или более.

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

- *Таймер обновления (Update timer*) задает частоту, с которой рассылаются сообщения об обновлении маршрутизации. Стандартно его значение равно 90 секундам.
- *Таймер действительности маршрута (Invalid timer*) задает промежуток времени ожидания, в течение которого маршрутизатор, не получая сообщения об обновлении по определенному маршруту, не рассылает информацию перед объявлением этого маршрута недействительным. В протоколе IGRP стандартно для этого параметра устанавливается значение в три раза бо́льше, чем период регулярной рассылки анонсов маршрутов.
- *Таймер удержания информации (Hold timer*) задает время, в течение которого информация о ненадежных маршрутах игнорируется. В протоколе IGRP стандартным значением для этого параметра принимается утроенное значение периода рассылки анонсов маршрутов, к которому добавляется 10 секунд.
- *Таймер сброса маршрута (Flush timer*) задает время до того момента, когда маршрут будет удален из таблицы маршрутизации. Стандартно значение этого параметра в семь раз больше периода рассылки анонсов маршрутизации.

В примере 18.8 приведена выводимая командой **`show ip protocols`** информация. Следует обратить внимание на строку, указывающую на функционирование протокола IGRP и значения его метрик.

Пример 18.8. Статистика маршрутизации протокола IGRP

```
RouterB# show ip protocols
Routing Protocol is "igrp 101"
Sending updates every 90 seconds, next due in 51 seconds
Invalid after 270 seconds, hold down 280, flushed after 630
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
IGRP maximum hopcount 100
IGRP maximum metric variance 1
```

```
Redistributing: igrp 101
Routing for Networks:
   192.168.2.0
   192.168.3.0
Routing Information Sources:

   Gateway Distance Last Update
   192.168.2.1 100 00:00:54
Distance: (default is 100)
```

Конфигурирование протокола IGRP

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

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

Для отключения процесса IGRP-маршрутизации используется форма этой команды с ключевым словом **no**:

```
RouterA(config)# no router igrp as-number
```

Под номером автономной системы понимается номер, идентифицирующий процесс маршрутизации протокола IGRP. Следует помнить, что такой номер не обязательно должен быть реальным номером автономной системы, которую присваивает соответствующая международная организация, например, ARIN, или номер частной автономной системы. Такой номер действует только внутри домена маршрутизации протокола IGRP и должен быть одинаков на всех маршрутизаторах, которые должны обмениваться информацией по протоколу IGRP. Этот номер представляет собой просто идентификатор процесса. Он также используется для маркировки информации о маршрутизации.

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

```
RouterA(config)# router igrp 101
RouterA(config-router)# network 192.168.1.0
```

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

```
RouterA(config)# no router igrp 101
RouterA(config-router)# no network 192.168.1.0
```

В примере 18.9 показана конфигурация протокола IGRP на маршрутизаторах *RouterA* и *RouterB*, принадлежащих автономной системе (Autonomous System — AS) с номером 101.

Пример 18.9. Конфигурирование протокола IGRP

```
RouterA(config)# router igrp 101
RouterA(config-router)# network 192.168.1.0
RouterA(config-router)# network 192.168.2.0
```

```
RouterB(config)# router igrp 101
RouterB(config-router)# network 192.168.2.0
RouterB(config-router)# network 192.168.3.0
```

Практическое задание 18.3.5. Конфигурирование протокола маршрутизации IGRP
В этой лабораторной работе требуется создать схему адресации с использованием адресов класса C и сконфигурировать на всех маршрутизаторах протокол IGRP.

Замена протокола RIP на IGRP в сети

Корпорация Cisco Systems в начале 1980-х годов была первой компанией в мире, которая, разработав протокол IGRP, смогла решить проблемы протокола RIP, связанные с маршрутизацией пакетов между внутренними маршрутизаторами сети. Протокол IGRP выбирает оптимальный путь для передачи данных на основании пропускной способности и задержки в канале сети между устройствами. Его конвергенция происходит значительно быстрее, чем конвергенция протокола RIP и, следовательно, протокол IGRP менее подвержен проблемам, которые связаны с возникновением петель в маршрутизации из-за неопределенности с выбором следующего транзитного узла. Кроме того, для этого фирменного протокола характерно менее строгое ограничение по количеству транзитных узлов (или, как говорят, диаметру сети), чем для наиболее распространенного дистанционно-векторного протокола RIP. Благодаря перечисленным выше усовершенствованиям протокол IGRP был развернут во многих крупных и сложных сетях с развитой топологией.

Ниже описаны основные действия, которые необходимо выполнить, чтобы заменить протокол RIP в сети на более современный IGRP.

Этап 1. Выполните команду **`show ip route`**, чтобы убедиться, что протокол RIP используется в качестве средства маршрутизации на маршрутизаторах (примеры 18.10 и 18.11).

Пример 18.10. Проверка работы существующего протокола маршрутизации для устройства RouterA

```
RouterA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
         inter area
       * - candidate default, U - per-user static route, o - ODR
```

```
       P - periodic downloaded static route

Gateway of last resort is not set

C        192.168.1.0/24 is directly connected, Loopback0
C        192.168.2.0/24 is directly connected, Serial0/0
R        192.168.3.0/24 [120/1] via 192.168.2.2, 00:01:09, Serial0/0
```

Пример 18.11. Проверка работы существующего протокола маршрутизации для устройства RouterB

```
RouterA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
           inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

I    192.168.1.0/24 [100/80135] via 192.168.2.2, 00:00:28, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

Этап 2. Следует сконфигурировать протокол IGRP для маршрутизаторов RouterA и RouterB, как показано в примере 18.12.

Пример 18.12. Конфигурирование протокола IGRP для маршрутизаторов RouterA и RouterB

```
! Конфигурация первого маршрутизатора
RouterA# configure terminal
RouterA(config)# router igrp 101
RouterA(config-router)# network 192.168.1.0
RouterA(config-router)# network 192.168.2.0
! Конфигурация второго маршрутизатора

RouterB# configure terminal
RouterB(config)# router igrp 101
RouterB(config-router)# network 192.168.2.0
RouterB(config-router)# network 192.168.3.0
```

Этап 3. Следует использовать команду **show ip protocols** для маршрутизаторов RouterA и RouterB и убедиться в том, что протокол запущен.

Этап 4. Следует ввести команду **show ip route** для обоих маршрутизаторов и убедиться, что необходимые сети присутствуют в таблице маршрутизации устройств.

Практическое задание 18.3.6. Стандартные маршруты в протоколах маршрутизации RIP и IGRP

В этой лабораторной работе необходимо сконфигурировать стандартный маршрут и распространить его по сети с помощью протокола RIP. После того как все в конфигурации устройств будет работать правильно, следует перейти в такой сети с протокола RIP на протокол IGRP и также сконфигурировать стандартный маршрут, а затем распространить его к другим устройствам.

Проверка конфигурации протокола IGRP

Для проверки правильности конфигурации протокола IGRP необходимо использовать команду **show ip route** и проанализировать маршруты IGRP, отмеченные символом "I".

Дополнительно используются следующие команды проверки конфигурирования протокола IGRP:

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

Для проверки правильности конфигурирования Ethernet-интерфейса следует ввести команду **show interface fa0/0**, как показано в примере 18.13.

Пример 18.13. Выводимая командой show interface информация

```
RouterA# show interface fa0/0
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 0009.7c89.5620 (bia 0009.7c89.5620)
Internet address is 192.168.1.1/24
--- Остальная информация опущена ---
```

Для того чтобы выяснить, функционирует ли протокол IGRP на маршрутизаторе, следует использовать команды, проиллюстрированные в примере 18.14.

Пример 18.14. Выводимая командами `show ip protocols` и `show running-config` информация

```
RouterA# show ip protocols
Routing Protocol is "igrp 101"
--- Остальная информация опущена ---
RouterA# show running-config | begin igrp
router igrp 101
network 192.168.1.0
network 192.168.2.0
!
--- Остальная информация опущена ---
```

Для проверки правильности указанного IP-адреса используется команда, приведенная в примере 18.15.

Пример 18.15. Выводимая командой `show running-config interface` информация

```
RouterA# show running-config interface fa0/0
Building configuration...
Current configuration:
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
end
```

В примере 18.16 показан результат выполнения команды **`show ip route`** и отображены маршруты, которые доступны через интерфейсы данного маршрутизатора.

Пример 18.16. Выводимая командой `show ip route` информация

```
RouterA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
          inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Serial0/0
I    192.168.3.0/24 [100/80135] via 192.168.2.2, 00:01:00, Serial0/0
```

Поиск и устранение ошибок в конфигурации протокола IGRP

Большинство ошибок в конфигурации протокола IGRP связаны с неверными параметрами команд **network**, с неверным указанием подсетей, которые не являются непрерывными, или неправильным указанием номеров автономных систем.

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

- команда **show ip protocols** используется для отображения общей информации протокола IP-маршрутизации;
- команда **show ip route** используется для отображения таблицы IP-маршрутизации маршрутизатора;
- команда **debug ip igrp events** используется для отображения информации общего характера об IGRP-маршрутизации для данной сети;
- команда **debug ip igrp transactions** отображает сообщения, полученные от соседних маршрутизаторов, в которых запрашивается обновление маршрутов, и широковещательные сообщения, посылаемые маршрутизатором-иииициатором соседнему маршрутизатору;
- команда **ping** используется для определения доступности конкретного IP-адреса;
- команда **traceroute** используется для трассировки пути перемещения пакета от компьютера пользователя к узлу сети Internet; при этом выводится число требуемых переходов и время, затрачиваемое на такие переходы.

В примере 18.17 показан результат выполнения команды **debug ip igrp events**.

Пример 18.17. Выводимая командой debug ip igrp events информация

```
RouterA# debug ip igrp events
IGRP event debugging is on
00:21:38: IGRP: sending update to 255.255.255.255 via FastEther-
net0/0 (192.168.1.1)

00:21:38: IGRP: Update contains 0 interior, 2 system, and 0 exterior
routes.
00:21:38: IGRP: Total routes in update: 2
00:21:38: IGRP: sending update to 255.255.255.255 via Serial0/0
(192.168.2.1)
00:21:38: IGRP: Update contains 0 interior, 1 system, and 0 exterior
routes.
00:21:38: IGRP: Total routes in update: 1
```

В примере 18.18 показан результат выполнения команды **debug ip igrp transactions**.

Пример 18.18. Выводимая командой `debug ip igrp transactions` информация

```
RouterA# debug ip igrp transactions
IGRP protocol debugging is on
00:22:17: IGRP: received update from 192.168.2.2 on Serial0/0
00:22:17: network 192.168.3.0, metric 80135 (neighbor 110)
00:23:07: IGRP: sending update to 255.255.255.255 via FastEther-
net0/0 (192.168.1.1)
00:23:07: network 192.168.2.0, metric=80125
00:23:07: network 192.168.3.0, metric=80135
00:23:07: IGRP: sending update to 255.255.255.255 via Serial0/0
(192.168.2.1)
00:23:07: network 192.168.1.0, metric=110
```

Если обнаруживается, что был задан неправильный номер автономной системы (AS), то его следует откорректировать, как показано в примере 18.19.

Пример 18.19. Корректировка номера автономной системы с включенным режимом отладки с помощью команды `debug ip igrp transactions`

```
RouterA(config)# no router igrp 102
RouterA(config)# router igrp 101
RouterA(config-router)# network 192.168.1.0
RouterA(config-router)# network 192.168.2.0
00:27:50: IGRP: broadcasting request on FastEthernet0/0
00:27:50: IGRP: sending update to 255.255.255.255 via
   FastEthernet0/0
(192.168.1.1)
00:27:51: IGRP: Update contains 0 interior, 0 system,
   and 0 exterior routes.
00:27:51: IGRP: Total routes in update: 0 - suppressing null
00:28:01: IGRP: sending update to 255.255.255.255 via
   FastEthernet0/0
(192.168.1.1)
00:28:01: network 192.168.2.0, metric=80125
00:28:01: network 192.168.3.0, metric=80135
00:28:01: IGRP: Update contains 0 interior, 2 system, and 0
   exterior routes.
00:28:01: IGRP: Total routes in update: 2
00:28:01: IGRP: sending update to 255.255.255.255 via Serial0/0
   (192.168.2.1)
00:28:01: network 192.168.1.0, metric=110
00:28:01: IGRP: Update contains 0 interior, 1 system, and 0 exterior
    routes.
00:28:01: IGRP: Total routes in update: 1
```

Лабораторная работа 18.3.7. Конфигурирование стандартного маршрута в протоколах RIP и IGRP

В этой лабораторной работе требуется сконфигурировать стандартный маршрут и с помощью протокола RIP распространить информацию среди остальных маршрутизаторов. После того как эта конфигурация будет правильно задана и протестирована, следует перейти с протокола RIP на протокол IGRP и для этого протокола также сконфигурировать стандартный маршрут.

Практическое задание 18.3.8. Распределение нагрузки среди маршрутов с неравными оценками с помощью протокола IGRP

В этой лабораторной работе требуется сконфигурировать и настроить протокол IGRP для распределения нагрузки по маршрутам с неравной стоимостью и пронаблюдать работу механизма распределения нагрузки с помощью команд отладки.

Резюме

В этой главе были рассмотрены следующие ключевые темы:

- при изменении топологии сети информация маршрутизации поддерживается в актуальном состоянии путем рассылки маршрутизаторами анонсов маршрутизации;
- петли в маршрутизации могут возникать в сети вследствие наличия альтернативных маршрутов, медленной конвергенции или несогласованных обновлений маршрутизации;
- для предотвращения зацикливания пакетов может быть задано максимально допустимое количество переходов;
- для предотвращения петель в маршрутизации могут быть использованы три механизма: расщепление горизонта, мгновенные изменения и таймеры удержания информации;
- различные дистанционно-векторные протоколы используют механизм удаления маршрутов в обратном направлении для предотвращения крупных петель маршрутизации и для получения информации о доступности подсети или сети;
- конфигурирование протоколов маршрутизации RIP и IGRP;
- использование команды **`ip classless`**;
- было объяснено, как найти и устранить ошибки в конфигурациях протоколов RIP и IGRP;
- описано тестирование протоколов RIP и IGRP;
- конфигурирование стандартных маршрутов.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Ключевые термины

Анонсы маршрутизации (routing update) — это сообщения, рассылаемые между маршрутизаторами объединенной сети, в которых содержится информация о достижимости сети и соответствующая оценка маршрута. Обновления маршрутизации обычно рассылаются с постоянными интервалами, а также в случае изменений в сетевой топологии. *Ср. с мгновенными изменениями (flash update).*

Внешние маршруты (exterior routes) представляют собой маршруты, ведущие к узлам, расположенным вне данной автономной системы и рассматриваемые в качестве возможного стандартного шлюза.

Внутренние маршруты (interior routes) — это маршруты между подсетями некоторой сети, подсоединенной к интерфейсу маршрутизатора. Если подсоединенная к маршрутизатору сеть не имеет подсетей, то внутренние маршруты протоколом IGRP не анонсируются.

Зацикливание пакета (count to infinity) — проблема, которая может возникнуть в некоторых алгоритмах маршрутизации с низкой скоростью конвергенции и состоящая в том, что маршрутизаторы бесконечно увеличивают метрику количества переходов к какой-либо сети. Для предотвращения такой проблемы обычно устанавливается максимально допустимое количество переходов.

Конвергенция (convergence) — это способность группы устройств объединенной сети, использующих конкретный протокол маршрутизации, согласовать друг с другом информацию о топологии сети после того, как в ней произошли изменения. Требуемое для этого время определяет скорость конвергенции.

Мгновенные изменения (triggered update) представляют собой сообщения об изменении маршрутизации, рассылаемые в случае изменения топологии сети, не дожидаясь истечения времени таймера анонсов.

Метрика маршрутизации (routing metric) — метод, с помощью которого алгоритм маршрутизации сравнивает маршруты. Информация о метрике маршрутов хранится в таблицах маршрутизации и рассылается в сообщениях обновления маршрутизации. В качестве параметров метрики могут использоваться ширина полосы пропускания, затраты на передачу, задержка, количество переходов, загрузка канала, максимальный модуль передачи (MTU), стоимость маршрута и надежность канала. Чаще всего ее называют просто метрикой, опуская вторую часть термиа.

Протокол маршрутизации (routing protocol) — это протокол, осуществляющий маршрутизацию путем реализации некоторого алгоритма маршрутизации. Примерами протоколов маршрутизации могут служить IGRP, OSPF и RIP.

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP) — это протокол внутреннего шлюза (IGP), разработанный корпорацией Cisco для решения проблем, возникающих при осуществлении маршрутизации в крупных неоднородных сетях. *Ср. с протоколом EIGRP. См. также IGP, OSPF и RIP.*

Протокол маршрутной информации (Routing Information Protocol — RIP) — это протокол внутреннего шлюза (IGP), поставляемый вместе с системой BSD UNIX. В свое время он являлся наиболее часто используемым протоколом локальных сетей. Протокол RIP в качестве метрики маршрутизации использует количество переходов.

Расщепление горизонта (split horizon) — это механизм маршрутизации, с помощью которого предотвращается рассылка информации о маршруте через интерфейс маршрутизатора, через который она была получена. Расщепление горизонта является одним из способов предотвращения образования петель маршрутизации.

Системные маршруты (system routes) — это маршруты между отдельными сетями, входящими в одну автономную систему. Программное обеспечение Cisco IOS создает системные маршруты на основе информации интерфейсов непосредственно подсоединенных сетей и информации, предоставляемой другими IGRP-маршрутизаторами или серверами доступа. Системные маршруты не содержат информацию о подсетях.

Смежное устройство (adjacent neighbor) — так называются два непосредственно соединенных маршрутизатора, обменивающиеся друг с другом информацией маршрутизации.

Сообщения удаления маршрутов в обратном направлении (poison reverse updates) представляют собой анонсы маршрутизации, используемые для предотвращения протяженных петель маршрутизации. Чаще всего увеличение метрики маршрута, как правило, свидетельствует о возникновении петель. В таком случае сообщения удаления рассылаются для удаления маршрута из таблицы маршрутизации и перевода его в режим удержания.

Таблица маршрутизации (routing table) — представляет собой некоторую разновидность базы данных, хранящуюся в маршрутизаторе или другом устройстве объединенной сети, в которой содержится информация о маршрутах к конкретным сетям-получателям и, в большинстве случаев, метрики, связанные с этими маршрутами.

Таймер действительности маршрута (invalid timer). Значение этого таймера задает время, в течение которого маршрутизатор в случае отсутствия сообщений об обновлении некоторого маршрута ожидает, перед тем как объявить этот маршрут недействительным. В протоколе IGRP стандартным значением этого таймера является утроенный период анонсов маршрутизации.

Таймер обновлений маршрутизации (update timer). Период этого таймера задает частоту рассылки обновлений маршрутизации. В протоколе IGRP стандартно значение этого таймера устанавливается равным 90 секундам.

Таймер сброса маршрутов (flush timer). Период этого таймера задает время, которое проходит до того, как маршрут будет удален из таблицы маршрутизации. В протоколе IGRP стандартное значение этого таймера равно значению периода обновлений маршрутизации, умноженному на семь.

Таймер удержания (hold-time timer) задает время, в течение которого новые сообщения об обновлениях маршрутизации игнорируются. В протоколе IGRP стандартное значение таймера удержания равно утроенному значению периода обновлений маршрутизации, к которому добавляется 10 секунд.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. К каким записям таблицы маршрутизации обращается маршрутизатор в первую очередь?

а) К записям, относящимся к непосредственно подсоединенным сетям или подсетям.

б) К записям, информация в которых была получена с помощью программного обеспечения Cisco IOS.

в) К записям, для которых известны IP-адреса и маски подсетей.

г) К записям, информация в которых была получена от других маршрутизаторов.

2. Какое из приведенных выражений наилучшим образом описывает статический маршрут?

а) Запись таблицы маршрутизации, используемая для направления фреймов, для которых адрес следующего перехода не указан явным образом в таблице маршрутизации.

б) Явно сконфигурированный и введенный в таблицу маршрут, которому отдается предпочтение перед маршрутами, выбранными протоколами динамической маршрутизации.

в) Маршрут, который автоматически подстраивается к изменениям сетевой топологии и изменениям характера передаваемых данных.

г) Маршрут, который самопроизвольно настраивается для передачи фреймов внутри сетевой топологии.

3. Какое из приведенных выражений наилучшим образом описывает стандартный маршрут?

а) Запись таблицы маршрутизации, используемая для пересылки фреймов, для которых адрес следующего перехода не указан явным образом в таблице маршрутизации.

б) Маршрут, который был явным образом сконфигурирован и введен в таблицу маршрутизации.

в) Маршрут, который автоматически подстраивается к изменениям сетевой топологии и изменениям характера передаваемых данных.

г) Маршрут, который самопроизвольно настраивается для передачи фреймов внутри сетевой топологии.

4. Для чего используются внешние протоколы маршрутизации?

а) Для обмена информацией между узлами некоторой сети.

б) Для обмена информацией внутри отдельной автономной системы.

в) Для обмена данными между автономными системами.

г) Для создания обеспечивающей совместимость инфраструктуры между сетями.

5. Для чего используются внутренние протоколы маршрутизации?

а) Для создания обеспечивающей совместимость инфраструктуры между сетями.

б) Для обмена данными между автономными системами.

в) Для обмена информацией между узлами некоторой сети.

г) Для обмена информацией внутри отдельной автономной системы.

6. Какая из приведенных ниже задач выполняется в режиме глобального конфигурирования?

а) Задание номеров IP-сетей путем указания номеров подсетей.

б) Включение в маршрутизаторе протокола маршрутизации, такого, как RIP и IGRP.

в) Конфигурирование для сетей и подсетей адресов и масок.

г) Указание метрики маршрутизации для нахождения наилучшего маршрута к каждой подсети.

7. Какую метрику использует протокол RIP для определения наилучшего маршрута, по которому следует отправить сообщение?

а) Полосу пропускания.

б) Количество переходов.

в) Изменяется в зависимости от типа сообщения.

г) Административное расстояние.

8. Какую команду следует использовать в том случае, если есть подозрение, что один из маршрутизаторов, подсоединенных к данной сети, сообщает неправильную информацию маршрутизации?

а) `router(config)# show ip route`.

б) `router# show ip route`.

в) `router> show ip protocol`.

г) `router(config-router)# show ip protocol`.

9. Для чего отображается таблица IP-маршрутизации?

а) Для указания маршрутизатору расписания рассылки обновлений маршрутизации.

б) Для просмотра адресов сетей-получателей и соответствующих им транзитных переходов.

в) Чтобы узнать, откуда поступают дейтаграммы.

г) Для установки параметров и фильтров для маршрутизатора.

10. Какую из приведенных ниже команд следует использовать для того, чтобы узнать, какой протокол маршрутизации сконфигурирован в маршрутизаторе?

а) `router> show router protocol`.

б) `router(config)> show ip protocol`.

в) `router(config)# show router protocol`.

г) `router> show ip protocol`.

11. Что означает последнее число в такой команде: `Router (config)# ip route 2.0.0.0 255.0.0.0 1.0.0.2 5`?

а) Количество переходов.

б) Количество маршрутов к пункту назначения.

в) Административное расстояние.

г) Номер ссылки на получателя в таблице маршрутизации.

12. О чем говорит значение административного расстояния, равное 15-ти?

а) О том, что IP-адрес является статическим.

б) О том, что IP-адрес является динамическим.

в) О том, что полученная информация о маршрутах из данного источника относительно надежна.

г) О том, что полученная информация о маршрутах из данного источника относительно ненадежна.

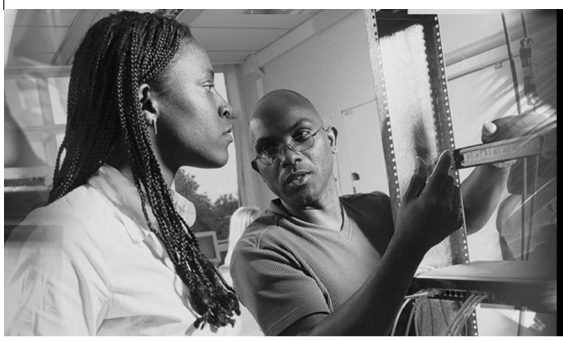
13. Какую из приведенных ниже команд следует использовать в том случае, если к объединенной сети добавлена новая локальная сеть и требуется вручную добавить эту сеть в таблицу маршрутизации?

а) `router (config)> ip route 2.0.0.0 255.0.0.0 via 1.0.0.2`.

б) `router (config)# ip route 2.0.0.0 255.0.0.0 1.0.0.2`.

в) `router (config)# ip route 2.0.0.0 via 1.0.0.2`.

г) `router (config)# ip route 2.0.0.0 1.0.0.2 using 255.0.0.0`.



ГЛАВА 19
Сообщения об ошибках и управляющие сообщения протокола TCP/IP

В этой главе...

- описаны функции протокола ICMP;
- рассмотрены различные типы сообщений об ошибках протокола ICMP и методы их идентификации;
- рассмотрены возможные причины появления сообщений об ошибках протокола ICMP и методы их идентификации;
- рассмотрены разнообразные управляющие сообщения протокола ICMP, используемые в современных сетях;
- рассмотрены ситуации, в которых используются управляющие сообщения протокола ICMP;
- описан механизм доставки сообщений протокола ICMP;
- рассмотрены эхо-сообщения;
- указаны дополнительные средства сообщений об ошибках;
- описаны сообщения о перенаправлении пакетов протокола ICMP;
- рассмотрены механизмы синхронизации времени и методы оценки времени доставки информации;
- описаны информационные запросы и форматы ответных сообщений;
- рассмотрены сообщения обнаружения маршрутизаторов;
- описаны запросы маски адреса;
- описаны сообщения-запросы к маршрутизаторам;
- описаны сообщения управления потоком и заторами в сети.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

протокол управляющих сообщений в сети Internet, с. 846,
протокол управления передачей/протокол сети Internet, с. 847,
дейтаграмма, с. 848,
ping, с. 850,
одноадресатное сообщение, с. 862,
широковещательное сообщение, с. 862,
многоадресатный адрес, с. 864.

После того как мы рассмотрели процесс конфигурирования маршрутизатора, следует изучить сообщения об ошибках и управляющие сообщения стека протоколов управления передачей и протокола Internet (Transmission Control Protocol/Internet Protocol — TCP/IP). В этой главе описан процесс пересылки Internet-протоколом управляющих сообщений (Internet Control Message Protocol — ICMP) и функции управления и контроля ошибок. Кроме того, в ней рассматриваются возможные причины появления сообщений об ошибках протокола ICMP и их идентификация.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в этой главе.

Обзор сообщений об ошибках стека протоколов TCP/IP

Основная функция протокола IP заключается в обеспечении обмена данными между узлами сети. Структура протокола IP позволяет решать задачи, связанные с сетями и отдельными их узлами. Такая возможность отличает протокол IP от немаршрутизируемых протоколов, которые работают с отдельными станциями и узлами, но не могут различать целые сети. Влияние и распространение протокола IP настолько расширилось, что, кроме использования его в качестве протокола передачи данных по глобальной сети Internet, он стал стандартным внутренним протоколом в малых локальных сетях, в которых использование возможностей маршрутизации протокола IP не является обязательным.

Ограничение протокола IP состоит в том, что он является системой негарантированной доставки. В нем отсутствуют механизмы, гарантирующие, что данные будут доставлены получателю независимо от проблем, которые могут возникнуть в сети. Данные могут не поступить к получателю по различным причинам, таким, как сбой в работе оборудования, неправильное конфигурирование или некорректная информация о маршрутах. Если промежуточное устройство, такое, как маршрутизатор, выходит из строя или устройство-получатель отсоединено от сети, то доставка данных становится невозможной. В этом причина того, что приложения, использующие протокол IP, обычно работают быстрее — они не используют механизмы контроля ошибок и надежной доставки, имеющиеся в протоколе TCP. Для обнаружения упомянутых выше ошибок при передаче протокол IP использует *протокол управляющих сообщений в сети Internet* (*Internet Control Message Protocol — ICMP*). Протокол ICMP уведомляет отправителя данных о том, что при их доставке произошла ошибка.

В следующих разделах приведен обзор различных типов сообщений об ошибках протокола ICMP и их формат. Знание сообщений об ошибках протокола ICMP и потенциальных причин появления таких сообщений является существенной частью процесса поиска и устранения ошибок в сетях.

Протокол управляющих сообщений в сети Internet (ICMP)

Протокол ICMP является одним из компонентов *стека TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол сети Internet)*, который компенсирует неспособность протокола IP гарантированно доставлять данные. Вместе с тем протокол ICMP не устраняет ненадежность передачи данных протоколом IP. Он лишь уведомляет отправителя данных о том, что при их доставке возникли проблемы. На рис. 19.1 показано место протокола ICMP в модели TCP/IP.

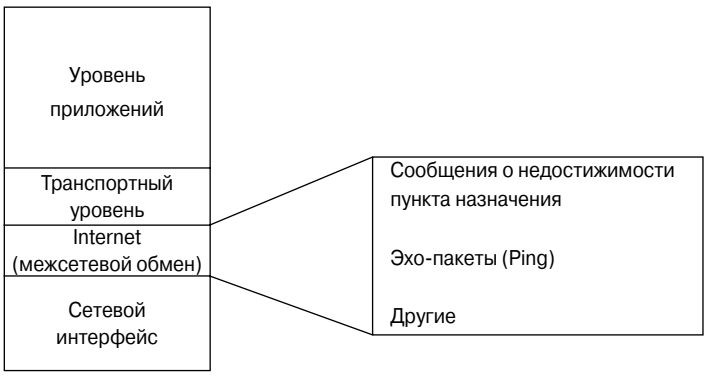


Рис. 19.1. Протокол ICMP и модель TCP/IP

В этом разделе рассматриваются различные аспекты протокола ICMP, включая доставку сообщений этого протокола, сообщения об ошибках и их устранение, а также вопросы достижимости сетей.

Извещения об ошибках и исправление ошибок

Протокол ICMP является механизмом отправки сообщений об ошибках для протокола IP. Если при доставке дейтаграммы происходит ошибка, протокол ICMP сообщает об этом отправителю дейтаграммы. Например, предположим, что *рабочая станция 1*, показанная на рис. 19.2, посылает дейтаграмму *рабочей станции 6*. Если соответствующий интерфейс *маршрутизатора B* выходит из строя, этот маршрутизатор использует протокол ICMP для отправки *рабочей станции 1* сообщения о том, что доставка дейтаграммы оказалась невозможной. Протокол ICMP не устраняет возникшую в сети проблему.

В примере на рис. 19.2 ICMP не пытается устранить проблему с интерфейсом *маршрутизатора B*, которая не позволяет доставить дейтаграмму. Все, что может сделать протокол ICMP, — это отправить *рабочей станции 1* сообщение об ошибке.

Маршрутизатор B не уведомляет промежуточные устройства о неудачной попытке доставки дейтаграммы. Соответственно, *маршрутизатор B* не посылает ICMP-сообщения *маршрутизаторам A* и *Б*, а также переславшему данные ближайшему устройству. У *маршрутизатора B* нет информации о том, по какому маршруту поступила

к нему эта *дейтаграмма*. Дейтаграммы содержат только информацию об IP-адресах отправителя и получателя, но не содержат информацию о промежуточных устройствах. Устройству, отправляющему сообщение, известен лишь IP-адрес отправителя, с которым можно установить связь. Хотя *маршрутизаторы А* и *Б* не уведомляются об ошибке непосредственно, они все же могут узнать о вышедшем из строя интерфейсе *маршрутизатора В*. Однако распространение подобной информации соседним маршрутизаторам не входит в функции протокола ICMP. Вместо этого протокол ICMP сообщает отправителю о состоянии доставляемого пакета, но не распространяет информацию об изменениях в сети.

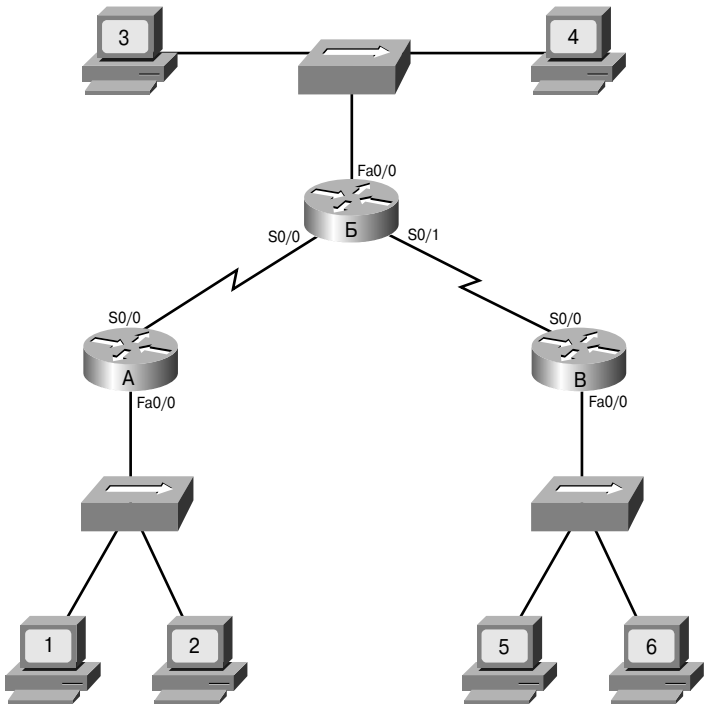


Рис. 19.2. Пересылка сообщений об ошибках

Доставка сообщений протокола ICMP

Сообщения протокола ICMP доставляются с использованием протокола IP. ICMP-сообщения инкапсулируются в дейтаграммы, точно так же, как и обычные данные, доставляемые по протоколу IP. В табл. 19.1 показана инкапсуляция ICMP-пакета в поле данных IP-дейтаграммы. Заголовок фрейма может формироваться по протоколу локальной сети, такому, как Ethernet, или по протоколу распределенной сети, такому, например, как HDLC.

Таблица 19.1. Инкапсуляция данных протокола ICMP

Заголовок фрейма	Заголовок IP-дейтаграммы	Заголовок протокола ICMP	Данные протокола ICMP
Заголовок фрейма	Заголовок IP-дейтаграммы	Поле данных IP-дейтаграммы	
Заголовок фрейма	Поле данных фрейма		

Когда данные поступают на сетевой уровень, они инкапсулируются в дейтаграмму. После этого дейтаграмма и инкапсулированные в ней данные вновь инкапсулируются во фрейм на канальном уровне. Сообщения протокола ICMP содержат в заголовках свою собственную информацию. Однако эта информация вместе с данными протокола ICMP инкапсулируется в дейтаграмму и передается таким же образом, что и все остальные данные. Поэтому сообщения об ошибках также подвержены риску быть утерянными при передаче. Таким образом, может возникнуть ситуация, в которой сами сообщения об ошибках могут создать новые ошибки, что лишь усложнит ситуацию с затором в уже работающей со сбоями сети. По этой причине ошибки, созданные сообщениями ICMP, не генерируют свои собственные ICMP-сообщения. Следовательно, возможен случай, когда при доставке дейтаграммы происходит ошибка, но о ней не сообщается отправителю данных.

Недостижимые сети

Возможность осуществления связи через сеть зависит от описанных ниже трех основных условий.

- В станции-отправителе и получателе должен быть правильно сконфигурирован стек протоколов TCP/IP. Это требование включает в себя установку средств стека протоколов TCP/IP и соответствующее конфигурирование IP-адреса и маски подсети. Если предполагается отправка дейтаграмм за пределы локальной сети, то должен быть сконфигурирован и стандартный шлюз.
- Для передачи дейтаграммы от устройства-отправителя, находящегося в одной сети, в сеть получателя через другие сети в последних должны присутствовать соответствующие промежуточные устройства. Эту функцию выполняют маршрутизаторы.
- На интерфейсах маршрутизатора должны быть правильно сконфигурированы протокол TCP/IP и протокол маршрутизации или статические маршруты.

Если перечисленные выше условия не выполнены, то осуществление связи невозможно. Например, отправитель может послать дейтаграмму по несуществующему IP-адресу или устройству-получателю, которое отсоединено от сети. Причиной невозможности доставки может стать также маршрутизатор, если соответствующий его интерфейс вышел из строя или он не обладает информацией, необходимой для нахождения сети-получателя. В таком случае недоступная сеть получателя называется *недостижимой сетью* (*unreachable network*).

Сообщения о недостижимости пункта назначения могут включать в себя следующие виды информации:

- **сеть недостижима —** это сообщение обычно свидетельствует об ошибках в маршрутизации или адресации;
- **узел недостижим —** это сообщение обычно свидетельствует об ошибках при доставке, например, об ошибочной маске подсети;
- **протокол недоступен (недостижим) —** это сообщение обычно свидетельствует о том, что пункт назначения не поддерживает протокол верхнего уровня, указанный в пакете;
- **порт недостижим —** это сообщение обычно свидетельствует о том, что TCP-порт (сокет) недоступен.

На рис. 19.3 показан маршрутизатор, получающий пакет, который он не может доставить в конечный пункт назначения. Невозможность доставить пакет может быть связана с тем, что маршрут к пункту назначения неизвестен. Поскольку такого маршрута нет, маршрутизатор посылает отправителю сообщение протокола ICMP о недостижимости узла.

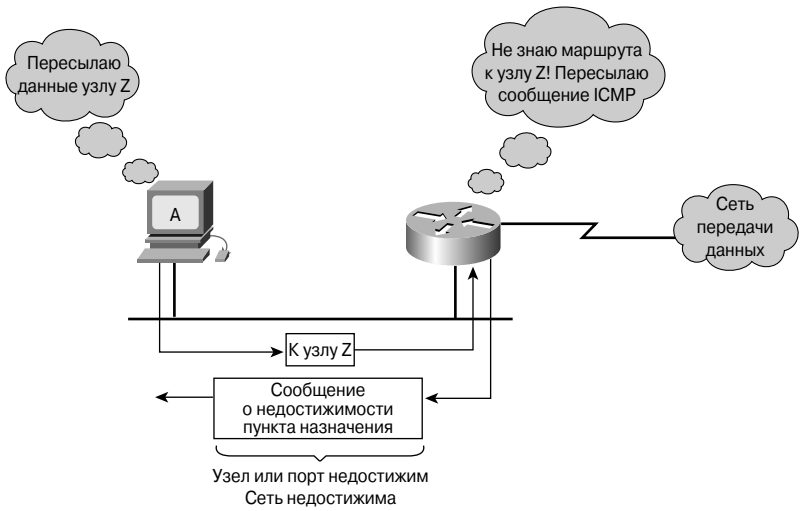


Рис. 19.3. Отправка ICMP-сообщения о недостижимости узла

Использование команды ping для проверки достижимости пункта назначения

Протокол ICMP может быть использован для тестирования доступности конкретного пункта назначения. На рис. 19.4 показано, как протокол ICMP используется для отправки сообщения эхо-запроса устройству-получателю. Когда устройство-получатель получает этот запрос, оно создает ответное сообщение и направляет его

устройству, которое было отправителем запроса. Получение отправителем запроса этого эхо-ответа свидетельствует о достижимости получателя с помощью протокола IP.

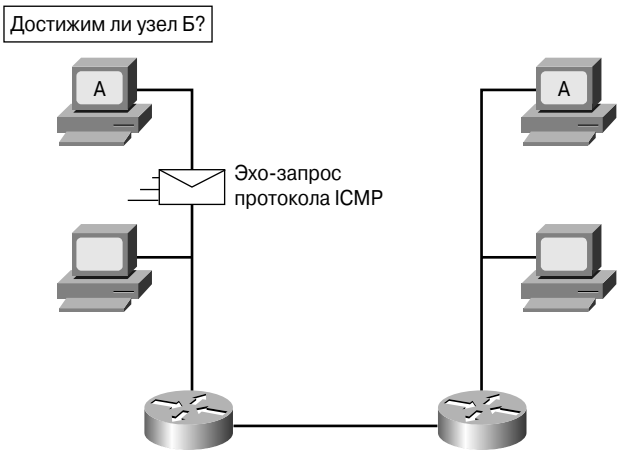


Рис. 19.4. Эхо-запрос

Сообщение эхо-запроса обычно генерируется с помощью команды **`ping`**, как показано в примере 19.1. В нем команда **`ping`** используется с IP-адресом устройства-получателя. Пример 19.1 и рис. 19.5 иллюстрируют успешное выполнение команды **`ping`** (отправку эхо-запроса и получение эхо-ответа).

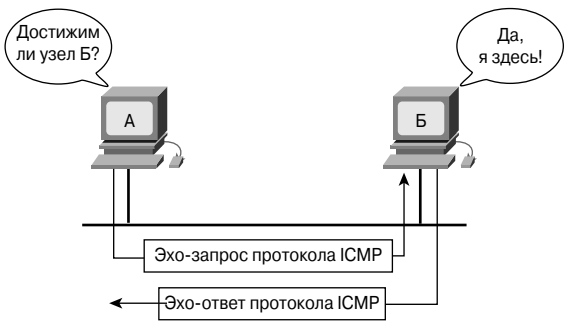


*Рис. 19.5. Выполнение команды **`ping`***

Пример 19.1. Эхо-запрос, инициированный командой `ping`

```
C:\> ping 198.133.219.25

Pinging 198.133.219.25 with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=30ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
```

```
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247

Ping statistics for 198.133.219.25:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
      Minimum = 20ms, Maximum = 30ms, Average = 22ms

C:\>
```

Дополнительная информация: использование команды `ping` совместно с DNS-именем устройства-получателя, успешное выполнение команды и коды ответов команды

Как показано в примере 19.2, команда **`ping`** также может быть использована с DNS-именем устройства-получателя (при условии наличия работающей службы DNS).

Пример 19.2. Использование команды `ping` с DNS-именем устройства-получателя

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

Pinging www.Cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=30ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247
Reply from 198.133.219.25: bytes=32 time=20ms TTL=247

Ping statistics for 198.133.219.25:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 20ms, Maximum = 30ms, Average = 22ms
C:\>
```

В приведенных выше примерах, выполненных на рабочей станции, команда **`ping`** порождает четыре эхо-запроса, на которые поступает четыре ответа, которые подтверждают наличие IP-соединения между двумя устройствами. Для маршрутизатора вывод на экран результата выполнения команды **`ping`** несколько отличается от выводимой этой командой информации для рабочей станции. В примере 19.3 показаны успешный и неудачный результаты выполнения команды **`ping`** для проверки соединения между маршрутизаторами А и Б (IP-адрес 192.168.100.100). Восклицательный знак (!) указывает на успешное выполнение команды, а точка (.) свидетельствует об отрицательном результате (пакет утерян). В табл. 19.2 приведены коды ответов, генерируемые при выполнении команды **`ping`** между устройствами Cisco.

Пример 19.3. Положительный и отрицательный результаты выполнения команды `ping` для маршрутизатора

```
RouterA# ping 192.168.100.100

Type escape sequence to abort.

Sending 5, 100byte ICMP Echoes to 192.168.100.100, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/36 ms

RouterA# ping 192.168.100.100

Type escape sequence to abort.
Sending 5, 100byte ICMP Echoes to 192.168.100.100, timeout is 2 seconds:
. . . . .
Success rate is 0 percent (0/5)
```

Таблица 19.2. Коды ответов от устройства корпорации Cisco для команды `ping`

Код	Значение	Возможные причины
!	Каждый восклицательный знак свидетельствует о получении эхо-ответа ICMP	Команда **`ping`** была успешно выполнена
.	Каждая точка указывает, что время таймера ожидания ответа сервером истекло	Это сообщение может свидетельствовать о наличии одной или нескольких из перечисленных ниже проблем: ■ выполнение команды **`ping`** было заблокировано списком доступа или брандмауэром; ■ у транзитного маршрутизатора не было пути к пункту назначения и он не смог отправить сообщение о недостижимости протокола ICMP; ■ на пути к получателю имеются проблемы физического соединения
U	Было получено сообщение о недостижимости протокола ICMP	У транзитного маршрутизатора нет маршрута к получателю
C	Было получено сообщение о подавлении отправителя (source quench) протокола ICMP	Устройство на маршруте (возможно, сам получатель) получает избыточное количество данных. В этом случае следует проверить его входные очереди
&	Было получено сообщение ICMP об истечении времени существования пакета	Возможно, в сети имеется кольцевой маршрут

Презентация: приложение `ping` протокола ICMP
В этой видеопрезентации проиллюстрирован процесс проверки связи между маршрутизаторами с помощью команды **`ping`**.

Обнаружение слишком длинных маршрутов

При осуществлении связи в сети могут возникать проблемы. Например, возможна ситуация, в которой дейтаграмма движется по замкнутому маршруту и не поступает к получателю. Возможна также другая ситуация, когда между отправителем и

получателем нет маршрута, что связано с ограничениями, налагаемыми протоколом маршрутизации. Первая из упомянутых ситуаций возникает, когда два маршрутизатора бесконечно пересылают дейтаграмму друг другу. В этом случае каждый маршрутизатор полагает, что второй маршрутизатор является следующим переходом на пути к пункту назначения. Возможной причиной этого может быть неверная информация о маршрутах. У протокола маршрутизации может также существовать ограничение на расстояние, которое пакету разрешается пройти по сети. Например, в протоколе RIP максимальное количество транзитных переходов равно 15-ти — это означает, что пакет может пройти только через 15 маршрутизаторов.

В каждой из таких ситуаций возникает недопустимо длинный маршрут. Независимо от того, имеется ли на маршруте петля или превышено максимально возможное количество переходов, пакет прекращает свое существование, поскольку в этом случае исчерпывается время его существования (Time-To-Live — TTL). Значение TTL обычно выражает максимально допустимое конкретным протоколом маршрутизации количество переходов. Параметр TTL задается каждой дейтаграмме и при каждой обработке дейтаграммы маршрутизатором уменьшается на единицу. Когда значение становится равным нулю, пакет отбрасывается. Для уведомления устройства-отправителя о том, что значение TTL было превышено, протокол ICMP использует сообщения об истечении времени существования пакета.

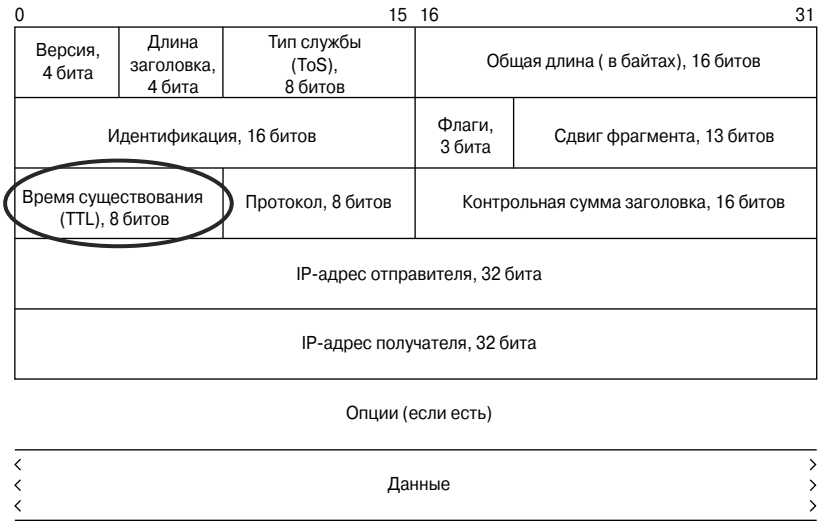


Рис. 19.6. Поле TTL в IP-пакете

Презентация: поле TTL протокола ICMP
В этой видеопрезентации проиллюстрирован механизм использования параметра TTL маршрутизаторами для определения того, когда следует отбросить пакет.

Эхо-сообщения

Как и все остальные типы пакетов, сообщения ICMP имеют специальные форматы. Каждое из приведенных в табл. 19.3 сообщений протокола ICMP имеет свои собственные уникальные характеристики. Однако все форматы сообщений ICMP начинаются со следующих трех полей:

- поля типа (Type);
- поля кода (Code);
- поля контрольной суммы (Checksum).

Поле типа указывает тип отправляемого ICMP-сообщения. Поле кода включает в себя дополнительную информацию, связанную с типом сообщения. Поле контрольной суммы, как и в других типах пакетов, используется для проверки целостности данных после передачи.

Таблица 19.3. Типы сообщений протокола ICMP

Номер сообщения ICMP	Тип сообщения
0	Эхо-ответ
3	Пункт назначения недостижим
4	Сообщение о подавлении отправителя (source quench)
5	Запрос перенаправления/изменения
8	Эхо-запрос
9	Анонс маршрутизатора
10	Выбор маршрутизатора
11	Истекло время существования пакета
12	Ошибочные параметры
13	Запрос текущей временной метки (timestamp)
14	Ответ на запрос текущей временной метки
15	Запрос информации
16	Ответ на запрос информации
17	Запрос маски адреса
18	Ответ на запрос маски адреса

На рис. 19.7 показан формат сообщений эхо-запроса и эхо-ответа. Для каждого типа сообщения приведены соответствующие номера типа и кода. Поля идентификатора (Identifier) и последовательного номера (Sequence Number) для сообщений эхо-запроса и эхо-ответа являются уникальными. Они используются для установления соответствия между эхо-запросом и эхо-ответом. Поле данных содержит необязательную дополнительную информацию, которая может быть частью эхо-запроса или эхо-ответа.

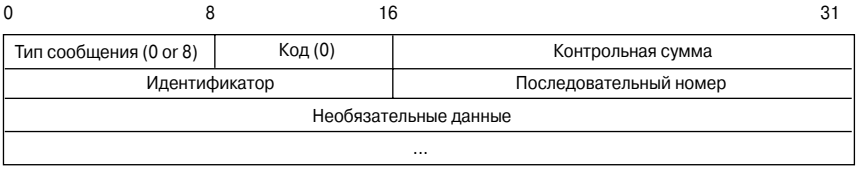


Рис. 19.7. Формат сообщений эхо-запроса и эхо-ответа

Сообщение о недостижимости получателя

На рис. 19.8 показано, что дейтаграммы не всегда могут быть отправлены получателю. Причинами невозможности доставить данные могут быть неисправности аппаратного обеспечения, неправильно сконфигурированный протокол, отказ интерфейса или неверная информация маршрутизации. В этом случае протокол ICMP пересылает отправителю дейтаграммы сообщение о недостижимости пункта назначения, которое указывает на то, что доставка невозможна.

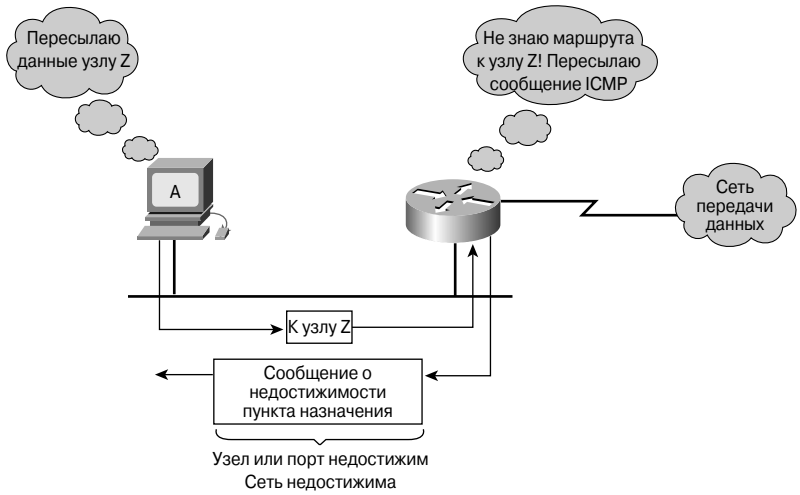


Рис. 19.8. Отправка ICMP-сообщения о недостижимости узла

На рис. 19.9 показан заголовок сообщения ICMP о недостижимости пункта назначения. Значение “3” в поле типа указывает на то, что это сообщение о недостижимости получателя. Значение кода указывает причину, по которой пакет не мог быть доставлен. Код в данном случае равен нулю, что указывает на недостижимость сети. В табл. 19.4 приведены возможные значения поля кода и их описание.

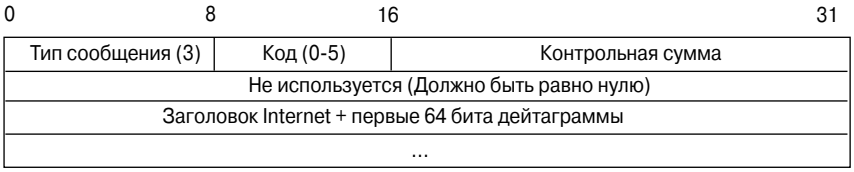


Рис. 19.9. Формат ICMP-сообщения о недостижимости получателя

Таблица 19.4. Значения поля кода и их описание

Значение поля кода	Описание
0	Сеть недостижима
1	Узел недостижим
2	Протокол не поддерживается
3	Порт недостижим
4	Требуется фрагментация, бит DF установлен
5	Маршрут отправителя недействителен
6	Сеть получателя неизвестна
7	Узел получателя неизвестен
8	Узел отправителя изолирован
9	Связь с сетью передачи данных административно запрещена
10	Связь с узлом передачи данных административно запрещена
11	Для данного типа службы сеть недостижима
12	Для данного типа службы узел недостижим

Сообщение о недостижимости также может быть отправлено в том случае, когда для пересылки пакета требуется его фрагментация. Обычно фрагментация необходима при пересылке дейтаграммы из сети технологии Token Ring в сеть Ethernet. Если дейтаграмма не допускает фрагментации, то пакет не может быть направлен далее. Вследствие такой ситуации пересылается сообщение о недостижимости. Это сообщение может быть также сгенерировано в том случае, если недоступны связанные с протоколом IP службы, такие, как протокол FTP и Web-службы. Для устранения сбоев и ошибок в IP-сети необходимо правильно понимать возможные причины получения сообщений о недостижимости.

Презентация: сообщение о недостижимости получателя протокола ICMP
В этой видеопрезентации проиллюстрирован механизм рассылки сообщений о недостижимости получателя в протоколе ICMP.

Другие типы сообщений об ошибках

Устройства, обрабатывающие дейтаграммы, могут оказаться неспособными переслать дейтаграмму из-за ошибки в ее заголовке. Хотя такой тип ошибки не связан

с состоянием сети-получателя или узла-получателя, все же такая дейтаграмма не может быть обработана и доставлена по назначению. В этом случае отправителю дейтаграммы посылается сообщение протокола ICMP типа 12 о наличии проблемы с параметром. На рис. 19.10 показан заголовок сообщения о проблеме с параметром. Заголовок такого сообщения содержит поле указателя (Pointer). Если поле кода содержит значение 0, то поле указателя сообщает о номере октета дейтаграммы, вызвавшего ошибку.

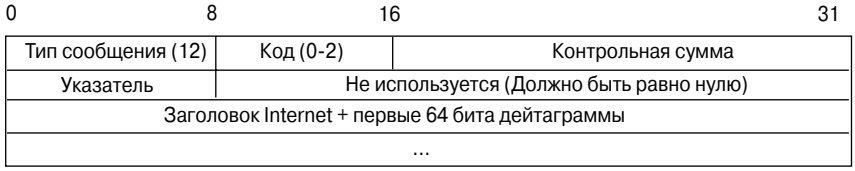


Рис. 19.10. Формат сообщения о проблеме с параметром

Обзор управляющих сообщений стека протоколов TCP/IP

Протокол ICMP (Internet Control Message Protocol — протокол управляющих сообщений в сети Internet) является неотъемлемой частью стека протоколов TCP/IP. Все реализации протокола IP должны включать в себя средства ICMP. Предпосылки такого строгого требования просты. Прежде всего, поскольку протокол IP не гарантирует доставку данных, он не содержит методов, которые позволяют уведомлять сетевые узлы о происходящих ошибках. В самом протоколе IP нет также встроенных методов пересылки информационных или управляющих сообщений сетевым узлам. Здесь на помощь приходит протокол ICMP, который выполняет всю "черную" работу по рассылке служебной информации для протокола IP.

Введение в управляющие сообщения

В отличие от сообщений об ошибках, управляющие сообщения не являются следствием потери пакетов или ошибок при их передаче. Эти сообщения информируют узлы сети о таких событиях, как затор в сети или наличие более предпочтительного шлюза к удаленной сети. Как и все сообщения протокола ICMP, управляющие сообщения инкапсулируются в IP-дейтаграммы. Протокол ICMP использует эти дейтаграммы для передачи сообщений через несколько сетей.

Протокол ICMP использует несколько типов управляющих сообщений; в табл. 19.3 приведены некоторые типичные управляющие сообщения. Часть этих сообщений обсуждается в следующих разделах.

Запросы протокола ICMP о перенаправлении пакета/изменении маршрута

Типичным управляющим сообщением протокола ICMP является запрос о перенаправлении пакета/изменении маршрута. Этот тип сообщения может быть инициирован только шлюзом (маршрутизатором). Для всех устройств, которые осуществляют связь с несколькими IP-сетями, должен быть сконфигурирован стандартный шлюз. Под стандартным шлюзом понимается адрес порта маршрутизатора, который подключен к той же сети, в которой находится данное устройство. На рис. 19.11 показано устройство, подсоединенное к маршрутизатору, который имеет доступ к Internet.

После того как узел А был сконфигурирован с IP-адресом Fa 0/0 в качестве стандартного шлюза, он использует этот IP-адрес для достижения любой сети, к которой не подсоединен непосредственно. Как правило, узел А подсоединяется только к одному шлюзу. Однако в некоторых случаях узел подсоединяется к сегменту, который имеет два или более непосредственно подсоединенных маршрутизатора. В таком случае стандартному шлюзу узла может потребоваться использование запроса о перенаправлении/изменении, для того чтобы сообщить узлу наилучший маршрут к определенной сети.

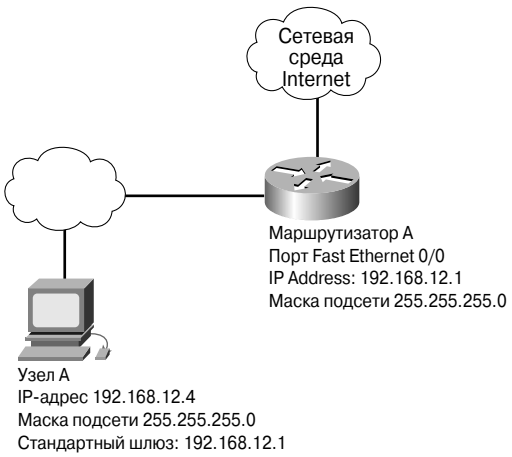


Рис. 19.11. Запрос на перенаправление

Стандартные шлюзы пересылают запрос протокола ICMP о перенаправлении/изменении маршрута только в том случае, если выполнены приведенные ниже условия.

- Интерфейс, через который пакет поступает в маршрутизатор, совпадает с тем, с которого пакет пересылается после маршрутизации.
- Сеть или подсеть, к которой относится IP-адрес отправителя, совпадает с сетью или подсетью, которой соответствует IP-адрес следующего транзитного перехода пакета после маршрутизации.

- Дейтаграмма маршрутизируется не от отправителя (т.е. не маршрутизируется от той точки, в которой были сформированы данные).
- Маршрут перенаправления не является другим маршрутом перенаправления протокола ICMP или стандартным маршрутом.
- Маршрутизатор сконфигурирован для отправки запросов о перенаправлении. Стандартно маршрутизаторы Cisco обладают способностью отправлять запросы ICMP о перенаправлении. Для отключения перенаправлений протокола ICMP используется подкоманда интерфейса **`no ip redirects`**.

Для запроса о перенаправлении/изменении маршрута используется формат, показанный на рис. 19.12. Код типа сообщения для такого запроса равен пяти. Кроме того, значения кода запроса могут быть равными нулю, единице, двум или трем. Смысл этих значений кодов и соответствующие действия приведены в табл. 19.5.

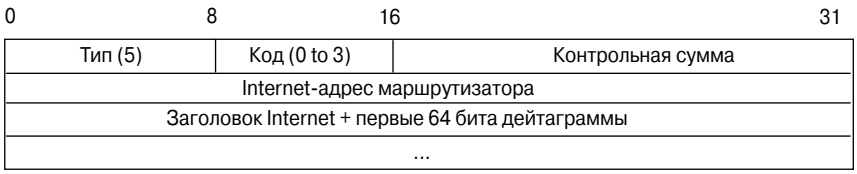


Рис. 19.12. Формат сообщения запроса о перенаправлении

Таблица 19.5. Значения кодов и соответствующие действия

Значение кода	Действие
0	Перенаправить дейтаграммы конкретной сети
1	Перенаправить дейтаграммы конкретному узлу
2	Перенаправить дейтаграммы для конкретного типа службы и сети
3	Перенаправить дейтаграммы для конкретного типа службы и узла

Получатель запроса о перенаправлении должен использовать Internet-адрес шлюза, указанный в сообщении протокола ICMP о перенаправлении, в качестве IP-адреса маршрутизатора при пересылке пакетов в конкретную сеть. В примере, показанном на рис. 19.10, сообщение протокола ICMP о перенаправлении посылается маршрутизатором А узлу Б и содержит Internet-адрес шлюза 192.168.12.2, который является IP-адресом маршрутизатора Б.

Синхронизация текущего времени и оценка времени транзитного перехода

Стек протоколов TCP/IP позволяет системам осуществлять связь друг с другом на больших расстояниях через многие транзитные сети. Однако в каждой отдельной сети временная синхронизация осуществляется индивидуальным способом. Такая ситуация может вызвать проблемы в том случае, если узлы, находящиеся в разных

сетях, пытаются осуществить связь, используя программное обеспечение, требующее синхронизации времени. Для того чтобы решить эту проблему, в протоколе ICMP используются сообщения особого типа, содержащие информацию о текущем времени.

Сообщения о текущем времени позволяют одному узлу запросить у другого удаленного узла временную метку. Отвечая на такой запрос, удаленный узел посылает ответное сообщение протокола ICMP со значением текущего времени. На рис. 19.13 показан формат запроса текущего времени и ответа на него.

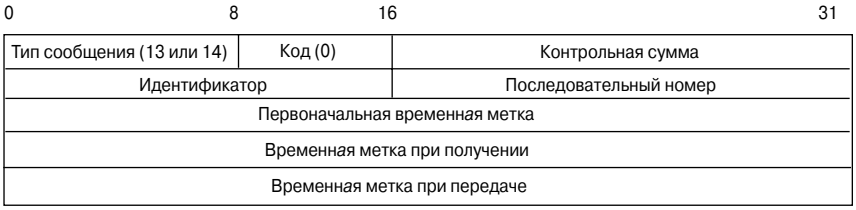


Рис. 19.13. Запрос текущего времени

Поле типа (Type) в сообщении запроса текущего времени ICMP может быть равно 13-ти для текущего времени или 14-ти — для ответа на этот запрос. Значение поля кода (Code) всегда устанавливается равным нулю, поскольку другие дополнительные параметры отсутствуют. В запросе текущего времени содержится начальное значение текущего времени (originate timestamp), которое указывает время на запрашивающем узле непосредственно перед отправкой запроса. Временем получения (receive timestamp) является текущее время узла-получателя в момент получения им запроса. Время передачи (transmit timestamp) вставляется в сообщение ответа на запрос непосредственно перед его отправкой. Время отправки запроса, время его получения и время передачи выражаются в микросекундах и отсчитываются от полуночи по всеобщему времени (Universal Time — UT).

Все ответные сообщения протокола ICMP на запрос текущего времени содержат первоначальное время отправки, время получения и время передачи. Используя три указанных значения, узел, инициировавший запрос, может оценить время прохождения пакета по сети, вычитая первоначальное время из времени передачи. Однако такая оценка будет всего лишь приблизительным результатом, поскольку истинное транзитное время может изменяться в широких пределах, в зависимости от интенсивности передачи данных в сети и возможных заторов. Используя три временны*е* метки, узел, пославший запрос ICMP о текущем времени, может также оценить локальное время на удаленном компьютере.

Сообщения ICMP с временно*й* меткой предоставляют простой способ оценки локального времени на удаленном узле и позволяют установить время транзитного прохождения пакета по сети. Однако такой механизм не является наилучшим способом получения информации. Вместо него протоколы стека TCP/IP более высоких уровней, такие, как синхронизирующий сетевой протокол (Network Time Protocol — NTP), могут выполнить синхронизацию времени более надежным способом.

Форматы информационных запросов и ответных сообщений

Информационные запросы протокола ICMP и соответствующие ответные сообщения первоначально были предназначены для того, чтобы узел мог определить номер сети, в которой он находится. На рис. 19.14 показаны форматы информационных запросов и ответных сообщений.

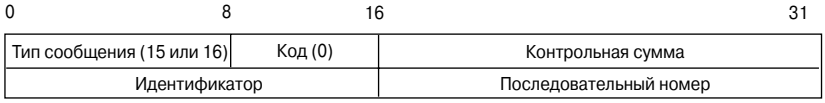


Рис. 19.14. Формат информационных запросов и ответных сообщений

В таком сообщении могут использоваться два кода типа. Код типа, равный 15-ти, указывает на то, что это сообщение информационного запроса. Код типа, равный 16-ти, соответствует ответному информационному сообщению. Этот тип сообщений протокола ICMP в настоящее время считается устаревшим. Сейчас для определения узлами номера сети, к которой они подсоединены, используются такие протоколы, как BOOTP и протокол динамического конфигурирования узла (Dynamic Host Configuration Protocol — DHCP).

Запрос маски адреса

Когда сетевой администратор осуществляет разбиение крупной сети на несколько подсетей, создается новая маска подсети. Эта маска необходима для выделения из IP-адреса порций битов, определяющих номера сети, подсети и узла. Если узлу неизвестна маски подсети, он может послать запрос о маске адреса локальному маршрутизатору. Если адрес такого маршрутизатора известен, запрос может быть отправлен как *одноадресатное сообщение*. Если же он неизвестен, запрос посылается как *широковещательное сообщение*. При получении такого сообщения маршрутизатор отправляет ответное сообщение, в котором содержится маска адреса. Этот ответ с маской адреса идентифицирует требуемую маску подсети. Например, предположим, что узел расположен в сети класса B и имеет IP-адрес 172.16.5.3. Поскольку этому узлу неизвестна маска подсети, он рассылает широковещательное сообщение с запросом маски адреса.

```
Source address          172.16.5.3
Destination address     255.255.255.255
Protocol                ICMP = 1
Type                    Address Mask Request = AM1
Code                    0
Mask                    0
```

Этот широковещательный запрос получает локальный маршрутизатор, имеющий IP-адрес 172.16.5.1, и отправляет ответное сообщение с маской адреса:

```
Source address          172.16.5.1
Destination address       172.16.5.3
```

```
Protocol                ICMP = 1
Type                    Address Mask Reply = AM2
Code                    0
Mask                    255.255.255.0
```

На рис. 19.15 показан формат фрейма для запроса маски адреса. В табл. 19.6 перечислены типы сообщений ICMP для запроса маски адреса. Следует обратить внимание, что для сообщения-запроса и для сообщения-ответа используется один и тот же формат. Однако тип 17 сообщения предназначен только для запроса, а тип 18 — только для ответа на запрос.

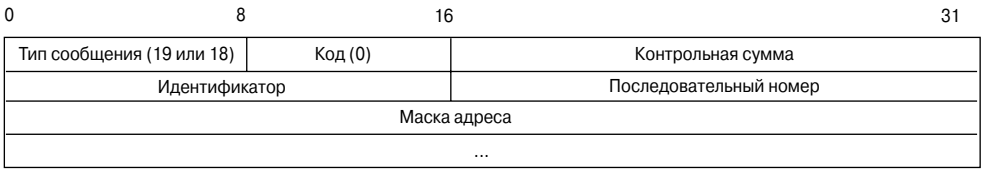


Рис. 19.15. Запрос маски адреса

Таблица 19.6. Сообщения запроса маски протокола ICMP

Поле сообщения ICMP	Описание
Тип 17	Сообщение запроса маски адреса
Тип 18	Ответ на запрос маски адреса
Код 0	Сообщение запроса маски адреса
Код 0	Ответ на запрос маски адреса
Контрольная сумма	Для вычисления контрольной суммы ее поле должно быть равно нулю. В будущем контрольная сумма может быть заменена другим полем
Идентификатор	Идентификатор, который помогает устанавливать соответствие между запросами и ответами. Он может быть равен нулю
Последовательный номер	Последовательный номер используется для установки соответствия между запросами и ответами на них. Он может быть равен нулю
Маска адреса	32-битовая маска. Шлюз, получивший запрос маски адреса, должен ответить на него, указав в поле маски адреса (Address Mask field) 32-битовую маску, биты которой указывают подсеть и сеть для подсети, из которой этот запрос был получен. Если переславший запрос узел не знает свой собственный IP-адрес, он может оставить в поле отправителя значение 0; в этом случае ответ должен быть широковещательным. Однако такого подхода следует избегать, а по возможности вообще исключать, поскольку он увеличивает ненужную широковещательную нагрузку на сеть. Даже в том случае, когда ответы имеют широковещательный характер, нет необходимости устанавливать соответствие между запросами и ответами на них, поскольку для подсети возможна только одна маска. Поля идентификатора и последовательного номера могут быть проигнорированы. Тип сообщения AM1 может быть получен от шлюза или от узла. Тип AM2 может быть получен от шлюза или от узла, выполняющего функции шлюза

Сообщения об обнаружении маршрутизатора

Если для какого-либо узла не был сконфигурирован стандартный шлюз, он может получить информацию о доступных маршрутизаторах в процессе обнаружения маршрутизаторов. Такой процесс начинается с рассылки узлом всем маршрутизаторам сообщения, в котором используется *многоадресатный адрес* (*multicast*), о поиске маршрутизатора, с использованием специальной многоадресатной группы с адресом 224.0.0.2. На рис. 19.16 показан формат сообщения ICMP о поиске маршрутизатора. Это сообщение может быть также разослано широковещательно для того, чтобы найти и те маршрутизаторы, на которых многоадресатная рассылка не сконфигурирована. В документе RFC 1812 указано, что маршрутизаторы должны поддерживать процесс обнаружения маршрутизаторов для всех сетей, с которыми они непосредственно соединены. Однако такое утверждение не всегда справедливо. Если сообщение поиска маршрутизатора будет отправлено маршрутизатору, который не поддерживает процесс обнаружения маршрутизаторов, то ответа на такое сообщение не последует.

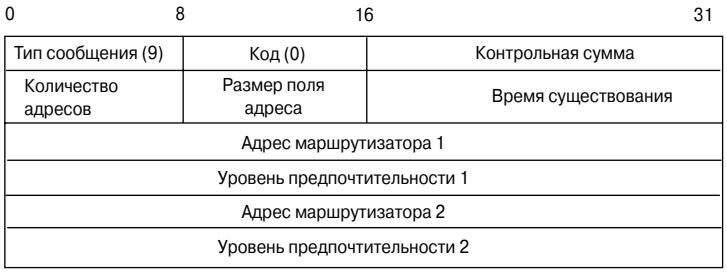


Рис. 19.16. Сообщение об обнаружении маршрутизатора

Если же такое сообщение получит маршрутизатор, который поддерживает требуемый процесс, он отправит ответное сообщение об анонсировании маршрутизатора. В табл. 19.7 описаны все поля формата фрейма.

Таблица 19.7. Формат фрейма анонсов маршрутизатора

Поле фрейма ICMP	Описание
Тип	9
Тип	0
Контрольная сумма	Для вычисления контрольной суммы ее поле должно быть равно нулю
Количество адресов	Количество адресов маршрутизаторов, анонсируемых в данном сообщении
Размер адресной записи	Количество 32-битовых слов, содержащих информацию об адресах маршрутизаторов (в описываемой версии протокола это значение равно двум)
Время существования	Максимальное время (в секундах), в течение которого адреса маршрутизаторов считаются действительными

Окончание табл. 19.7

Поле фрейма ICMP	Описание
Адреса маршрутизаторов	IP-адрес(а) маршрутизатора, посылающего сообщение. Номер интерфейса, с которого отсылается сообщение
Уровень приоритета	Предпочтительность адреса каждого маршрутизатора.
	Предпочтительность или приоритет данного адреса маршрутизатора в качестве стандартного по отношению к адресам других маршрутизаторов этой же подсети. Число со знаком и двумя дополнениями; чем больше это значение, тем предпочтительнее маршрутизатор

Сообщение о поиске маршрутизатора

Сообщение ICMP о поиске маршрутизатора генерируется узлом как реакция на отсутствие стандартного шлюза. Это сообщение рассылается методом многоадресатной рассылки. Отправка сообщения является первым этапом в процессе обнаружения маршрутизатора. Локальный маршрутизатор отвечает сообщением-анонсом маршрутизатора, в котором указывается стандартный шлюз для этого локального узла. На рис. 19.17 показан формат соответствующего фрейма, а в табл. 19.8 описаны значения каждого поля.

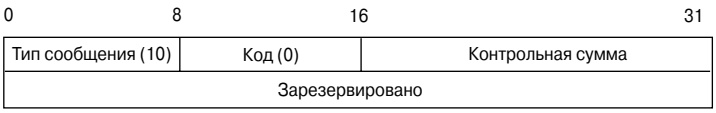


Рис. 19.17. Сообщение о поиске маршрутизатора

Таблица 19.8. Описание полей фрейма сообщения о поиске маршрутизатора

Поле ICMP	Описание
Тип	10
Код	0
Контрольная сумма	Шестнадцатибитовое дополнение единицами полей ICMP-сообщения, начиная с поля типа сообщения ICMP. Для вычисления контрольной суммы ее поле должно быть равно нулю
Зарезервировано	Посылается как 0; при получении это поле игнорируется

Сообщения о переполнении и управление потоком данных

Если сразу несколько компьютеров пытаются получить доступ к одному и тому же получателю, то такой получатель может быть переполнен поступающими данными. Состояние переполнения или, как говорят, затора может также возникнуть в том случае, когда высокоскоростная локальная сеть LAN начинает передавать данные в низкоскоростное соединение распределенной сети WAN. Затор в сети или у получателя

приводит к отбрасыванию и, следовательно, к потере данных. Для уменьшения количества потерянных данных необходимо направить отправителю данных, вызвавших переполнение, соответствующее сообщение ICMP. Такой тип сообщения ICMP называется *сообщением о подавлении отправителя (source quench message)*. Это сообщение уведомляет отправителя данных о возникшем переполнении и предлагает ему уменьшить скорость передачи пакетов. В большинстве случаев затор вскоре исчезает. После этого при отсутствии повторных сообщений о переполнении источник постепенно повышает скорость передачи. Стандартно большинство маршрутизаторов Cisco не рассылают сообщения о подавлении отправителя. Такая установка объясняется тем, что сами сообщения о заторе могут усугубить состояние переполнения.

Сообщение о подавлении отправителя может эффективно использоваться в малых/домашних офисах (Small Office, Home Office — SOHO). В таком офисе, например, может быть сеть из четырех компьютеров, соединенных с помощью кабеля 5-й категории и подключенных к разделяемому доступу к среде Internet (Internet Connection Sharing — ICS) через общий модем со скоростью передачи 56 Кбит/с. Очевидно, что передаваемые по LAN-сети этого офиса со скоростью 10 Мбит/с данные легко могут поглотить полосу пропускания 56 Кбит/с канала распределенной сети. Такая ситуация может привести к потере данных и необходимости повторной их передачи. При использовании сообщений протокола ICMP узел, выступающий в схеме ICS в роли шлюза, может предложить другим рабочим станциям снизить скорость передачи до приемлемого уровня. Такое снижение скорости передачи предотвратит постоянную потерю данных.

Резюме

В этой главе были рассмотрены следующие ключевые темы:

- протокол IP является методом негарантированной доставки, который использует сообщения протокола ICMP для уведомления отправителя о том, что данные не были доставлены получателю;
- сообщения эхо-запросов и эхо-ответов позволяют сетевому администратору протестировать соединения протокола IP для обнаружения ошибок конфигурирования и сбоев в сети;
- сообщения протокола ICMP передаются с использованием протокола IP, поэтому их доставка также не гарантирована;
- пакеты протокола ICMP содержат в заголовке пакета свою собственную специальную информацию, которая начинается с полей типа сообщения (Type field) и кода (Code field);
- существуют следующие разновидности управляющих сообщений протокола ICMP:
  - сообщения протокола ICMP о запросе перенаправления или изменения;
  - сообщения протокола ICMP о временной синхронизации и оценке времени транзитного прохождения пакета;

- сообщения информационных запросов протокола ICMP и ответов на них;
- сообщения запросов маски адреса и ответы на них;
- сообщения об обнаружении маршрутизатором протокола ICMP;
- сообщения о поиске маршрутизатором протокола ICMP;
- сообщения ICMP о переполнении и сообщения управления потоком.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Ключевые термины

ping (Packet Internet Groper — запросчик сети Internet) — команда, используемая для отправки эхо-запроса протокола ICMP и получения на него ответа. Часто используется в IP-сетях для проверки достижимости сетевого устройства.

Дейтаграмма (datagram) — в IP-сетях так часто называют пакеты.

Одноадресатная рассылка (unicast) представляет собой сообщение, отправляемое одному сетевому получателю.

Пакеты многоадресатной рассылки (multicast) — это пакеты, которые копируются в сети и рассылаются по заданному набору сетевых адресов.

Протокол управляющих сообщений сети Internet (Internet Control Message Protocol — ICMP) представляет собой Internet-протокол сетевого уровня, сообщающий об ошибках и предоставляющий другую информацию относительно обработки IP-пакетов. Описан в документе RFC 792.

Стек протоколов TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/протокол сети Internet) — общее название для стека протоколов, разработанного министерством обороны США в 70-х годах XX в. для использования в охватывающих весь мир объединенных сетях. Наиболее известными протоколами этого стека являются протоколы TCP и IP.

Широковещательные пакеты (broadcast) — это пакеты данных, рассылаемые всем узлам сети.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Справедливо ли утверждение: протокол ICMP является протоколом сообщений об ошибках стека протоколов IP?

   а) Справедливо.

   б) Несправедливо.

2. Что означает аббревиатура ICMP?

   а) Протокол внутренних управляющих сообщений (Internal Control Message Protocol).

   б) Портал управляющих сообщений сети Internet (Internet Control Message Portal).

   в) Протокол передачи содержимого (Internal Content Message Protocol).

   г) Протокол управляющих сообщений в сети Internet (Internet Control Message Protocol).

3. Справедливо ли утверждение: сообщения протокола ICMP инкапсулируются в дейтаграммы таким же образом, как и все другие данные, передаваемые с помощью протокола IP?

   а) Справедливо.

   б) Несправедливо.

4. Справедливо ли утверждение: если дейтаграммы требуется передать за пределы локальной сети, то должен быть сконфигурирован стандартный шлюз?

   а) Справедливо.

   б) Несправедливо.

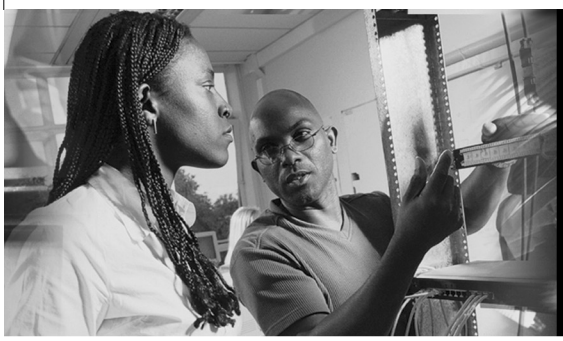
5. Что означает аббревиатура TTL?

   а) Время перечисления (Time-To-List).

   б) Время существования (Time-To-Live).

   в) Существование терминала (Terminal-To-Live).

   г) Перечисление терминалов (Terminal-To-List).



ГЛАВА 20
Поиск и устранение неисправностей в маршрутизаторах

В этой главе...

- описаны методы базового тестирования сети;
- рассмотрены некоторые методы проверки таблиц маршрутизации;
- описано применение команды **`ping`** для проведения базового тестирования связи между узлами сети;
- описано применение команды telnet для проверки программного обеспечения уровня приложений между узлом-отправителем и узлом-получателем;
- описан порядок поиска и устранения неисправностей путем тестирования по уровням модели OSI;
- описано применение команды **`show interfaces`** для поиска проблем первого и второго уровней;
- описано применение команд **`show ip route`** и **`show ip protocol`** для определения параметров маршрутизации;
- описано применение команды **`show cdp`** для проверки наличия связи между узлами на втором уровне;
- описано применение команды **`traceroute`** для определения пути пакета при прохождении между сетями;
- описано применение команды **`show controller serial`** для проверки подключения соответствующего типа кабеля;
- описано применение основных команд отладки **`debug`** для отображения работы маршрутизатора.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

карта сетевого интерфейса, с. 883,
ping, с. 884,
telnet, с. 887,
тестовые пакеты, с. 889,
traceroute, с. 893.

В этой главе приводится обзор тестовых процедур для проверки сети. Основное внимание уделено необходимости структурного подхода к поиску и устранению неисправностей. В ней также описан процесс поиска и устранения основных неисправностей маршрутизаторов.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Проверка таблицы маршрутизации

Маршрутизатор узнает о маршрутах к сетям-получателям, используя протокол динамической маршрутизации. Он может также узнать маршруты, если они сконфигурированы сетевым администратором. Часто для получения информации о маршрутах маршрутизатор использует сочетание динамической и статической маршрутизации. Независимо от того, каким образом маршрутизатору становится известен наилучший маршрут к получателю, он заносит этот маршрут в таблицу маршрутизации. В этом разделе описаны методы исследования и интерпретации содержимого таблицы маршрутизации. Ниже подробно рассмотрены следующие вопросы:

- использование команды **`show ip route`**;
- определение стандартного шлюза (так называемого шлюза последней надежды — gateway of last resort);
- определение источника маршрута и адреса получателя;
- определение административного расстояния маршрута;
- определение метрики маршрута;
- определение следующего транзитного перехода на маршруте;
- определение последних обновлений маршрута;
- использование нескольких эквивалентных маршрутов к пункту назначения.

Использование команды show ip route

Одной из первичных функций маршрутизатора является определение наилучшего маршрута к получателю. Маршрутизатор узнает о путях к получателю, также называемых маршрутами, из конфигурации, заданной администратором, или от других маршрутизаторов при помощи протоколов маршрутизации. Маршрутизаторы сохраняют информацию о маршрутах в таблицах маршрутизации, находящихся в их оперативной памяти (Random-Access Memory — RAM). Таблицы маршрутизации содержат список наилучших доступных маршрутов, используемых маршрутизаторами для принятия решений о пересылке пакетов.

Команда **`show ip route`** отображает содержимое таблицы IP-маршрутизации. В этой таблице содержатся ссылки на все известные сети и подсети, а также коды,

указывающие, каким способом была получена эта информация. С командой **show ip route** могут быть использованы следующие параметры:

- параметр **connected** используется для отображения таблицы непосредственно подсоединенных к конкретному маршрутизатору сетей;
- при использовании параметра **network** отображается подробная информация маршрутизации для конкретной сети;
- параметр **rip** используется для отображения информации таблицы маршрутизации протокола RIP для конкретного маршрутизатора;
- параметр **igrp** используется для отображения информации таблицы маршрутизации протокола IGRP в конкретном маршрутизаторе;
- параметр **static** используется для отображения статической информации таблицы маршрутизации в маршрутизаторе.

Таблица маршрутизации устанавливает логическое соответствие между префиксом сети и выходным интерфейсом. Когда маршрутизатор получает пакет, предназначенный для сети 192.168.4.46, он ищет в своей таблице маршрутизации префикс 192.168.4.0/24. После этого на основе соответствующей позиции таблицы устройство пересылает пакет на выходной интерфейс (Ethernet0). Если маршрутизатор получает пакет, предназначенный для сети 10.3.21.5, он пересылает его на интерфейс Serial 0/0.

Кроме того, рассматриваемый маршрутизатор отбрасывает все пакеты, предназначенные для сетей, отсутствующих в его таблице маршрутизации. Для пересылки пакетов в другие пункты назначения таблица маршрутизации узла должна содержать больше маршрутов. Новые маршруты могут быть добавлены в таблицу двумя способами:

- посредством **статической маршрутизации** (**Static routing**). Сетевой администратор вручную задает маршруты к одной или более сетям-получателям;
- посредством **динамической маршрутизации** (**Dynamic routing**). Для обмена информацией о маршрутах и самостоятельного выбора наилучшего маршрута маршрутизаторы выполняют действия, требуемые используемым протоколом маршрутизации.

Задаваемые администратором маршруты называются *статическими (static)*, поскольку они не изменяются до тех пор, пока не будут вручную перепрограммированы сетевым администратором. Маршруты, полученные от других маршрутизаторов, называются *динамическими (dynamic)*, поскольку они автоматически изменяются при получении от соседних маршрутизаторов сообщений об обновлении маршрутов, содержащих новую информацию. Каждый из описанных выше методов имеет присущие ему достоинства и недостатки.

Практическое задание 20.1.1. Проверка таблицы маршрутизации с помощью команды `show ip route`

В этой лабораторной работе следует сконфигурировать протоколы маршрутизации RIP и IGRP и исследовать с помощью команды **`show ip route`** влияние на таблицу маршрутизации двух протоколов.

Презентация: таблица маршрутизации

В этой презентации подробно проиллюстрирован процесс построения таблицы маршрутизации маршрутизатором.

Указание стандартного шлюза

Нерационально и даже нежелательно, чтобы маршрутизатор владел информацией обо всех возможных пунктах назначения. Вместо этого в маршрутизаторе задается стандартный маршрут, называемый также шлюзом последней надежды (gateway of last resort). Стандартный маршрут используется маршрутизатором в том случае, когда он не может найти в своей таблице маршрутизации запись, соответствующую конкретной сети-получателю. Этот стандартный маршрут используется для передачи пакета другому маршрутизатору, называемому шлюзом последней надежды, в надежде, что последний сможет переслать пакет в требуемом направлении.

Основным достоинством стандартного маршрута является масштабируемость, что позволяет поддерживать таблицы маршрутизации минимального размера. Маршруты подобного типа позволяют маршрутизаторам пересылать пакеты, предназначенные произвольному узлу сети Internet, без необходимости поддерживать запись в таблице маршрутизации для каждой сети, входящей в сеть Internet. Во многих случаях стандартный маршрут указывает на сеть Internet-провайдера. Стандартные маршруты могут статически вводиться администратором или устанавливаться динамически посредством какого-либо протокола маршрутизации.

Установка стандартного маршрута производится администратором. До того, как маршрутизаторы смогут динамически обмениваться информацией о маршрутах, администратор должен сконфигурировать стандартный маршрут хотя бы на одном устройстве. Для конфигурирования статического стандартного маршрута администратор может использовать одну из двух приведенных ниже команд:

`ip route 0.0.0.0 0.0.0.0` или

`ip default-network`.

Команда **`ip default-network`** устанавливает стандартный маршрут в сетях, использующих динамические протоколы маршрутизации. Она применяется в протоколах маршрутизации IGRP и EIGRP для указания и распространения по сети стандартного маршрута-кандидата[1].

[1] *Такое название подчеркивает тот факт, что при использовании указанных протоколов в сети может быть несколько стандартных маршрутов, из которых будет выбран наилучший. — Прим. ред.*

Команда глобального конфигурирования **ip default-network 195.16.11.0** задает сеть класса C с адресом 195.16.11.0 в качестве пункта назначения пакетов, для которых в таблице маршрутизации отсутствует соответствующая запись. Когда у маршрутизатора имеется маршрут к каждой сети, указанной в команде **ip default-network**, он помечается флагом кандидата в стандартные маршруты. Конфигурация с использованием рассматриваемой команды предполагает рассылку посредством протокола маршрутизации, что следует использовать указанную сеть в качестве получателя в том случае, если точное соответствие в таблице маршрутизации не найдено. Следует помнить, что маршрутизатор, на сеть которого указывает рассматриваемая команда, также должен "знать" маршруты к искомой сети-получателю или содержать в своей конфигурации явно указанный с помощью команды **ip route 0.0.0.0 0.0.0.0** маршрут к следующему стандартному шлюзу.

Альтернативным способом конфигурирования стандартного маршрута является использование команды **ip route 0.0.0.0 0.0.0.0**.

```
Router(config)# ip route 0.0.0.0 0.0.0.0
[next-hop-ip-address | exit-interface]
```

После конфигурирования стандартного маршрута или сети выполнение команды **show ip route** приводит к следующему результату:

```
Gateway of last resort is 172.16.1.2 to network 0.0.0.0
```

Если маршрутизатор не находит требуемой сети в таблице маршрутизации, он отправляет пакет узлу 172.16.1.2.

Практическое задание 20.1.2. Стандартный шлюз
В этой лабораторной работе следует сконфигурировать протокол маршрутизации RIP и добавить в конфигурацию стандартные шлюзы (маршруты или сети). Далее следует убрать протокол RIP и сконфигурировать стандартные маршруты для протокола маршрутизации IGRP

Определение маршрута от сети-отправителя к сети-получателю

Для потоков данных, проходящих по сетевой среде, определение маршрута происходит на сетевом уровне. Функция определения наилучшего маршрута позволяет маршрутизатору оценить возможные пути к пункту назначения и выбрать предпочтительный способ обработки пакета. При оценке различных маршрутов службы маршрутизации используют информацию о топологии сети. Эта информация может быть сконфигурирована сетевым администратором или собрана в процессе динамической маршрутизации, происходящем в работающей сети.

Сетевой уровень обеспечивает негарантированную сквозную доставку пакетов через объединенную сеть. Для пересылки пакетов из сети-отправителя сети-получателю сетевой уровень использует таблицу маршрутизации протокола IP. После определения используемого маршрута маршрутизатор передает пакет с одного своего

интерфейса на другой или в порт, который соответствует наилучшему маршруту к пункту назначения пакета.

Использование адресов второго и третьего уровней при передаче пакета от отправителя получателю

В то время как для доставки пакета от отправителя получателю используются адреса сетевого (третьего) уровня, также известные как IP-адреса, важно понимать, что для передачи пакетов между маршрутизаторами используется иной тип адресов. Для того чтобы доставить пакет от отправителя получателю, используются адреса как второго, так и третьего уровня.

Адрес третьего уровня служит для передачи пакета от сети-отправителя сети-получателю. В процессе передачи пакета содержащиеся в нем IP-адреса отправителя и получателя остаются неизменными. Однако MAC-адрес (адрес второго уровня) изменяется на каждом переходе или маршрутизаторе. Использование адреса канального уровня необходимо потому, что узел-отправитель должен иметь возможность адресации маршрутизатора следующего перехода, которому будет пересылаться пакет. Кроме того, когда пакет поступает на последний узел, к которому непосредственно подсоединена LAN-сеть получателя, маршрутизатор посылает пакет непосредственно на MAC-адрес станции-получателя.

Интерактивная презентация: адреса второго и третьего уровней
После выполнения этого задания вы сможете легко ориентироваться в адресах второго и третьего уровней.

Определение административного расстояния маршрута

Одним из самых интригующих аспектов работы маршрутизаторов Cisco, особенно для тех, кто впервые сталкивается с маршрутизацией, является выбор устройством наилучшего из всех маршрутов, предлагаемых протоколом маршрутизации, заданных вручную и другими средствами выбора маршрутов. По мере того как маршрутизатор получает и обрабатывает сообщения об изменениях и другую информацию, он находит лучший путь к пункту назначения и пытается добавить этот маршрут к своей таблице маршрутизации.

Вопрос о том, добавлять ли представленный процессом маршрутизации маршрут, зависит от административного расстояния рассматриваемого маршрута. Если этот маршрут имеет наименьшее административное расстояние к пункту назначения, он заносится в таблицу маршрутизации; в противном случае маршрут отвергается. В табл. 20.1 перечислены стандартные значения административного расстояния для протоколов, поддерживаемых программным обеспечением Cisco.

Таблица 20.1. Стандартные административные расстояния

Тип маршрута	Административное расстояние
К непосредственно подсоединенной сети	0
Статический	1
Суммарный маршрут протокола EIGRP	5
Внешний сеанс протокола граничного шлюза (Border Gateway Protocol — eBGP)	20
Протокол EIGRP (внутренний)	90
Протокол IGRP	100
Протокол OSPF	110
Протокол IS-IS	115
Протокол RIP	120
Протокол EIGRP (внешний)	170
Внутрисетевой сеанс протокола граничного шлюза (Border Gateway Protocol — iBGP)	200

Определение метрики маршрута

Для определения наилучшего маршрута к пункту назначения протоколы маршрутизации используют какую-либо *метрику (metric)*. Метрика характеризует предпочтительность маршрута. Некоторые протоколы маршрутизации для вычисления метрики используют только один параметр; например, протокол RIP версии 1 для определения метрики маршрута использует количество переходов на маршруте к пункту назначения. Другие протоколы маршрутизации могут использовать такие параметры, как количество переходов, ширина полосы пропускания, задержка, нагрузка, надежность, тактовая задержка, максимальный модуль передачи (Maximum Transmission Unit — MTU) или стоимость маршрута. Эти параметры описаны в табл. 20.2.

Каждый алгоритм маршрутизации использует свои критерии для выбора наилучшего маршрута. Для каждого маршрута в сети алгоритм маршрутизации генерирует некоторое число, называемое значением метрики. Обычно чем меньше метрика, тем лучше маршрут. Такие параметры, как полоса пропускания и задержка, являются статическими в том смысле, что они остаются неизменными для каждого интерфейса маршрутизатора до тех пор, пока не будет изменена конфигурация маршрутизатора или перепроектирована сеть. Такие факторы, как нагрузка и надежность, являются динамическими — это означает, что они вычисляются маршрутизатором в реальном времени для каждого конкретного интерфейса.

Чем большее количество параметров учитывается метрикой, тем более гибко можно настроить параметры сети для достижения конкретных специфических целей. При вычислении метрики протокол IGRP стандартно использует два статических параметра: ширину полосы пропускания и задержку. Эти два параметра могут быть сконфигурированы вручную, что позволяет осуществлять полный контроль над

тем, как маршрутизатор выбирает маршруты. Протокол IGRP также может быть сконфигурирован для учета при вычислении метрики таких динамических параметров, как нагрузка и надежность. Используя эти динамические параметры, IGRP-маршрутизаторы могут принимать решения, основанные на текущем состоянии сети. Таким образом, если канал становится перегруженным или ненадежным, то протокол IGRP увеличивает значение метрики для маршрутов, пролегающих через этот канал. Но может оказаться, что альтернативные маршруты имеют меньшую метрику, чем перегруженные и ненадежные, и соответственно, они будут выбраны в качестве наилучших.

Таблица 20.2. Метрики маршрутов

Метрика	Описание
Количество переходов (Hop count)	Количество узлов-маршрутизаторов, через которые необходимо пройти пакету на пути к получателю. Выбирается маршрут с наименьшим количеством переходов
Ширина полосы пропускания (Bandwidth)	Скорость передачи, поддерживаемая каналом. Выбирается маршрут с наибольшей шириной полосы пропускания
Задержка (Delay)	Время, требуемое пакету для прохождения по каналу. Выбирается маршрут с наименьшей задержкой
Загрузка канала (Load)	Уровень активности передачи данных по каналу. Выбирается маршрут с наименьшей загрузкой
Надежность (Reliability)	Уровень ошибок в канале. Для маршрутизаторов Cisco это значение находится в диапазоне от 1 до 255, при этом значению 255 соответствует канал с максимальной надежностью. Выбираются маршруты с наивысшим уровнем надежности
Тактовая задержка (Ticks delay)	Используется протоколом IPX RIP и представляет собой число временны*х* интервалов длительностью 1/18 секунды, требуемых для пересылки пакета по каналу. Выбирается маршрут с наименьшей тактовой задержкой
Максимальный модуль передачи (Maximum transmission unit — MTU)	Максимальный размер пакета (в байтах), разрешенный для передачи по каналу. Выбирается маршрут с максимальным поддерживаемым всеми узлами размером модуля MTU
Стоимость (Cost)	Задаваемая администратором метрика. Выбирается маршрут с наименьшей стоимостью

Протокол IGRP вычисляет метрику маршрута путем сложения взятых с заранее определенным весовым коэффициентом значений для отдельных характеристик канала рассматриваемой сети. Эти значения (полоса пропускания, отношение полосы пропускания и нагрузки, задержка) в приведенной ниже формуле принимаются с постоянными весами K1, K2 и K3.

Метрика = [K1×полоса пропускания + K2×полоса пропускания/(256 – нагрузка) + + K3×задержка]×[K5/(надежность + K4)].

тем, как маршрутизатор выбирает маршруты. Протокол IGRP также может быть сконфигурирован для учета при вычислении метрики таких динамических параметров, как нагрузка и надежность. Используя эти динамические параметры, IGRP-маршрутизаторы могут принимать решения, основанные на текущем состоянии сети. Таким образом, если канал становится перегруженным или ненадежным, то протокол IGRP увеличивает значение метрики для маршрутов, пролегающих через этот канал. Но может оказаться, что альтернативные маршруты имеют меньшую метрику, чем перегруженные и ненадежные, и соответственно, они будут выбраны в качестве наилучших.

Таблица 20.2. Метрики маршрутов

Метрика	Описание
Количество переходов (Hop count)	Количество узлов-маршрутизаторов, через которые необходимо пройти пакету на пути к получателю. Выбирается маршрут с наименьшим количеством переходов
Ширина полосы пропускания (Bandwidth)	Скорость передачи, поддерживаемая каналом. Выбирается маршрут с наибольшей шириной полосы пропускания
Задержка (Delay)	Время, требуемое пакету для прохождения по каналу. Выбирается маршрут с наименьшей задержкой
Загрузка канала (Load)	Уровень активности передачи данных по каналу. Выбирается маршрут с наименьшей загрузкой
Надежность (Reliability)	Уровень ошибок в канале. Для маршрутизаторов Cisco это значение находится в диапазоне от 1 до 255, при этом значению 255 соответствует канал с максимальной надежностью. Выбираются маршруты с наивысшим уровнем надежности
Тактовая задержка (Ticks delay)	Используется протоколом IPX RIP и представляет собой число временны*х* интервалов длительностью 1/18 секунды, требуемых для пересылки пакета по каналу. Выбирается маршрут с наименьшей тактовой задержкой
Максимальный модуль передачи (Maximum transmission unit — MTU)	Максимальный размер пакета (в байтах), разрешенный для передачи по каналу. Выбирается маршрут с максимальным поддерживаемым всеми узлами размером модуля MTU
Стоимость (Cost)	Задаваемая администратором метрика. Выбирается маршрут с наименьшей стоимостью

Протокол IGRP вычисляет метрику маршрута путем сложения взятых с заранее определенным весовым коэффициентом значений для отдельных характеристик канала рассматриваемой сети. Эти значения (полоса пропускания, отношение полосы пропускания и нагрузки, задержка) в приведенной ниже формуле принимаются с постоянными весами K1, K2 и K3.

Метрика = [K1×полоса пропускания + K2×полоса пропускания/(256 – нагрузка) + + K3×задержка]×[K5/(надежность + K4)].

Стандартными значениями весов являются K1 = K3 = 1 и K2 = K4 = K5 = 0; в таком случае используется упрощенная формула расчета метрики протокола IGRP, в которой множитель [K5/(надежность + K4)] опущен. Композитная метрика рассчитывается по формуле:

Метрика = полоса пропускания + задержка.

Интерактивная презентация: метрики протоколов маршрутизации
В этой презентации подробно проиллюстрированы метрики протоколов маршрутизации.

Определение узла следующего перехода

Алгоритмы маршрутизации заполняют таблицы маршрутизации разнообразной информацией. Отраженная в этой таблице логическая связь между пунктом назначения и узлом следующего перехода указывает маршрутизатору, что оптимальным способом достичь этого пункта назначения является пересылка следующему находящемуся на маршруте к окончательному получателю транзитному переходу.

Когда маршрутизатор получает входящий пакет, он проверяет адрес пункта назначения и пытается связать этот адрес со следующим транзитным переходом маршрута.

Определение времени последнего обновления маршрута

Для поиска последних обновлений маршрута сетевой администратор может использовать такие команды:

- команда **`show ip route`** служит для отображения таблицы IP-маршрутизации маршрутизатора;
- команда **`show ip route`** *`network`* предоставляет подробную информацию в таблице маршрутизации для конкретной сети;
- команда **`show ip protocols`** используется для отображения информации протокола IP-маршрутизации;
- команда **`show ip rip database`** отображает содержимое частной базы данных протокола RIP в тех случаях, когда включен механизм рассылки обновлений по событиям.

Стандартно периодичность рассылки сообщений обновления маршрутизации составляет 30 секунд для протокола RIP и 90 секунд — для протокола IGRP.

В примере 20.1 показан результат работы команды **`show ip route`**.

Пример 20.1. Выводимая командой `show ip route` информация

```
rt1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
R 200.200.200.0/24 [120/1] via 192.168.10.2, 00:00:14, Serial0/0
C 192.168.10.0/24 is directly connected, Serial0/0
C 192.168.0.0/24 is directly connected, Loopback0
```

Маршрутизатор Rt1 получил обновление маршрутизации протокола RIP для сети 200.200.200.0 от сети 192.168.10.2. Обновления маршрутизации протокол RIP рассылает каждые 30 секунд; в данном примере затененная область показывает время, истекшее с момента последнего обновления.

В примере 20.2 приведена выводимая командой **`show ip route 200.200.200.0`** информация.

Пример 20.2. Результат выполнения команды `show ip route 200.200.200.0`

```
rt1# show ip route 200.200.200.0
Routing entry for 200.200.200.0/24
   Known via "rip", distance 120, metric 1
   Redistributing via rip
   Last update from 192.168.10.2 on Serial0/0, 00:00:11 ago
   Routing Descriptor Blocks:
   * 192.168.10.2, from 192.168.10.2, 00:00:11 ago, via Serial0/0
        Route metric is 1, traffic share count is 1
Rt1 has received a RIP update for the network 200.200.200.0 from
192.168.10.2.
RIP updates every 30 seconds and the last update was 11 seconds ago.
```

В примере 20.3 приведена информация, выводимая командой **`show ip protocols`**.

Пример 20.3. Результат выполнения команды `show ip protocols`

```
rt1# show ip protocols
Routing Protocol is "rip"
   Sending updates every 30 seconds, next due in 9 seconds
   Invalid after 180 seconds, hold down 180, flushed after 240
   Outgoing update filter list for all interfaces is
   Incoming update filter list for all interfaces is
   Redistributing: rip
   Default version control: send version 1, receive any version
      Interface Send Recv Triggered RIP Key-chain
      Serial0/0 1 1 2
      Loopback0 1 1 2
   Routing for Networks:
      192.168.0.0
      192.168.10.0
   Routing Information Sources:
```

```
      Gateway Distance Last Update
      192.168.10.2 120 00:00:03
   Distance: (default is 120)
```

В примере 20.4 приведена информация, выводимая по команде **show ip rip database**.

Пример 20.4. Результат выполнения команды show ip rip database

```
rt1# show ip rip database
192.168.0.0/24 auto-summary
192.168.0.0/24 directly connected, Loopback0
192.168.10.0/24 auto-summary
192.168.10.0/24 directly connected, Serial0/0
200.200.200.0/24 auto-summary
200.200.200.0/24
[1] via 192.168.10.2, 00:00:20, Serial0/0
```

Выводимая этой командой информация показывает, что последнее обновление маршрутизации произошло 20 секунд назад.

Практическое задание 20.1.8. Время последнего обновления маршрута
В этой лабораторной работе следует проверить информацию об анонсах протокола маршрутизации и определить, когда произошло последнее обновление таблицы маршрутизации RIP.

Несколько маршрутов к получателю

Большинство протоколов маршрутизации разрешает одновременно использовать несколько маршрутов к одному и тому же получателю. В отличие от одномаршрутных алгоритмов, эти алгоритмы с несколькими маршрутами позволяют передавать данные по нескольким каналам, обеспечивают большую надежность и более эффективное использование полосы пропускания.

Тестирование сети

Базовое тестирование сети следует проводить, последовательно переходя все уровни эталонной модели OSI, как показано на рис. 20.1.

Введение в тестирование сетей

Лучше всего начинать тестирование с первого уровня и при необходимости продолжать, переходя к более высоким уровням, вплоть до седьмого. Начиная с первого уровня, следует искать простые проблемы, например, не включенные в розетки шнуры питания.

Проблемы на втором уровне могут возникать вследствие неправильной конфигурации интерфейсов Ethernet, неправильной тактовой частоты; кроме того, следует

убедиться, что *карта сетевого интерфейса (Network Interface Card — NIC)* работоспособна.

Чаще всего проблемы в IP-сетях возникают из-за ошибок в схеме адресации, которые относятся к третьему уровню.

Далее в этой главе подробно рассматриваются различные проблемы, которые могут возникать на всех уровнях эталонной модели OSI. Прежде чем переходить к последующим этапам настройки, следует осуществить тестирование настроек адресов.

Каждый тест, описанный в этой главе, сосредоточен на сетевых операциях, осуществляемых на определенном уровне модели OSI.

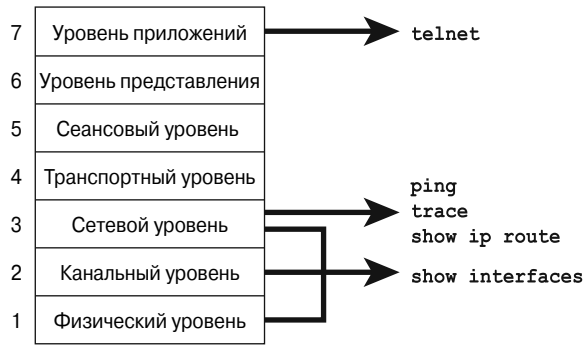


Рис. 20.1. Средства тестирования и эталонная модель OSI

Структурный подход к поиску и устранению неисправностей

Поиск и устранение неисправностей — это процесс, в ходе которого пользователь выявляет проблемы в сети. Он должен осуществляться в определенном порядке, определяемом установленными администрацией стандартами связи в сети. Чрезвычайно важной частью процесса поиска и устранения неисправностей является документация. На рис. 20.2 показана рекомендуемая логическая последовательность поиска и устранения неисправностей в сети.

На рис. 20.3 проиллюстрирован один из возможных подходов к поиску и устранению неисправностей в сети.

При структурном подходе все абоненты сети знают, что каждый участник процесса решил проблему. При беспорядочной реализации различных идей решение проблем становится хаотичным. Не применяя структурный подход, можно решить лишь немногие проблемы.

Способы поиска и устранения неисправностей, приведенные на блок-схемах рис. 20.2 и 20.3, не являются единственно возможными. Однако для бесперебойной и эффективной работы сети очень важно придерживаться определенного порядка работ.

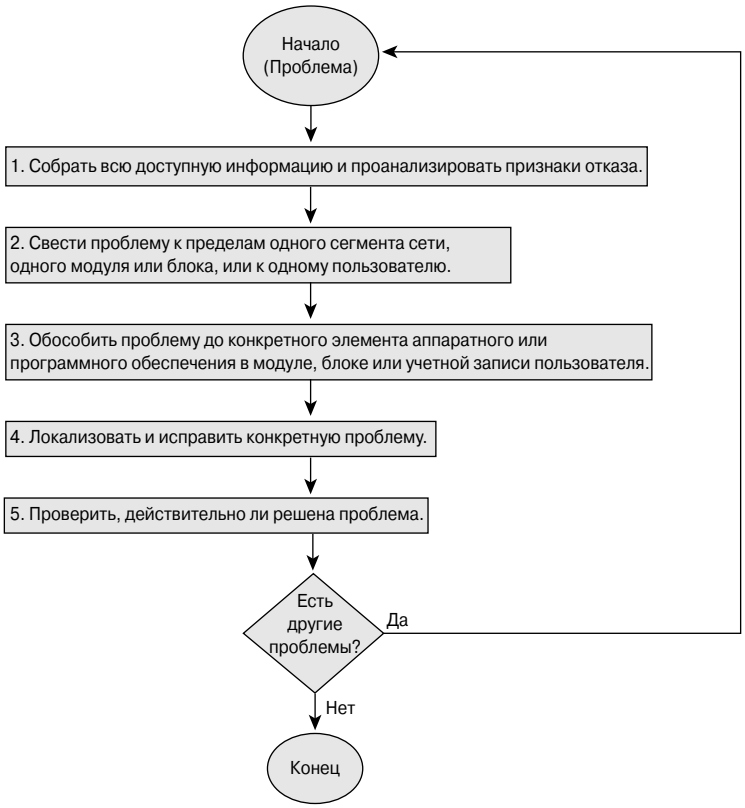


Рис. 20.2. Методика поиска и устранения неисправностей

Тестирование по уровням модели OSI

Тестирование следует начинать с первого уровня эталонной модели OSI и продолжать, если нужно, до седьмого. На первом, физическом, уровне могут возникать следующие ошибки:

- обрывы кабелей;
- отключенные кабели;
- кабели, подключенные не к соответствующим портам;
- неустойчивые соединения кабелей;
- для исполняемых задач используются несоответствующие кабели (следует правильно использовать консольные, перекрестные и прямые кабели);
- проблемы с трансиверами;
- неисправности кабелей аппаратуры передачи данных *(Data Communications Equipment — DCE)*;

- неисправности кабелей конечного оборудования *(Data Terminal Equipment — DTE)*;
- отключенные от питания устройства.

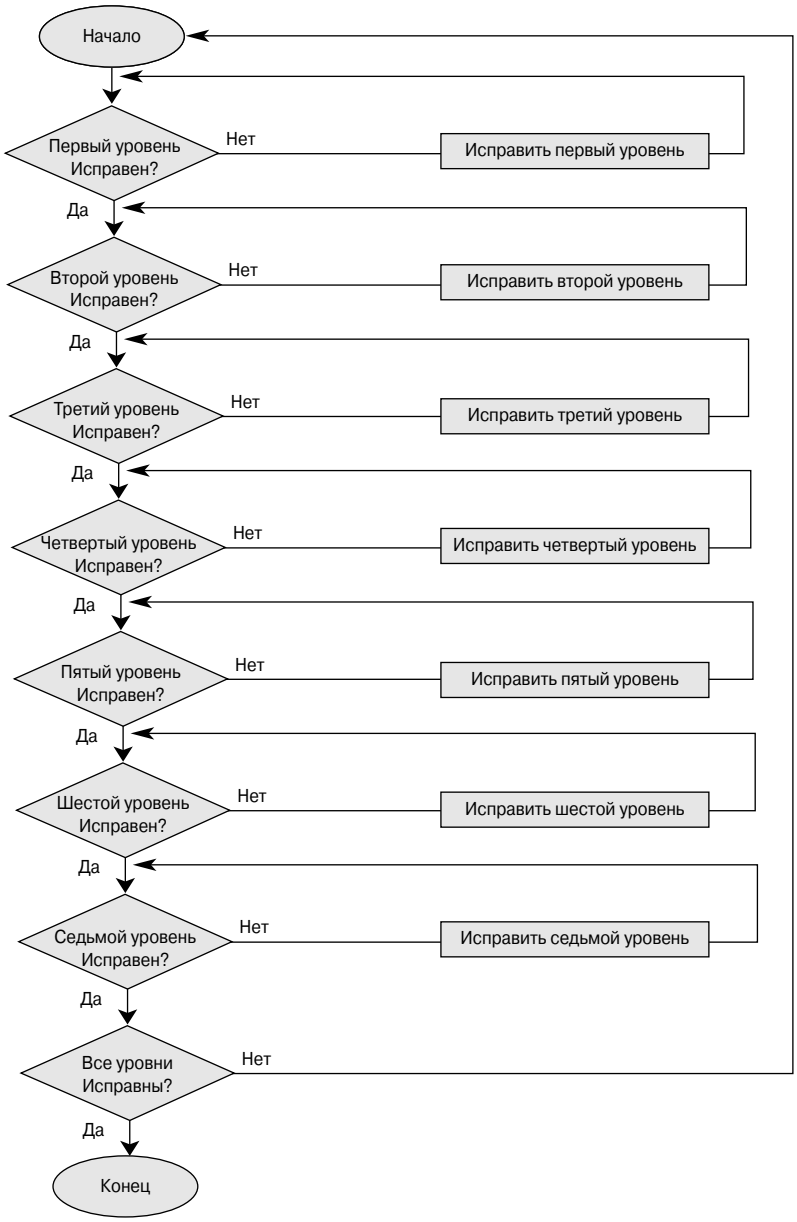


Рис. 20.3. Поиск и устранение неисправностей по уровням модели OSI

Решив все проблемы первого уровня, которые могли привести к возникновению проблемы в сети, следует перейти к поиску возможных проблем второго уровня.

К проблемам второго уровня относятся:

- неправильно настроенные последовательные интерфейсы;
- неправильно настроенные интерфейсы Ethernet;
- неправильная настройка инкапсуляции (стандартно для последовательных интерфейсов используется высокоуровневый протокол управления каналом (High-level Data Link Control — HDLC));
- неправильная настройка частоты синхронизации последовательных интерфейсов;
- неработоспособная *карта сетевого интерфейса (Network Interface Card — NIC)*.

Решив все проблемы первого уровня, которые могли привести к возникновению проблемы в сети, следует перейти к поиску возможных проблем третьего уровня.

К проблемам третьего уровня относятся следующие:

- не включен протокол маршрутизации;
- включен не тот протокол маршрутизации, который нужен;
- протокол маршрутизации настроен неправильно;
- указаны неправильные IP-адреса;
- указаны неправильные маски подсети;
- установлен неправильный стандартный шлюз.

Если в сети возникают проблемы с установлением соединения, сначала необходимо найти в сети точку пропадания пакетов. Для этого можно применить средства тестирования связи между узлами сети, например, команды **`ping`** и telnet. На третьем уровне для тестирования связи применяется команда **`ping`**. На седьмом уровне для проверки программного обеспечения уровня приложений между станцией-отправителем и станцией-получателем используется команда telnet. Все указанные команды подробнее обсуждаются ниже в настоящей главе.

Интерактивная презентация: проверка сети согласно уровням эталонной модели OSI
В этой презентации описан процесс поиска и устранения неисправностей согласно уровням модели OSI.

Поиск и устранение неисправностей первого уровня с помощью индикаторов

При поиске и устранении неисправностей очень полезны индикаторы устройств. Большинство сетевых интерфейсов имеет светодиодные индикаторы, указывающие на наличие соединения. Такие индикаторы называются *индикаторами соединения (link light)*. На интерфейсе могут быть также индикаторы, указывающие на наличие

передачи (TX) или приема (RX). Функции карты сетевого интерфейса относятся к первому и второму уровням.

Некоторые индикаторы указывают на наличие проблем на первом уровне сети, в частности, на такие неисправности:

- обрывы кабелей;
- отключенные кабели;
- кабели, подключенные не к соответствующим портам;
- неустойчивые соединения кабелей;
- для исполняемых задач используются несоответствующие кабели;
- проблемы с трансиверами;
- отключено питание устройства.

При использовании неисправного или неправильного кабеля может светиться индикатор, указывающий на плохое соединение или на его отсутствие.

Обязательно убедитесь, что все кабели включены в соответствующие гнезда. Удостоверьтесь, что все перекрестные коммутационные соединения подключены к нужным точкам, для них используются соответствующие кабели и применяется требуемый метод подключения. Проверьте правильность использования гнезд концентраторов для соответствующих виртуальных сетей (VLAN) или доменов коллизий, установку соответствующих параметров для протокола связующего дерева и прочие факторы.

Проверьте правильность использования кабелей. При наличии непосредственного соединения между двумя конечными устройствами, например, между персональным компьютером и маршрутизатором или между двумя коммутаторами, может понадобиться специальный кабель с перекрестной распайкой проводников. Убедитесь в правильном подключении и хорошем состоянии кабеля, включенного в определенный порт интерфейса. Если вам кажется, что соединение некачественное, выньте и вставьте кабель еще раз и проверьте надежность соединения. Если кабель включен в настенный разъем, проверьте правильность соединения кабеля с помощью кабельного тестера.

Проверьте также используемый трансивер и убедитесь, что используется трансивер нужного типа, что он правильно подключен и настроен. Если проблема не решается путем замены кабеля, попробуйте заменить трансивер, если вы вообще его используете.

Перед началом диагностики или комплексного поиска неисправностей всегда проверяйте наличие питания устройств. Некоторые проблемы возникают вследствие элементарнейших ошибок!

Поиск неисправностей на третьем уровне с помощью команды ping

Команда *ping* предназначена для тестирования наличия связи сети. Для содействия диагностике связи в базовой сети во многих сетевых протоколах поддерживается эхо-протокол, используемый для проверки маршрутизации протокольных пакетов.

Команда **ping** отправляет пакет узлу-получателю и ожидает ответный пакет. В результате с помощью эхо-протокола можно оценить надежность маршрута к узлу и задержки на маршруте, сделать вывод о достижимости и работоспособности узла. Команда **ping** предоставляет информацию о минимальном, среднем и максимальном времени, необходимом для доставки ping-пакета в указанную систему и его возврата. Для проверки аппаратного соединения и логического адреса сетевого уровня в команде **ping** используется *протокол управляющих сообщений в сети Internet (Internet Control Message Protocol — ICMP)*. Эта команда является основным средством тестирования сети.

В сети, показанной на рис. 20.4, адресат команды **ping 172.16.1.5** успешно ответил на все пять отправленных дейтаграмм, показанных в примере 20.5.

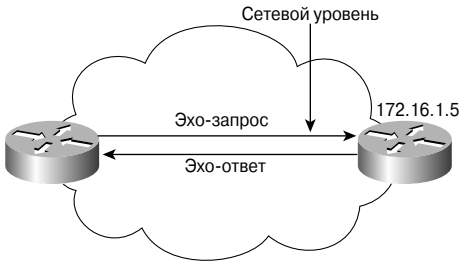


Рис 20.4. Тестирование сети командой ***ping***

Пример 20.5. Результаты выполнения команды ping для узла с адресом 172.15.1.5

```
Router> ping 172.16.1.5
Type escape sequence to abort
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max – 1/3/4 ms
Router>
```

Каждый восклицательный знак (!) означает полученный ответ. Если на дисплей выводятся точки (.), это означает, что приложение маршрутизатора не дождалось ответа адресата команды **ping** на отправленный пакет. Команду **ping** можно применять для базовой диагностики работоспособности сети.

Тестирование сети при помощи команды **ping** происходит путем отправки эхо-запросов протокола ICMP и ожидания ответов. При тестировании соединений эта команда отслеживает количество отправленных пакетов, количество полученных ответов, долю потерянных пакетов и промежуток времени, необходимый для доставки пакетов получателю и получения ответов. С помощью этой информации пользователь может проверить и способность рабочих станций поддерживать связь с другими узлами, и наличие потерь информации.

Команду **ping** можно выполнить как в пользовательском режиме EXEC, так и в привилегированном режиме EXEC. С помощью этой команды можно проверить наличие связи в сетях AppleTalk, сетях обслуживания без установления соединения ISO *(Connectionless Network Service — CLNS)*, а также сетях IP, Novell, Apollo, VINES, DECnet и XNS.

Сообщения в протоколе ICMP используются для выполнения разнообразных задач. Список сообщений протокола ICMP приведен в табл. 20.3.

Таблица 20.3. Различные типы сообщений протокола ICMP

Сообщение	Назначение сообщения
Destination unreachable (получатель недоступен)	Сообщает узлу-отправителю о проблеме при доставке пакета
Time exceeded (превышено время)	Для доставки пакета понадобилось слишком много времени, и пакет был отброшен
Source quench (подавление отправителя)	Отправитель передает данные быстрее, чем их можно переслать. Сообщение передает запрос отправителю на уменьшение скорости передачи данных
Redirect (перенаправление)	Маршрутизатор, отправляющий это сообщение, получил какой-то пакет, лучший маршрут для которого может быть предоставлен другим маршрутизатором. Сообщение указывает пользователю на необходимость использования лучшего маршрута
Echo (эхо)	Используется командой **ping** для проверки связи между узлами
Parameter problem (проблема с параметром)	Используется для определения неправильно указанного параметра
Timestamp (временная метка)	Используется для определения времени доставки пакета к отдельным узлам в прямом и обратном направлениях
Address mask request/reply (запрос/ответ маски адреса)	Служит для запроса и получения информации о маске подсети, которую следует использовать
Router advertisement and selection (анонс и выбор маршрутизатора)	С помощью этого сообщения узлы могут динамически получать информацию об IP-адресах маршрутизаторов, закрепленных за подсетью

С помощью расширенного командного режима команды **ping** пользователи могут указать поддерживаемые параметры заголовка IP-пакета. Такая установка дает маршрутизатору возможность провести более широкий ряд тестов. Для входа в расширенный режим команды **ping** необходимо в привилегированном режиме ввести с клавиатуры эту команду без параметров и нажать клавишу <Enter>. В командной строке будет запущен интерактивный диалог, в котором можно задать основные параметры, в том числе и расширенные команды (Extended Commands). В ответ на запрос подсказки расширенных команд следует ввести слово **yes** (да) — таким образом задается расширенный набор параметров команды **ping**. Расширенная команда **ping** работает точно так же, как обычная, но поддерживает управление некоторыми

дополнительными параметрами, в частности, размером пакетов и частотой их пересылки.

Можно выполнить команду **`ping`**, когда сеть работает хорошо, и проследить за ее работой в нормальных условиях. В таком случае при поиске неисправностей результаты ее работы можно будет с чем-то сравнить.

Поиск неисправностей на седьмом уровне с помощью команды telnet

Telnet представляет собой протокол виртуального терминала, входящий в стек протоколов TCP/IP. Он позволяет проверять работу программного обеспечения уровня приложений между станцией-отправителем и станцией-получателем. На сегодняшний день это самый полный из существующих простых механизмов тестирования. Соответствующая служба позволяет осуществлять соединения с удаленными устройствами, собирать информацию и выполнять команды и прикладные программы.

Протокол telnet является самым полным из существующих механизмов тестирования, поскольку для установления сеанса с удаленным узлом в нем на сетевом уровне используется протокол IP, а на транспортном — TCP. Если служба или протокол telnet работает успешно, скорее всего, в канале есть устойчивая связь.

Команда telnet эмулирует виртуальный терминал и позволяет администраторам использовать возможности протокола telnet для соединения с другими сетевыми устройствами (например, маршрутизаторами и коммутаторами), которые используют протокол TCP/IP. Если с помощью протокола telnet можно осуществить удаленный доступ к маршрутизатору, то к этому маршрутизатору может обратиться, по крайней мере, одно приложение TCP/IP. Успешное соединение по протоколу telnet указывает на нормальное функционирование приложения верхнего уровня и служб низших уровней. Пример соединения по протоколу telnet проиллюстрирован на рис. 20.5.

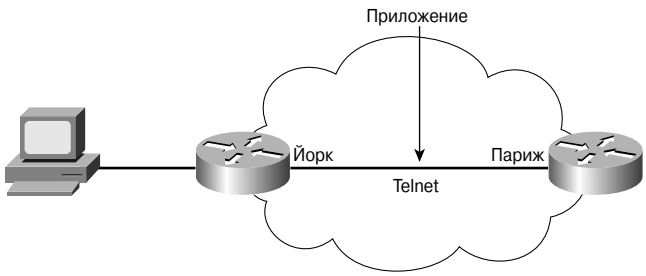


Рис. 20.5. Использование протокола telnet

Если администратор может с помощью протокола telnet обратиться к одному маршрутизатору, а к другому — нет, скорее всего, сбой сеанса telnet происходит вследствие отдельных проблем с адресацией, назначением имен или разрешением доступа. Такие проблемы могут существовать в маршрутизаторе администратора или в маршрутизаторе, который отказал при выполнении функций объекта telnet.

Если произошел сбой во время сеанса связи по протоколу telnet от одного узла, попытайтесь осуществить связь с маршрутизатором и несколькими другими устройствами. Для основательного тестирования попробуйте воспользоваться также командой **ping**. Если узел можно проверить с помощью команды **ping**, а при попытке связи по протоколу telnet отсутствует приглашение командной строки входа в систему, следует проверить вот что:

- работает ли обратное преобразование DNS-имени клиента? Многие серверы telnet не позволяют осуществлять соединения с IP-адресами, не имеющими имени в базе сервера DNS. Это обычная проблема для адресов, назначенных службой DHCP, в которых администратор не ввел имя в поле DNS для пулов DHCP;
- возможно, приложение telnet неспособно прийти к соглашению об удовлетворительных параметрах и поэтому не устанавливает соединение. В маршрутизаторах Cisco процесс согласования можно просмотреть с помощью команды **debug telnet**. Необходимо найти сообщения об ошибках, недействительный IP-адрес или DNS-имя, которые могут указывать на проблему;
- возможно, протокол telnet на сервере-получателе отключен или ему не назначен или недоступен стандартный порт 23. Следует помнить, что стандартным портом протокола telnet является порт 23.

Практическое задание 20.2.6. Поиск неисправностей с помощью команд ping и telnet
В этой лабораторной работе полученные знания о первых трех уровнях модели OSI используются для диагностики ошибок конфигурации с помощью служебных команд **ping** и telnet.

Поиск и устранение неисправностей в маршрутизаторах

Проблемы в маршрутизации относятся к наиболее сложным неисправностям, которые приходится устранять сетевому администратору. Поиск неполадки и принятие правильного решения по ее устранению исключительно сложны, поэтому разработано множество инструментов, которые могут облегчить этот процесс. В текущем разделе основное внимание уделено таким средствам и инструментам, а также методам их практического применения.

Поиск неисправностей на первом уровне с помощью команды show interfaces

В состав программного обеспечения Cisco IOS входит множество команд поиска неисправностей. К наиболее известным принадлежат команды группы **show**. С помощью одной или нескольких команд **show** можно всесторонне обследовать маршрутизатор. Команда **show interfaces** используется для проверки состояния и статистики интерфейсов. С помощью различных ее вариантов можно проверять

состояние разнообразных интерфейсов. Например, состояние интерфейсов FastEthernet можно узнать с помощью команды **show interfaces fastethernet**; если же указать данную команду без параметров, то интерфейс командной строки выведет на экран информацию обо всех интерфейсах. Эта команда позволяет также узнать о состоянии конкретного интерфейса. Например, просмотреть состояние последовательного интерфейса 0/0 можно с помощью команды **show interfaces serial 0/0**, а состояние интерфейса FastEthernet 0/0 — с помощью команды **show interfaces fa 0/0**.

Команда **show interfaces** отображает состояние двух важных составляющих интерфейсов. Их можно отнести к функциям первого и второго уровней.

- **Физическая (аппаратная) составляющая**. К аппаратной части относятся кабели, разъемы и интерфейсы, которые отображают состояние физического соединения между устройствами.
- **Логическая (программная) составляющая**. Состояние программного обеспечения отображает такие сообщения, как *тестовые пакеты* соединений, управляющую и пользовательскую информацию, передаваемую между соединенными устройствами. Логическая составляющая относится к состоянию протокола на канальном уровне передачи данных между двумя соединенными интерфейсами соседних маршрутизаторов.

Такие важные составляющие выходных данных команды **show interfaces serial,** как состояние линии и состояние протокола, показаны в примере 20.6.

Пример 20.6. Результат выполнения команды show interface serial

```
Cougars# show interface serial 0
Serial0 is up, line protocol is up
Hardware is HD64570
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:02:57
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 8 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Первый параметр (`Serial0 is up`) относится к аппаратному уровню и несет существенную информацию о том, получает ли интерфейс сигнал обнаружения несущей от противоположного конца линии (устройства DCE). Если линия отключена, это может указывать на проблему лабораторного соединения, когда один из абонентов выключен "административно" (т.е. администратором). Если интерфейс выключен административным способом, это означает, что он отключен вручную при конфигурировании.

Команда **`show interfaces`** также предоставляет информацию, помогающую диагностировать другие проблемы первого уровня, обнаружить которые не так легко.

Увеличение количества переключений несущей частоты (carrier transition) в последовательном канале может быть вызвано такими проблемами:

- разрыв соединения со стороны сети поставщика услуг;
- аппаратные сбои в коммутаторах, модулях обработки данных или маршрутизаторах.

Увеличение счетчиков входных ошибок в выводимой командой **`show interfaces`** информации возможно вследствие нескольких перечисленных ниже типов ошибок, которые относятся к первому уровню эталонной модели.

- Неисправное оборудование телефонной компании.
- Помехи в последовательном канале.
- Неправильное использование кабеля или длина кабеля превышает предельно допустимую.
- Повреждение кабеля или соединения.
- Неисправный модуль обслуживания канала или модуль обработки данных.
- Аппаратная неисправность маршрутизатора.

Другой областью исследования является количество сбросов интерфейса (reset). Сбросы интерфейса возникают из-за большого количества пропущенных тестовых пакетов. Проблемы на первом уровне могут возникать также в силу следующих причин:

- низкое качество телефонных линий, приводящее к переключению сигнала несущей;
- возможные аппаратные неисправности модуля обслуживания канала, модуля обработки данных или маршрутизатора.

Количество ошибок следует рассматривать по отношению к объему обработанного маршрутизатором трафика и продолжительности сбора статистической информации. Маршрутизатор собирает статистику, которая предоставляет информацию

об интерфейсе. Статистика отражает работу маршрутизатора с момента запуска или с момента последней очистки счетчиков, как показано в примере 20.7.

Пример 20.7. Накопление статической информации

```
Cougars# show interface serial 0
Serial0 is up, line protocol is up
Hardware is HD64570
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:02:57
```

Если в выводимой командой **show interfaces** информации показано, что счетчики никогда не сбрасывались, определите время работы маршрутизатора с помощью команды **show version**, как показано в примере 20.8.

Пример 20.8. Время непрерывной работы маршрутизатора

```
Cougars# show version
Cisco Internetwork Operating System Software
IOS (tm) 2600 Software (C2600-BNSY-L), Version 12.2(6h), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
Compiled Mon 26-Aug-02 23:23 by kellythw
Image text-base: 0x0303ED8C, data-base: 0x00001000


ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTLDR: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c),
RELEASE SOFTWA RE (fc1)


Cougars uptime is 14 minutes
```

Чтобы обнулить счетчики, следует применить команду **clear counters**, как показано в примере 20.9. Обнулять счетчики нужно после устранения проблемы интерфейса. Обнуление счетчиков позволяет получить четкое представление о текущем состоянии сети и убедиться в том, что проблема устранена.

Пример 20.9. Команда `clear counters`

```
Cougars# clear counters
Clear "show interface" counters on all interfaces [confirm]yes
Cougars#
00:17:24: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
Cougars#
```

Поиск неисправностей на втором уровне с помощью команды show interfaces

Команда **show interfaces** является, возможно, единственным и важнейшим средством обнаружения проблем первого и второго уровней эталонной модели взаимодействия открытых систем в маршрутизаторе. Первый выходной параметр — линия — относится к физическому уровню. Второй параметр — протокол — указывает, пригоден ли интерфейс к использованию с точки зрения процессов программного обеспечения Cisco (Cisco IOS), которые управляют протоколами передачи данных в линии. Последний параметр зависит от успешного получения тестовых пакетов линии. Если интерфейс не получил три тестовых пакета подряд, считается, что протокол отказал.

При отказе линии протокол также отключается из-за отсутствия физического канала передачи, пригодного для работы протокола. Такое случается при отказе интерфейса, при наличии аппаратной проблемы или если интерфейс отключен "административным" способом (т.е. вручную администратором) в силу соответствующей настройки.

Если интерфейс включен, а протокол линии не работает, это указывает на наличие проблемы второго уровня. Возможными причинами могут быть:

- отсутствие тестовых пакетов в линии;
- отсутствие синхроимпульсов;
- несоответствие инкапсуляции;
- интерфейс отключен;
- при аутентификации на линии были переданы неправильные параметры.

Перечисленные проблемы можно обнаружить, если при вводе команды **show interfaces** появляется строка сообщения: "`interface is up and the line protocol is down`" (интерфейс работает, а протокол линии — нет). С помощью команд **clockrate** и **encapsulation** убедитесь, что нет несоответствия в конфигурации интерфейсов.

После настройки последовательного интерфейса подтвердите изменения и убедитесь в работоспособности интерфейса с помощью команды **show interfaces**.

Поиск неисправностей на втором уровне с помощью команды show cdp

Протокол обнаружения устройств Cisco (Cisco Discovery Protocol — CDP) передает смежным узлам информацию об устройстве, например, его MAC- и IP-адреса и интерфейсы, через которые пересылается информация.

Команда `show cdp neighbors` отображает информацию об устройствах, которые подключены к текущему, как показано в примере 20.10.

Пример 20.10. Результат выполнения команды `show cdp neighbors`

```
routerA# show cdp neighbors
Capability Codes:
R — Router, T — Trans Bridge,
B — Source Route Bridge,
S — Switch, H — Host, I — IGMP

Device ID   Local Interface   Holdtime   Capability   Platform   Port   ID
routerB     Eth 0             151        R            2501       Eth    0
routerB     Ser 0             165        R            2501       Ser    0
```

Выводимая этой командой информация нужна для отладки проблем со связью между устройствами. Если подозрение падает на ненадежное кабельное соединение, то перед тем как изменять какие-либо настройки, включите интерфейсы командой **`no shutdown`** и выполните команду **`show cdp neighbor detail`**, как показано в примере 20.11.

Пример 20.11. Результат выполнения команды `show cdp neighbor detail`

```
routerA# show cdp neighbors detail
Device ID: routerB
Entry address(es):
IP address: 198.92.68.18
Platform: 2501, Capabilities: Router
Interface: Ethernet0, Port ID (outgoing port): Ethernet0
Holdtime: 143 sec
```

При нормальной работе физического уровня в выводимой такой командой информации должны быть перечислены все остальные устройства Cisco, непосредственно подключенные к данному маршрутизатору. Если заведомо существующее устройство не показано, возможно, связь с ним нарушена на первом уровне.

При использовании протокола CDP следует уделять особое внимание вопросам безопасности. Этот протокол передает большое количество информации об устройствах, и ее распространение может представлять потенциальную угрозу безопасности. По соображениям безопасности, настраивать конфигурацию протокола CDP следует только для каналов между устройствами Cisco, а для пользовательских портов и каналов, управляемых из другой точки, средства CDP следует отключать.

Поиск неисправностей на третьем уровне с помощью команды traceroute

Команда **`traceroute`** применяется для отображения маршрутов, по которым проходят пакеты при доставке их в пункты назначения. Также ее можно использовать для последовательного тестирования третьего (сетевого) уровня эталонной модели и контроля характеристик системы.

При выполнении команды **traceroute** можно получить список успешно пройденных тестовыми запросами узлов, как показано в примере 20.12. При успешной доставке данных в пункт назначения в списке перечисляются все маршрутизаторы, через которые проходила дейтаграмма. Такие выходные данные можно сохранить для поиска неисправностей в сети в дальнейшем.

Пример 20.12. Результат выполнения команды `traceroute`

```
Cougars> traceroute 168.71.8.2
traceroute to pc-b.Cisco.com (168.71.8.2), 30 hops max, 40 byte packets
1 routerb (168.71.6.3) 3 ms 3 ms 3 ms
2 * * *
3 * * *
4 * * *
5 * * *
Cougars>
```

По выводимой командой **traceroute** информации можно определить конкретный узел, в котором произошел сбой. Для каждого маршрутизатора по маршруту на терминале выводится строка, которая отображает IP-адрес интерфейса, принявшего данные. Если выводится символ "звездочка" (<*>), то это означает, что пакет был утерян. Локализовать проблему можно, сравнив со схемой сети подключение последнего узла, указанного в выводимом списке.

Команда **traceroute** предоставляет информацию об относительных характеристиках каналов. Время двухсторонней передачи сообщения (Round-Trip Time — RTT) — это время, необходимое для пересылки эхо-пакета и получения ответа, как показано в примере 20.12. В этом примере для каждого из трех отправленных пакетов время двухсторонней передачи (RTT) равно трем миллисекундам (мс). Такие данные будут полезны, т.к. помогут получить приблизительное представление о задержках передачи по каналу. Поскольку выводимые значения являются приблизительными, их нельзя использовать для точной оценки характеристик соединений; тем не менее, их можно сохранить и в дальнейшем использовать для поиска проблем и мониторинга характеристик сети.

Устройство, получающее пакет, который отправлен командой **traceroute**, должно также владеть информацией о том, как переслать ответ отправителю запроса. Чтобы данные команд **ping** и **traceroute** успешно проходили маршрут между маршрутизаторами в оба конца, должны быть известны маршруты в обе стороны. Отсутствие ответа не обязательно указывает на наличие проблемы, поскольку сообщения ICMP могут быть или отфильтрованы на некотором участке промежуточным узлом, или для них могут быть установлены ограничения по скорости. Более всего такое утверждение касается сети Internet.

Команда **traceroute** отправляет последовательность сообщений посредством протокола пользовательских дейтаграмм (UDP) по несуществующему адресу порта на удаленный узел. Для первой последовательности из трех посланных дейтаграмм значение в поле времени существования пакета (Time-To-Live — TTL) устанавливается

равным единице. Если время существования пакета равно 1, то оно истекает на первом маршрутизаторе по маршруту. Такой маршрутизатор пересылает в ответ сообщение об истечении времени (Time Expired Message — TEM), которое означает истечение срока существования дейтаграммы.

Далее пересылаются еще три дейтаграммы, для каждой из которых величина TTL равна 2. В результате отправки такой последовательности второй маршрутизатор на маршруте возвращает сообщения протокола ICMP об истечении времени (TEM). Процесс продолжается до тех пор, пока пакеты не достигнут нужного получателя или не будет превышено максимальное значение параметра TTL. Стандартное максимальное значение времени TTL для команды **traceroute** составляет 30 (т.е. 30 транзитных переходов).

Поскольку пересылаемые дейтаграммы направлены в несуществующий порт, вместо сообщений ICMP об истечении времени (TEM) отправителю пересылаются сообщения ICMP о невозможности доставить пакет в указанный порт. Такая ситуация указывает на недостижимость порта и завершение процесса трассировки маршрута; программа **traceroute** по такому сигналу прекращает обмен сообщениями.

Практическое задание 20.3.4. Поиск неисправностей с помощью команды traceroute
В этой лабораторной работе описано, как с помощью команд **traceroute** и **tracert** убедиться в том, что средства сетевого уровня между отправителем, получателем и каждым маршрутизатором по маршруту следования пакета функционируют правильно.

Поиск неисправностей маршрутизации с помощью команд show ip route и show ip protocol

Команды **show ip route** и **show ip protocol** отображают информацию о протоколах маршрутизации и таблице маршрутизации.

Команда **show ip route**, возможно, является самой важной командой для поиска неисправностей маршрутизации. Она выводит содержимое таблицы маршрутизации протокола IP. Результаты работы команды, которые приведены в примере 20.13, показывают все известные маршрутизатору подсети и сети, а также способы получения информации о них.

Пример 20.13. Результат выполнения команды show ip route

```
Cougars> show ip route
Codes: C – connected, S – static, R – RIP, M – mobile, B – BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP
i – IS-IS, L1 – IS-IS level 1, L2 – IS-IS level 2
* - candidate default

Gateway of last resort is not set

    144.253.0.0 is subnetted (mask is 255.255.255.0), 1 subnets
C 144.253.100.0 is directly connected. Ethernet1
```

```
R 153.50.0.0 [120/1] via 183.8.128.12, 00:00:09, Ethernet0
    183.8.0.0 is subnetted (mask is 255.255.255.128), 4 subnets
R     183.8.0.128 [120/1] via 183.8.128.130.00, 00:00:17, Serial0
                  [120/1] via 183.8.64.130, 00:00:17, Serial1
C 183.8.128.0 is directly connected, Ethernet0
C 183.8.64.128 is directly connected, Serial1
C 183.8.128.128 is directly connected, Ethernet0
```

Если в какой-либо сети возникают сбои при попытке установить связь с узлом, результаты работы команды **show ip route** можно использовать для проверки наличия маршрута к такой сети.

Если в выводимой командой **show ip route** информации не приведены ожидаемые известные маршруты или приведены неизвестные маршруты, возможная причина проблемы может состоять в отсутствии обмена информацией о маршрутизации. В таком случае с помощью команды **show ip protocols**, как показано в примере 20.14, проверьте, правильно ли сконфигурирован протокол маршрутизации.

Пример 20.14. Результаты выполнения команды show ip protocols

```
Router> show ip protocol
Routing Protocol is rip
Sending updates every 30 seconds, next due in 13 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Redistributing:   rip
Routing for Networks:
183.8.0.0
144.253.0.0
Routing Information Sources:
Gateway Distance Last Update
183.8.128.12 120 0:00:14
183.8.64.130 120 0:00:19
183.8.128.130 120 0:00:03
Distance:   (default is 120)
```

После введения команды **show ip protocols** на экран выводится информация о протоколе маршрутизации IP для всего маршрутизатора. С помощью этой команды можно проверить, какие протоколы маршрутизации включены, какие сети рассылают свои данные, какие интерфейсы присылают обновления, а также просмотреть информацию об отправителях обновлений маршрутов. В выводимой командой **show ip protocols** информации также присутствуют дополнительные настройки протоколов маршрутизации, таймеры, фильтры и прочая информация, относящаяся ко внутренним механизмам средств обнаружения маршрутов. Если настроено несколько протоколов маршрутизации, то информация о каждом из них приводится в отдельном подразделе.

Команду **show ip protocols** можно использовать для диагностики проблем маршрутизации, например, идентификации маршрутизатора, предоставляющего о

себе неправильную информацию. Результаты работы этой команды позволяют проверить, установлены ли необходимые протоколы, какие сети рассылают свои данные, а также получить сведения о соседних узлах. Следует иметь в виду, что, если отсутствует документация, в которой указаны желаемые результаты выполнения такой команды, обнаружить проблему очень трудно, если вообще возможно. Это касается любого процесса поиска неисправностей.

Практическое задание 20.3.5. Поиск и устранение неисправностей с помощью команд `show ip route` и `show ip protocol`

В этой практической лабораторной работе необходимо с помощью команд **`show ip route`** и **`show ip protocol`** найти и устранить проблемы в конфигурации протоколов маршрутизации в сети.

Поиск неисправностей соединений маршрутизатора с помощью команды show controllers

Настройка и поиск неисправностей маршрутизаторов зачастую осуществляется удаленно. В таком случае визуально осмотреть соединения и интерфейсы маршрутизатора невозможно. Чтобы определить тип подключенного кабеля без осмотра кабелей, используется команда **`show controllers serial`**, проиллюстрированная в примере 20.15.

Пример 20.15. Выводимая командой `show controllers serial` информация

```
Cougars# show controllers serial 0/0
QUICC Serial unit 0
idb at 0x20A31A8, driver data structure at 0x20A4C60
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x0
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x0006
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:

! --- Часть выводимой информации опущена ---

DTE V.35 serial cable attached.

! --- Часть выводимой информации опущена ---
```

Функция определения типа кабеля, который обнаружен контроллером, пригодится для поиска интерфейсов, к которым вовсе не подключен кабель, подключен неправильный или поврежденный кабель.

При выполнении команды **`show controllers serial 0/0`** отправляется запрос интегральной микросхеме, которая управляет последовательными интерфейсами; в ответ она предоставляет информацию о физическом интерфейсе. Предоставляемая разными микросхемами контроллеров информация может определенным

образом отличаться. Даже в маршрутизаторах одного типа могут использоваться различные микросхемы, например, разных производителей.

Какой бы контроллер не использовался, при применении команды **show controllers serial** можно получить огромный объем информации. Кроме сведений о типе кабеля, большая часть выводимой информации содержит внутренние технические подробности о состоянии микросхемы контроллера; без конкретных знаний о микросхеме эта информация не нужна.

Применение команды debug

Команда **debug** позволяет локализировать проблемы с протоколами и неправильные настройки. Она нужна для вывода динамических данных и событий. Поскольку команды группы **show** отображают только статическую информацию, они предоставляют лишь статическую картину работы маршрутизатора. Данные, получаемые в результате выполнения команды **debug**, обеспечивают более глубокое понимание текущих событий в процессе работы маршрутизатора. К таким событиям относятся коммутация трафика через интерфейс, сообщения об ошибках, выдаваемые узлами сети, диагностические пакеты отдельных протоколов и другие данные, полезные при поиске неисправностей. Образец данных, полученных при выполнении команды **debug ip rip**, приведен в примере 20.16.

Пример 20.16. Команда `debug ip rip`

```
Router# debug ip rip
RIP Protocol debugging is on
Router#
RIP: received update from 183.8.128.130 on Serial0
183.8.0.128 in 1 hops
183.8.64.128 in 1 hops
0.0.0.0 in 16 hops (inaccessible)
RIP: received update from 183.8.64.140 on Seria11
183.8.0.128 in 1 hops
183.9.128.128 in 1 hops
0.0.0.0 in 16 hops (inaccessible)
RIP: received update from 183.8.128.130 on Seria10
183.8.0.128 in 1 hops
183.8.64.128 in 1 hops
0.0.0.0 in 16 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Ethernet0 (183.8.128.2)
subnet 183.8.0.128, metric 2
subnet 183.8.64.128, metric 1
subnet 183.8.128.128, metric 1
default 0.0.0.0, metric 16
network 144.253.0.0, metric 1
RIP: sending update to 255.255.255.255 via Ethernet1
(144.253.100.202)
default 0.0.0.0, metric 16
network 153.50.0.0, metric 2
network 183.8.0.0, metric 1
```

Затененные строки в примере 20.16 свидетельствуют о том, что отладка протокола RIP включена и показывает, какие маршруты, сети и интерфейсы являются доступными, а какие — нет.

Динамический стиль работы команды **debug** осуществляется за счет системных ресурсов, что приводит к сильной перегрузке процессора и может нарушить нормальную работу маршрутизатора. Поэтому использовать эту команду следует умеренно. С помощью команд отладки (debug) можно исследовать отдельные типы трафика, т.е. рекомендуется сузить поле поиска проблемы до нескольких вариантов. Иными словами, команды группы **debug** следует использовать для выделения конкретных проблем, а не для наблюдения за нормальной работой сети.

ВНИМАНИЕ!

В частности, команду **debug all** следует применять как можно реже, т.к. она может привести к нарушению нормальной работы сети.

Стандартно маршрутизатор отправляет выводимые командой **debug** данные и системные сообщения на консоль. Если для обследования маршрутизатора используется сеанс telnet, выводимые командой данные и системные сообщения можно перенаправить на удаленный терминал. В сеансе telnet следует выполнить команду **terminal monitor**, и тогда системные сообщения будут отправляться на виртуальный терминал. Выбирать команды группы **debug** из сеанса telnet следует с особой осторожностью. Нельзя использовать команду, которая приведет к созданию средствами отладки дополнительного трафика. В таком случае сеанс telnet быстро заполнит трафиком канал связи или же маршрутизатор исчерпает один или несколько ресурсов. Такого нарастания трафика можно избежать, следуя хорошему правилу: ни в коем случае не применять команду **debug** к порту, на котором установлен сеанс.

Результаты выполнения команды **debug** с разными параметрами отличаются. Одна комбинация приведет к частому выводу большого количества строк, а другая выводит строчку-две каждые несколько минут. В примере 20.17 приведен результат выполнения команды **debug ip packet detail**[2].

Пример 20.17. Результат выполнения команды debug ip packet detail

```
Router# debug ip packet detail
10w6d: TCP src=1075, dst=80, seq=785595392, ack=3448593899,
   win=64240 ACK
10w6d: IP: s=192.168.120.145
(Ethernet0/0), d=192.168.119.9 (Ethernet0 /0),
g=192.168.119.9, len 60, forward
```

[2] *Как раз этим вариантом команды следует пользоваться с особой осторожностью на загруженных маршрутизаторах. — Прим. ред.*

```
10w6d: TCP src=1075, dst=80, seq=785595392, ack=3448599739,
   win=64240 ACK
10w6d: IP: s=192.168.120.145 (Ethernet0 /0), d=192.168.119.9
  (Ethernet0 /0),
g=192.168.119.9, len 60, forward
10w6d: TCP src=80, dst=1075, seq=3448603559, ack=785595392,
  win=8446 ACK PSH
10w6d: IP: s=192.168.120.145 (Ethernet0), d=192.168.119.9
  (Ethernet0 /0),
g=192.168.119.9, len 60, forward
10w6d: TCP src=1075, dst=80, seq=785595392, ack=3448604710,
   win=64240 ACK
10w6d: IP: s=10.1.1.81
(Serial0 /0), d=224.0.0.10, len 64, rcvd 2, proto=88
10w6d: IP: s=210.107.197.105
(Serial0 /0), d=192.168.119.255, len 1028,
access denied
10w6d: ICMP type=8, code=0
10w6d: IP: s=10.1.1.82
(local), d=224.0.0.10 (Serial0 /0), len 22,
sending broad/multicast, proto=88
10w6d: IP: s=0.0.0.0 (Ethernet0 /0), d=255.255.255.255, len 590,
   rcvd 2
10w6d: UDP src=68, dst=67
10w6d: IP: s=192.168.120.50 (Ethernet0 /0), d=192.168.120.255
   (Ethernet0 /0),
len 243, rcvd 3
Router# undebug all
All possible debugging has been turned off
GAD#
```

Дополнительной службой программного обеспечения Cisco IOS, которая повышает ценность результатов работы команды **debug**, является команда **timestamp**. Она помечает сообщение команды **debug** временной меткой, поэтому в сообщениях указано время, когда произошло событие, и интервал времени между событиями. При использовании команды **service timestamps debug uptime** может приводиться время (в формате `час:минуты:секунды`) вывода, продолжительность работы маршрутизатора с момента последнего включения или указываться время последнего выполнения команды **reload**.

Команды **no debug all** и **undebug all** отключают выдачу всех диагностических сообщений. Для отключения конкретной команды **debug** используется команда в форме **no debug** *параметр*. Например, если отладка для отслеживания протокола RIP была включена командой **debug ip rip**, ее можно отключить командой **no debug ip rip**. Просмотреть все, что в данный момент исследуется с помощью команды **debug**, можно, используя команду **show debugging**.

Практическое задание 20.3.5. Поиск и устранение неисправностей с помощью команды `debug`

В этой практической работе для сбора диагностической информации и для отслеживания проблем маршрутизации используется систематический процесс поиска неисправностей на основе модели OSI. Для облегчения поиска неисправностей применяется команда **`debug`**.

Резюме

В этой главе были рассмотрены следующие ключевые понятия:

- для поддержки бесперебойной и эффективной работы сети следует ее периодически тестировать. Тестирование должно проводиться последовательно, по уровням эталонной модели взаимодействия открытых систем;
- при поиске и устранении неисправностей следует применять структурный подход;
- при поиске неисправностей полезны такие команды, как **`ping`** и telnet;
- для определения состояния каналов между маршрутизаторами можно использовать команду **`traceroute`**;
- с помощью разных команд группы **`show`** можно различить проблемы первого и второго уровней;
- проблемы маршрутизации легче распознать с помощью команд **`show ip route`** и **`show ip protocol`**;
- с помощью основных команд группы **`debug`** можно получить информацию о работе маршрутизатора.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Ключевые термины

Ping — отправитель запросов сети Internet. Представляет собой эхо-сообщение протокола ICMP и ответ на него. Применяется в сетях с использованием протокола IP для тестирования достижимости сетевого устройства.

Telnet представляет собой стандартный протокол эмуляции терминала в стеке протоколов TCP/IP. Служба telnet применяется для удаленного соединения эмуляции терминала и позволяет пользователям входить в удаленные системы и пользоваться ресурсами точно так же, как в локальной системе.

Traceroute — это программа, отслеживающая маршрут, по которому пакет проходит на пути к получателю. Она присутствует во многих операционных системах. В основном эта программа используется для отладки проблем маршрутизации между узлами.

Карта сетевого интерфейса (Network Interface Card — NIC) представляет собой плату, которая позволяет осуществлять передачу и прием данных компьютерной системой в сети.

Тестовый пакет (keepalive) — это сообщение, отправляемое одним сетевым устройством, которое сигнализирует другому сетевому устройству о работоспособности виртуального канала между ними.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. Какое утверждение является правильным при базовом тестировании сети?

а) Следует последовательно переходить от одного уровня модели OSI к следующему.

б) Можно обследовать любой уровень модели OSI на выбор.

в) Следует начинать с уровня управления.

г) Необходимо вести поиск проблем модели OSI в случайном порядке.

2. Какой подход следует применять, начиная поиск неисправности в сети?

а) Сначала следует применять структурный подход.

б) Сначала можно применять случайный подход.

в) Сначала можно применять любой подход из известных.

г) Сначала можно применять метод проб и ошибок.

3. При поиске неисправностей в сети с какого уровня модели OSI следует начинать работу?

а) С первого.

б) Со второго.

в) С третьего.

г) С четвертого.

4. Если нужно проверить связь в сети, какую основную команду следует использовать?

а) **`telnet`**.

б) **`ping`**.

в) **debug**.

г) **traceroute**.

5. Если администратору сети нужно проверить программное обеспечение уровня приложений между станцией-отправителем и станцией-получателем, какую основную команду следует использовать?

а) **ping**.

б) **telnet**.

в) **debug**.

г) **traceroute**.

6. Администратор сети подозревает, что один из включенных в сеть маршрутизаторов посылает неправильную информацию о маршруте. Какой командой можно подтвердить или опровергнуть такое предположение?

а) `router(config)# show ip route`

б) `router# show ip route`

в) `router> show ip protocol`

г) `router(config-router)# show ip protocol`

7. Зачем следует выводить таблицу маршрутизации IP на консоль?

а) Чтобы задать расписание обновления маршрутизатора.

б) Чтобы определить адреса сетей-получателей и соответствующие им транзитные узлы.

в) Чтобы выяснить, откуда приходят дейтаграммы.

г) Чтобы задать для маршрутизатора параметры и фильтры.

8. Какую команду следует использовать для просмотра обновлений маршрутизации RIP при их отправлении и получении?

а) `router# show ip rip`

б) `router# debug ip protocols`

в) `router# debug ip rip`

г) `router# show ip rip update`

9. Динамический вывод команды **debug** осуществляется за счет системных ресурсов, что приводит к _____ перегрузке процессора.

а) Высокой.

б) Слабой.

в) Средней.

г) Максимальной.

10. Куда стандартно маршрутизатор направляет результаты работы команды **debug**?

а) На консоль.

б) На коммутатор.

в) На компьютер.

г) Пользователю.

11. Какой тип терминала предоставляет команда telnet?

а) Зарегистрированный.

б) Виртуальный.

в) Программный Cisco IOS.

г) Командный.

12. Что означает термин *ICMP*?

а) Параметр управляющих сообщений в сети Internet.

б) Протокол внутренних управляющих сообщений.

в) Протокол управляющих сообщений в сети Internet.

г) Характеристику управляющих сообщений в сети Internet.

13. Какие индикаторы надежного соединения присутствуют у большинства интерфейсов карт сетевого интерфейса?

а) Светодиод.

б) Катализатор.

в) Ответный.

г) Неактивный.

14. На каком уровне эталонной модели OSI используется служба telnet?

а) На первом.

б) На пятом.

в) На шестом.

г) На седьмом.

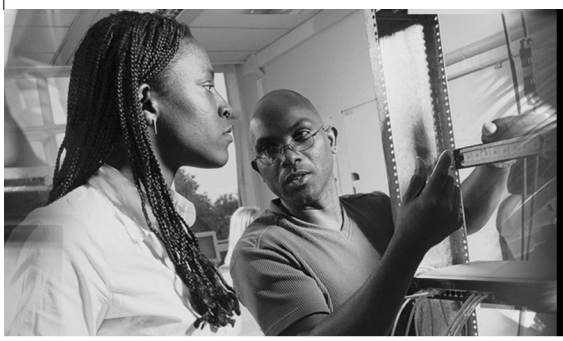
15. Если не включен протокол маршрутизации или невозможно определить IP-адрес, на каком уровне модели OSI администратор должен начинать поиск неисправности?

а) На первом.

б) На втором.

в) На третьем.

г) На четвертом.



ГЛАВА 21

Стек протоколов TCP/IP

В этой главе...

- описан механизм позитивных подтверждений и повторной передачи протокола TCP и его функции;
- описан механизм управления множественными сеансами обмена данными между станциями в протоколе TCP;
- дано определение портов, которые используются для служб и клиентов;
- приведен краткий список зарезервированных номеров портов;
- дано сравнение адресов MAC, IP и номеров портов;
- описаны основные функции протокола TCP;
- описана синхронизация и управление потоком в протоколе TCP;
- описана работа и процессы протокола пользовательских дейтаграмм (—UDP);
- указан нерегулируемый диапазон номеров портов и указывается, для чего они используются.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

протокол управления передачей, с. 909,
протокол передачи пользовательских дейтаграмм, с. 909,
атаки на отказ в обслуживании, с. 913,
управление потоком, с. 914,
механизм скользящего окна, с. 914,
зарезервированные порты, с. 923,
протокол IP, с. 926,
протокол ICMP, с. 926,
протокол ARP, с. 926,
протокол RARP, с. 926.

В этой главе описана работа стека протоколов TCP/IP, обеспечивающего связь между набором взаимосвязанных сетей и рассказано о компонентах стека, в частности, о протоколах передачи файлов, сообщений электронной почты, об удаленном входе в систему и о других практических применениях. В ней рассмотрены также надежные и ненадежные протоколы транспортного уровня, доставка дейтаграмм (пакетов) на сетевом уровне без установления соединения, а также механизм работы протокола преобразования адресов (Address Resolution Protocol — ARP) и обратного преобразования адресов (Reverse Address Resolution Protocol — RARP).

Обратите внимание на относящиеся к данной главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Дополнительная информация: стек протоколов TCP/IP

Набор протоколов TCP/IP разрабатывался в рамках исследований, которые проводило Управление перспективных исследовательских программ Министерства Обороны США (Defense Advanced Research Projects Agency — DARPA). Изначально он предназначался для обеспечения связи в пределах самого Управления. Позже стек протоколов TCP/IP был включен в комплект поставки операционной системы UNIX университета Беркли (Berkley). В наши дни набор протоколов TCP/IP является стандартом де-факто в межсетевой связи и служит механизмом транспорта в сети Internet, позволяя взаимодействовать миллионам компьютеров по всему миру. В этой главе основное внимание уделено стеку протоколов TCP/IP в силу нескольких причин, перечисленных ниже.

- Стек протоколов TCP/IP является всемирно доступным протоколом, который применяется на практике.
- Стек TCP/IP является полезным образцом для понимания других протоколов, поскольку содержит элементы, присущие многим технологиям.
- Набор протоколов TCP/IP важен, поскольку в маршрутизаторе он используется в качестве средства конфигурации.

Основная функция стека TCP/IP состоит в передаче информации между двумя сетевыми устройствами. При этом на нижних уровнях он очень похож на эталонную модель OSI и поддерживает все стандартные протоколы канального и физического уровней (рис. 21.1).

Наиболее тесная связь стека TCP/IP с моделью OSI наблюдается на седьмом уровне (уровне приложений), четвертом (транспортном) и третьем (сетевом). К этим уровням относятся протоколы разных типов, которые имеют разные назначения и выполняют различные функции, но все они отвечают за передачу информации. Уровни стека протоколов TCP/IP довольно хорошо соотносятся с уровнями модели OSI. Так, протокол TCP (на транспортном уровне или уровне обмена данными между двумя узлами) соответствует транспортному уровню, а уровень сети Internet — сетевому уровню модели OSI.

Набор протоколов TCP/IP позволяет осуществлять связь в пределах любого множества связанных сетей, одинаково хорошо подходит для связи локальных и распределенных сетей. К набору протоколов TCP/IP относятся не только спецификации и стандарты третьего и четвертого уровней (например, протоколы IP и TCP), но и спецификации, поддерживающие такие привычные приложения, как электронная почта, удаленный доступ к системе, эмуляция терминала и передача файлов.

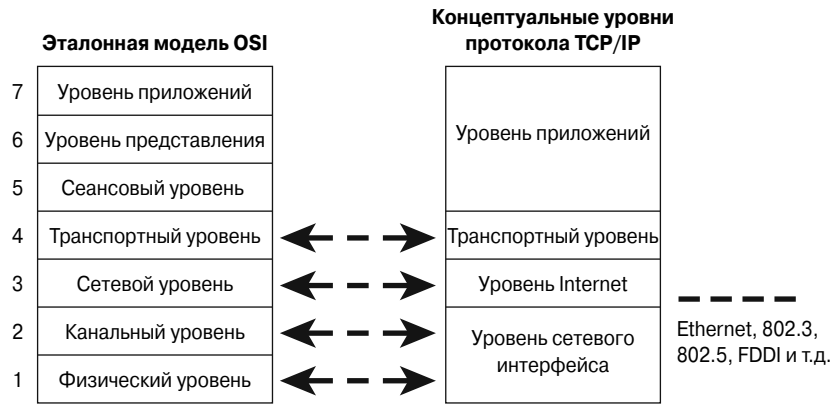


Рис. 21.1. Четырехуровневая модель стека TCP/IP

Стек протоколов TCP/IP и уровень приложений

- **Система доменных имен (Domain Name System — DNS**) используется в сети Internet для преобразования имен доменов и их публично доступных узлов в адреса IP. Такое преобразование относится к функциям транспортного уровня, поскольку оно обслуживает вышестоящий уровень (уровень приложений), а его обслуживает нижестоящий (межсетевой) уровень.
- **Служба имен сети Internet для Windows (Windows Internet Naming Service — WINS**) — представляет собой стандарт и протокол, разработанный корпорацией Microsoft для операционной системы Microsoft Windows NT, который автоматически устанавливает соответствие межу названиями рабочих станций NT и именами доменов сети Internet.
- **HOSTS** — это файл, создаваемый администраторами сети и хранящийся на серверах. Файл используется для статической привязки IP-адресов к символьным именам компьютеров.
- **Почтовый протокол (Post Office Protocol — POP3**) представляет собой открытый стандарт сети Internet для приема электронной почты с почтового сервера на компьютер пользователя. С помощью этого протокола пользователи могут получать сообщения из почтовых ящиков, используя различные уровни безопасности.
- **Простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP**) управляет передачей сообщений электронной почты в компьютерных сетях. Он не обеспечивает передачи каких-либо данных, кроме обычного текста.
- **Простой протокол сетевого управления** (**Simple Network Management Protocol — SNMP**) — это протокол, обеспечивающий средства управления и наблюдения за сетевыми устройствами, управление конфигурацией, сбором статистики, характеристиками и безопасностью.
- **Протокол передачи файлов (File Transfer Protocol — FTP)** представляет собой —надежную службу с установлением соединения, которая использует протокол TCP для передачи файлов между удаленными системами, поддерживающими протокол FTP. Она поддерживает двунаправленный обмен файлами в двоичном формате и формате ASCII (American standard code for information interchange — Американский стандартный код обмена информацией).
- **Простой протокол передачи файлов (Trivial File Transfer Protocol — TFTP**) — это служба без установления соединения, использующая протокол UDP. Протокол TFTP используется маршрутизатором для передачи файлов конфигурации и образов операционной системы IOS,

а также для передачи файлов между системами, поддерживающими протокол TFTP. Этот протокол используется в некоторых локальных сетях, поскольку в стабильном окружении он работает быстрее, чем протокол FTP.

- **Протокол передачи гипертекста (Hypertext Transfer Protocol — HTTP**) — это стандартный протокол сети Internet, поддерживающий обмен информацией как во Всемирной сети, так и в пределах внутренних сетей. Он поддерживает обмен различными типами файлов, в том числе текстами, графическими изображениями, звуковыми и видеофайлами. Данный протокол определяет порядок выдачи Web-браузерами запросов информации, отправляемых на Web-серверы.

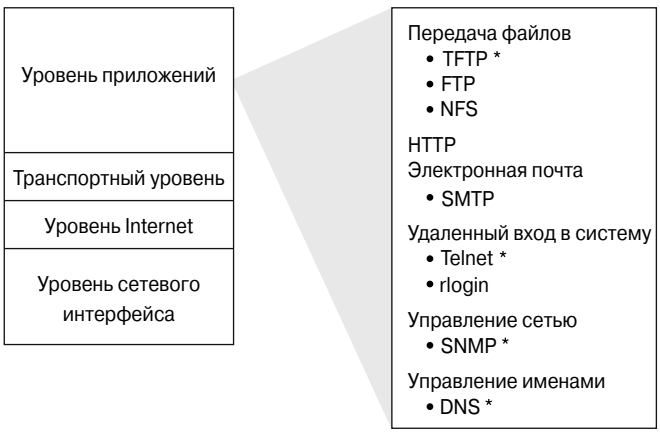


Рис. 21.2. Протоколы уровня приложений

В следующем списке перечислены некоторые полезные средства протоколов поиска и устранения неисправностей.

- **Telnet** — стандартный протокол эмуляции терминала, используемый клиентами для установки соединения удаленного терминала со службами Telnet-сервера. Этот протокол позволяет пользователям осуществлять дистанционное подключение к маршрутизаторам для ввода команд конфигурации.
- **Отправитель пакетов по сети Internet (Packet Internet Groper — команда ping)** определяет доступность удаленного сетевого устройства. В программе ping используются *эхо-запросы (echo request)* и *ответные сообщения (reply messages) протокола управляющих сообщений в сети Internet (Internet Control Message Protocol — ICMP)*.
- Во многих системах имеется **программа трассировки маршрута (traceroute program)**. Она аналогична программе или команде ping за тем исключением, что программа трассировки маршрута предоставляет больше информации, чем ping. Эта программа трассирует маршрут следования пакета к пункту назначения и применяется для отладки проблем маршрутизации.

Сетевому специалисту необходимо также знать несколько служебных программ операционной системы Windows.

- **NBTSTAT** — служебная программа, которая применяется для разрешения имен протокола NetBIOS, а также для удаления записей из кэш-памяти службы поиска имен.
- **NETSTAT** — служебная программа, предоставляющая информацию о статистике стека TCP/IP. Ее можно использовать для отслеживания состояния соединений стека TCP/IP и итоговых отчетов протоколов ICMP, TCP и UDP.

- **ipconfig и winipcfg** —служебные программы, применяемые для просмотра существующих настроек сети во всех *сетевых интерфейсных платах (Network Interface Card — NIC)* устройства. Их можно использовать для просмотра MAC-, IP-адреса, маски подсети, адреса шлюза, а также информации системы DNS и *протокола динамической конфигурации узла (Dynamic Host Configuration Protocol — DHCP)*.

Стек TCP/IP и транспортный уровень

В этом разделе описан *протокол управления передачей (Transmission Control Protocol — TCP)*, который в стеке TCP/IP является протоколом четвертого уровня. Протокол TCP является надежным протоколом с установлением соединения. Для обеспечения надежной доставки данных в нем используются синхронизация (synchronization), механизм скользящего окна (windowing) и согласование размера (window size), порядковые номера (sequence numbers) и подтверждения (acknowledgements — ACK).

Транспортный уровень позволяет устройству пользователя сегментировать данные от нескольких приложений высшего уровня для размещения в одном потоке данных четвертого уровня. Устройство-получатель может изменять компоновку сегментов приложений верхнего уровня. Поток данных четвертого уровня является логическим каналом между конечными точками сети и обеспечивает транспортное сообщение между узлом-отправителем и узлом-получателем. Иногда такой метод называют *сквозной передачей (end-to-end service)*. На транспортном уровне также предусмотрено два протокола (рис. 21.3).

- *Протокол TCP* — надежный протокол с установлением соединения, который обеспечивает управление потоком благодаря изменяемому размеру окна (sliding window). Надежность обеспечивается за счет использования порядковых номеров и подтверждений. Протокол TCP повторно передает все неподтвержденные данные и создает между приложениями конечных пользователей виртуальный канал. Преимущество протокола TCP состоит в том, что он обеспечивает гарантированную доставку сегментов данных.
- *Протокол UDP (протокол передачи пользовательских дейтаграмм — User Datagram Protocol)* является ненадежным протоколом без установления соединения, который отвечает за передачу сообщений, но не обеспечивает встроенной проверки доставки сегментов. Преимущество, которое присуще данному протоколу, — это скорость. Поскольку он не предусматривает использования подтверждений, по сети посылается меньше сигналов управления, что ускоряет передачу.

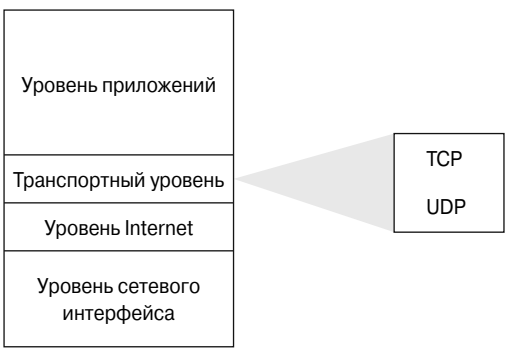


Рис. 21.3. Протоколы транспортного уровня

Формат сегментов в протоколах TCP и UDP

Как уже упоминалось выше, протокол TCP является протоколом с установлением соединения. Это означает, что конечные станции знают друг о друге и постоянно обмениваются информацией о соединении. Классический пример связи с установлением соединения, который, правда, взят не из области компьютерной техники, — это телефонный разговор между двумя людьми. Хороший пример диалога без установления соединения — —это работа обычной почты. Положив письмо в почтовый ящик, можно надеяться, что благодаря работе почтовой службы оно будет доставлено, но нельзя в этом быть уверенным. На рис. 21.4 изображен формат заголовка сегмента в протоколе TCP, определения полей которого описаны ниже.

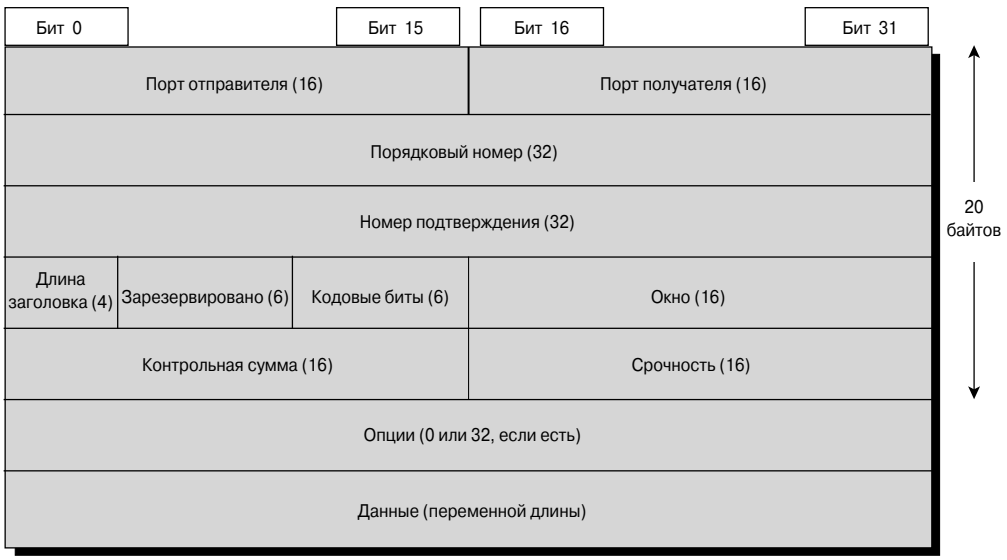


Рис. 21.4. Формат сегмента в протоколе TCP

- **Порт отправителя (Source port) —** номер порта отправителя данного сегмента.
- **Порт получателя (Destination port)** — номер порта получателя данного сегмента.
- **Порядковый номер (Sequence number)** — номер, используемый для обеспечения правильной последовательности размещения получаемых данных. Такой номер представляет собой первый байт поля данных пользователя.
- **Номер подтверждения (Acknowledgement number)** — следующий ожидаемый байт потока TCP; такой номер всегда равен порядковому номеру плюс единица и по нему можно восстановить номер последнего успешно доставленного байта.
- **Длина заголовка (Header length) —** количество 32-разрядных слов в заголовке.
- **Зарезервированное поле —** значения битов устанавливаются равными нулю.
- **Кодовые биты (Code bits)** — функции управления коммуникацией, например, установка и завершение сеанса.
- **Окно (Window)** — количество октетов, которые хочет послать отправитель.
- **Контрольная сумма (Checksum)** — вычисляется для полей заголовка и данных.
- **Срочность (Urgent)** — указатель конца срочных данных.

- **Опции (Options)** — на данное время определена одна опция: размер сегмента потока TCP.
- **Данные (Data)** — данные протокола верхнего уровня.

При использовании протокола UDP протоколы уровня приложений должны обеспечивать надежность, если это необходимо. В протоколе UDP не используются механизм скользящего окна и подтверждения. Он предназначен для приложений, которым не нужно собирать сегменты воедино. На рис. 21.5 изображен заголовок в протоколе UDP.

Порт отправителя (16)	Порт получателя (16)	Длина (16)	Контрольная сумма (16)	Данные (переменной длины)

Рис. 21.5. Формат заголовка в протоколе UDP

Принцип работы протокола TCP

Для межсетевой маршрутизации пакетов используются IP-адреса в заголовке пакета; по ним можно определить, в какой именно интерфейс должен быть перенаправлен пакет. Протокол IP не гарантирует доставки и не содержит механизмов, которые позволят убедиться в том, что пакет достиг получателя. За надежную доставку и регулирование потока данных от отправителя до пункта назначения отвечает транспортный уровень. Такая надежность обеспечивается за счет применения окон изменяемого размера (механизма скользящего окна), порядковых номеров и процесса синхронизации. Благодаря этому обеспечивается готовность и желание каждого узла начать связь, как показано на рис. 21.6.

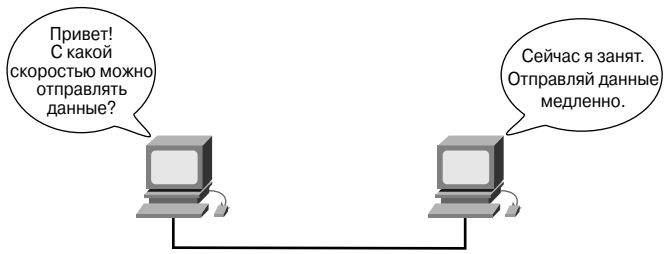


Рис. 21.6. Принцип работы протокола TCP

Чтобы усвоить основные понятия, которые связаны с надежностью и управлением потоком, можно представить себе двух людей, ведущих разговор. Сначала им нужно встретиться, возможно, пожать друг другу руки, чтобы подтвердить друг другу, что должен состояться разговор и передача информации. Если во время разговора и обмена информацией слушатель не расслышит какое-то слово, вероятно, он попросит человека повторить сказанное (для обеспечения надежности), потому что не разобрал слова (управление потоком). Транспортный уровень (четвертый уровень модели OSI) обеспечивает подобное описанному обслуживание для третьего уровня с помощью протокола TCP.

Синхронизация, или трехэтапное квитирование

Протокол TCP является протоколом с установлением соединения. Для установления виртуального соединения перед передачей данных два узла, устанавливающих связь, осуществляют процесс синхронизации. Процесс синхронизации обеспечивает готовность обеих сторон к передаче данных и позволяет им определить *первоначальные порядковые номера (Initial Sequence Numbers — ISN)*. Процесс согласования параметров связи называется *трехэтапным квитированием (three-way handshake)*.

Синхронизация осуществляется путем обмена пакетами с первоначальными порядковыми номерами и контрольным битом, который называется *SYN*, что означает *синхронизировать (synchronize)*. Пакеты, в которых содержится бит SYN, также называются *пакетами SYN*. Для успешного соединения требуется соответствующий механизм выбора первоначальной последовательности и несколько более сложный процесс квитирования для обмена первоначальными порядковыми номерами. Для синхронизации необходимо, чтобы каждая сторона отправила свой номер ISN и получила подтверждение и номер ISN от противоположной стороны соединения.

Каждая сторона должна получить номер ISN другой стороны и определенным образом послать подтверждение (ACK). Для установки виртуального соединения между двумя устройствами в ходе трехэтапного квитирования используется следующий процесс, состоящий из трех этапов.

1. Один узел (узел А) инициирует соединение и посылает пакет SYN с указанием его первоначального порядкового номера x. Определенный бит, установленный в поле кодовых битов заголовка сегмента в протоколе TCP, означает запрос соединения.
2. Получив пакет, узел Б записывает порядковый номер x, отвечает подтверждением x+1 и включает свой собственный первоначальный порядковый номер y. Номер x+1 в подтверждении означает, что узел получил все октеты до x включительно и теперь ожидает получения октета с порядковым номером x+1.
3. Узел-инициатор (А) отвечает простым подтверждением y+1 (порядковый номер второго узла плюс единица), сообщая о получении предыдущего подтверждения. На этом процесс установки соединения завершается.

Поскольку второй и третий этапы совмещаются в одном сообщении, этот обмен называется трехэтапным квитированием, или установлением соединения. Как показано на рис. 21.7, оба участника соединения синхронизируются согласно последовательности трехэтапного квитирования (установления соединения).

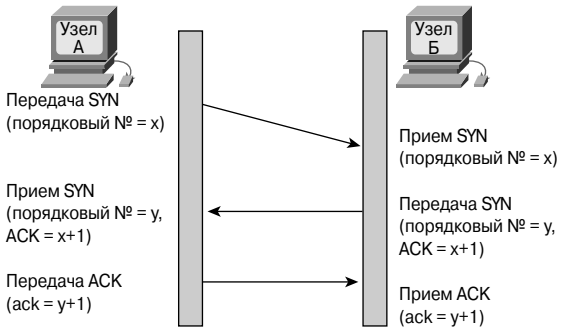


Рис. 21.7. Трехэтапное квитирование

Важно понимать, что порядковые номера относятся к началу связи между двумя устройствами. Порядковые номера служат для участвующих в коммуникации устройств опорными начальными номерами и дают возможность каждому узлу подтвердить (ACK) синхронизацию (SYN), а получателю убедиться в том, что отправитель отвечает на нужный запрос соединения.

Трехэтапное квитирование необходимо потому, что в протоколах на основе механизма TCP могут использоваться разные алгоритмы выбора номера ISN. Получателю первого номера ISN не может быть известно, является ли сегмент запоздавшим старым сегментом, если только он не сохранил последний порядковый номер предыдущего соединения, что не всегда возможно. Поэтому он должен выдать отправителю запрос на подтверждение сигнала SYN. В этот момент та или иная сторона может начать связь, а другая сторона может разорвать ее, поскольку протокол TCP является способом связи с взаимодействием равноправных узлов.

Интерактивная презентация: синхронизация в протоколе TCP
В этой презентации рассматривается механизм синхронизации в протоколе TCP.

Атаки на отказ в обслуживании

Атаки *на отказ в обслуживании (denial-of-service — DoS)* придуманы для отказа в обслуживании легальных узлов, пытающихся установить соединение. Такие атаки — обычный способ, используемый хакерами для блокирования нормальной реакции системы на внешние запросы. Одна из наиболее распространенных атак на отказ в обслуживании, которая происходит во время трехэтапного квитирования, называется лавинной рассылкой SYN-сообщений *(SYN flooding)*.

В процессе трехэтапного квитирования узел-инициатор отправляет пакет SYN. Пакет SYN, как и любой другой, содержит IP-адреса отправителя и получателя. Получатель использует такие адреса для отправки в ответ устройству-инициатору пакета подтверждения синхронизации SYN/ACK или сообщения об отказе в установлении связи.

Во время атаки с использованием лавинной рассылки сообщений хакер инициирует синхронизацию, но указывает ложный IP-адрес отправителя. Устройство-получатель отвечает несуществующему, недостижимому адресу IP и переходит в режим ожидания окончательного подтверждения (ACK) инициатора. Переведенный в режим ожидания запрос становится в очередь на соединение, или зону ожидания в памяти. Такое состояние ожидания требует от атакуемого устройства выделения на процесс ожидания системных ресурсов, например, памяти, до истечения времени установки соединения. Хакеры "заваливают" атакуемый узел такими фальшивыми запросами SYN, что приводит к использованию всех системных ресурсов на генерацию ответов и ожидание поддельных соединений и не дает возможности обрабатывать запросы обычных узлов.

Для защиты от рассмотренного выше класса атак администраторы могут уменьшить период ожидания соединения и увеличить размер очереди. Существует также программное обеспечение, позволяющее распознать данный тип нападения и принять защитные меры. На рис. 21.8 проиллюстрирована атака на отказ в обслуживании на этапе синхронизации.

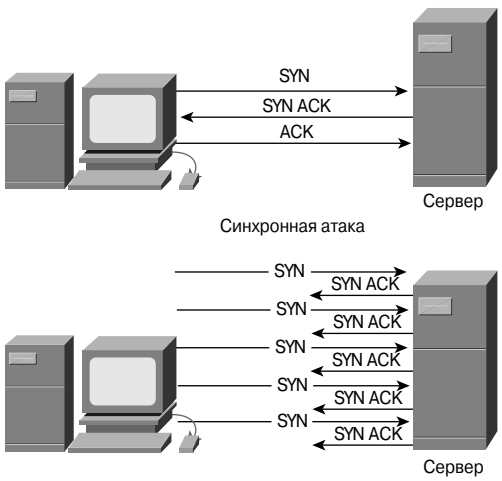


Рис. 21.8. Атака типа "отказ в обслуживании"

Механизм скользящего окна и размер окна

Часто возникает необходимость передать намного больше данных, чем можно послать в одном сегменте. В таком случае для обеспечения успешной передачи данные следует разбить на меньшие порции. За разбиение данных на сегменты отвечает протокол TCP. Этот процесс напоминает кормление ребенка. Поскольку большинство малышей не способно глотать огромные куски, мама часто делит еду на более мелкие кусочки, которые помещаются в ротик ребенка. Кроме того, получатель может не быть способен принимать данные с той же скоростью, с какой отправитель может отправлять их. Иногда различие в возможностях возникает из-за того, что

приемное устройство занято другими заданиями, в других случаях отправитель просто является более мощным устройством.

После сегментирования данные следует передать устройству-получателю. Одной из служб, предоставляемых протоколом TCP, является *управление потоком (flow control)*, которое регулирует количество данных, передаваемых в течение заданного периода. Процесс управления потоком использует *механизм скользящего окна (sliding window)*.

Размер окна определяет количество данных, которые могут быть переданы в один прием, до того, как должно быть получено подтверждение от получателя. После того как узел передаст все байты окна, он должен получить подтверждение о получении данных, а потом сможет отправлять следующие сообщения. Например, если размер окна равен единице, каждый отдельный сегмент должен быть подтвержден, прежде чем можно будет отправить следующий сегмент, как показано на рис. 21.9.

Для определения объема передаваемых данных в протоколе TCP используется *механизм скользящего окна* (sliding window). Изменяемый размер окна позволяет устройствам согласовать размер окна, благодаря чему они могут отправлять более одного байта без получения подтверждения, как показано на рис. 22.10. Изменяемый размер окна также позволяет устройству-получателю обращаться к отправителю. Если устройство-получатель не способно обрабатывать принимаемое количество данных, оно может сообщить о необходимости уменьшения количества пересылаемых данных. И наоборот, если устройство-получатель способно обработать больше данных, нежели поступает в данный момент, оно может выдать отправителю распоряжение увеличить количество пересылаемых данных.

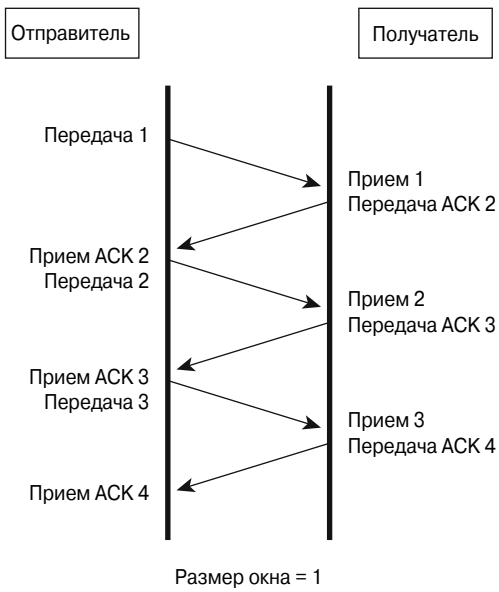


Рис. 21.9. Размер окна равен единице

Механизм скользящего окна работает следующим образом:

1. узел Б передает узлу А сообщение о том что он может работать с окном, размер которого равен шести (октетам или байтам);
2. узел А пересылает октеты (первый, второй и третий) узлу Б и перемещает окно вправо, сигнализируя таким образом, что он переслал три октета;
3. узел А *не* продолжит передавать данные до тех пор, пока не получит подтверждение (acknowledgment) от узла Б, что он получил все или некоторые из отправленных октетов;
4. узел Б, не дожидаясь получения всех шести октетов, после того как получит октет 3, переправит ожидаемое подтверждение 4 (expectational acknowledgment) узлу А;
5. после получения указанного сообщения узел А не должен ожидать подтверждения получения данных от узла Б; он продолжит пересылать данные до тех пор, пока размер окна не достигнет шести. Таким образом, узел А отправит октеты 4 и 5, как показано на рис. 21.12;
6. узел А получит и обработает подтверждение с номером 4 и передвинет границу окна (*slide*) таким образом, чтобы за один прием можно было отправить 6 октетов: три октета должны сопровождаться подтверждением плюс три октета, которые должны быть отправлены как можно быстрее.

Интерактивная презентация: механизм скользящего окна
В этой презентации необходимо расставить элементы в соответствии с выполняемыми функциями для механизма скользящего окна.

Порядковые номера сегментов

После того как протокол TCP разбивает данные на сегменты, эти сегменты передаются от отправителя получателю. Передача данных начинается после окончания процесса синхронизации и согласования размера окна, который определяет количество байтов, передаваемых в одном окне. По окончании передачи принятые сегменты данных должны быть скомпонованы. Поскольку никто не гарантирует поступления данных в порядке их передачи, в протоколе TCP эта проблема решается введением порядковых номеров. Протокол TCP присваивает всем передаваемым сегментам данных порядковые номера, благодаря которым получатель может правильно восстановить исходный порядок байтов. Порядковые номера указывают устройству-получателю правильный порядок, в котором следует расставлять принятые байты.

Порядковые номера также исполняют роль контрольных чисел, благодаря которым устройство-получатель может определить, все ли данные получены, и установить недостающие участки данных. В результате отправитель может повторно передать недостающие данные, как показано на рис. 21.11. Эта функция особо эффективна, поскольку отправитель должен повторно передавать только недостающие сегменты, а не весь массив данных.

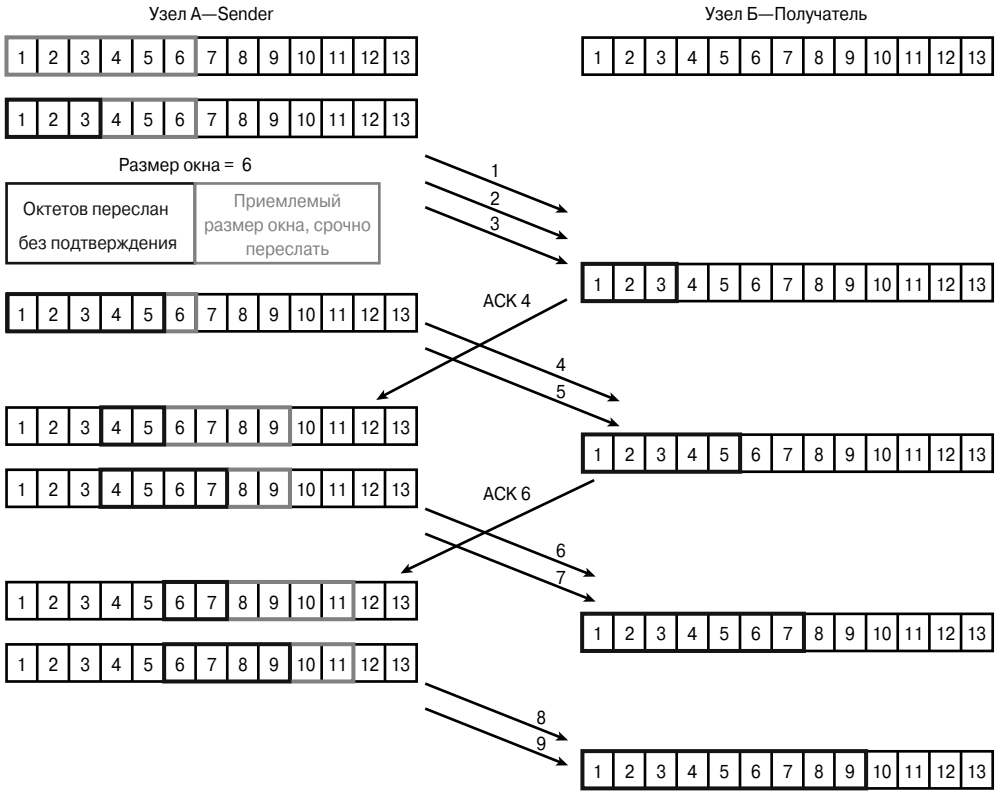


Рис. 21.10. Увеличение размера окна

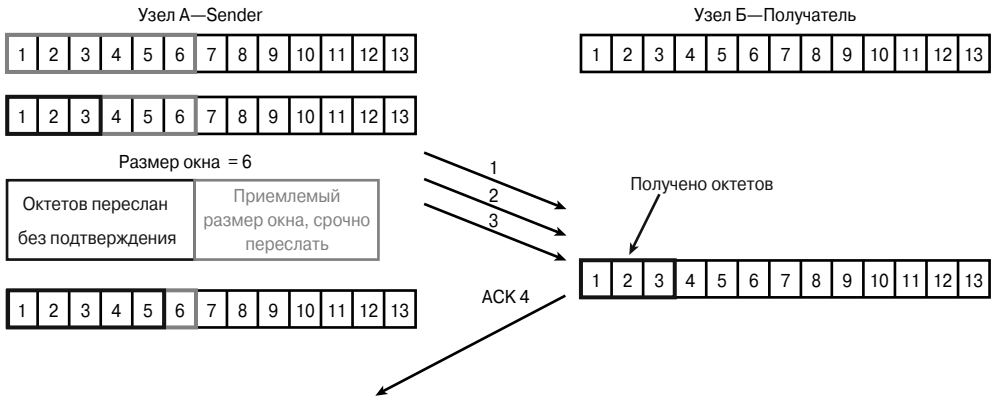


Рис. 21.11. Механизм скользящего окна

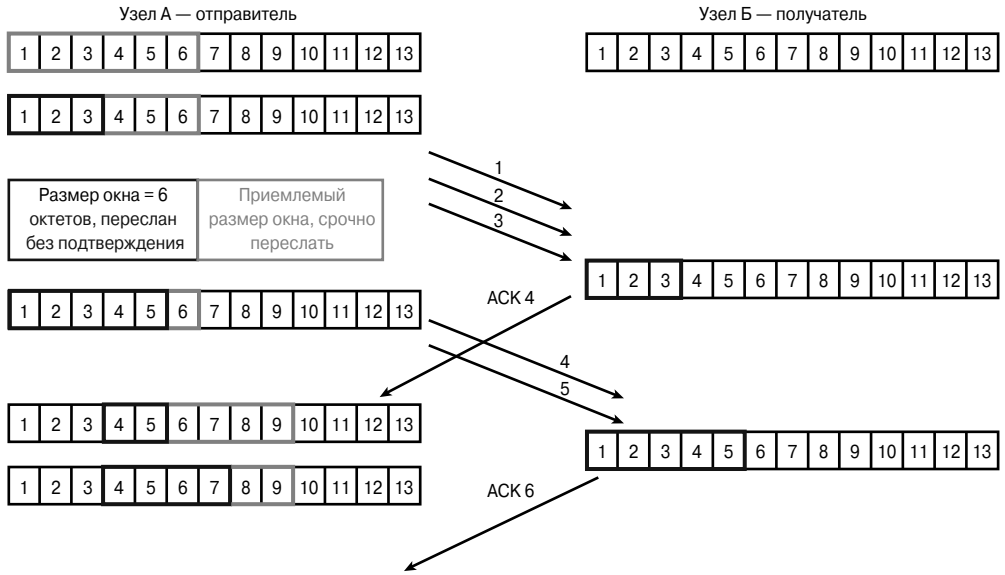


Рис. 21.12. Пример работы механизма скользящего окна

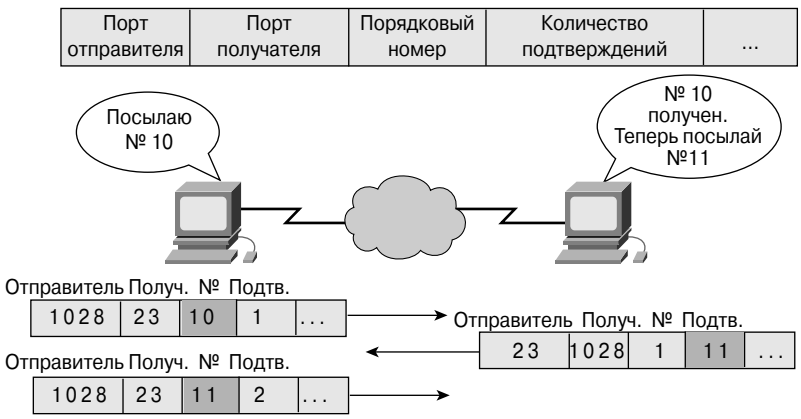


Рис. 21.13. Порядковые номера в подтверждениях

Перед передачей каждому сегменту протокола TCP присваивается номер. Выше в этой главе на рис. 21.4 был показан формат сегмента протокола TCP. Примечательно, что поле порядкового номера в формате сегмента следует за полем порта получателя. Станция-получатель посредством порядковых номеров протокола TCP компонует сегменты в целостное сообщение. Если в ряде порядковых номеров какой-либо из них отсутствует, этот сегмент передается повторно.

Подтверждение приема

Подтверждение применяется и для синхронизации, и в механизме изменяемого размера окон, и для восстановления последовательности данных. В сегменте протокола TCP поле порядкового номера следует за полем подтверждения, которое еще называется кодовым полем. В нем размещаются символы подтверждения (ACK) и синхронизации (SYN).

Одной из проблем, свойственных ненадежному протоколу IP, является отсутствие способа проверки, действительно ли пришли сегменты данных в пункт назначения. Поэтому последующие сегменты данных могут быть отправлены без уверенности в том, что предыдущие действительно получены. В протоколе TCP для управления потоком данных и подтверждения доставки данных используется подтверждение приема и повторная передача.

Подтверждение приема и повторная передача (Positive acknowledgement and retransmission — PAR) являются широко известными способами повышения надежности многих протоколов. Механизм PAR предусматривает, что при отправлении пакета отправитель запускает таймер и до отправки следующего пакета ждет подтверждения. Если установленное время истекает до получения отправителем подтверждения, он пересылает пакет повторно и перезапускает таймер. В протоколе TCP используется подтверждение с указанием ожидаемого сегмента, т.е. номер подтверждения относится к следующему ожидаемому октету.

Механизм скользящего окна представляет собой механизм управления потоком. Механизм скользящего окна предусматривает, что после передачи определенного объема данных устройство-отправитель должно получить подтверждение от устройства-получателя. Если размер окна равен трем, устройство-отправитель может отправить получателю три октета. После этого оно должно ждать подтверждения. Если устройство-получатель получит эти три октета, оно отправит устройству-отправителю подтверждение, после чего последнее может отправить еще три октета. Если устройство-отправитель не получит подтверждения, оно должно будет передать эти три октета повторно и снизить скорость передачи.

Практическое задание 21.1.6. Множественные сеансы между сетевыми узлами
В этом задании необходимо запустить службы HTTP на маршрутизаторах лабораторного комплекта устройств и проинспектировать мжножественные HTTP- и telnet-сеансы к ним на клиентском узле с помощью команды **`netstat`**.

Принцип работы протокола UDP

Стек TCP/IP содержит множество разных протоколов, каждый из которых предназначен для выполнения конкретной задачи. Протокол IP обеспечивает межсетевое сообщение третьего уровня без установления соединения. Протокол TCP гарантирует надежную передачу пакетов на четвертом уровне модели OSI с установлением соединения. Протокол UDP обеспечивает негарантированную передачу данных на четвертом уровне модели OSI без установления соединения.

И протокол TCP, и протокол UDP используют в качестве подчиненного протокола третьего уровня средства протокола IP. Кроме того, протоколы TCP и UDP используются разными протоколами уровня приложения. Протокол TCP обслуживает такие приложения, как FTP, HTTP, SMTP и DNS. Протокол UDP также относится к транспортному уровню и используется для приложений DNS, TFTP, SNMP и DHCP. На рис. 21.14 показано соотношение между протоколами прикладного, транспортного и сетевого уровней.

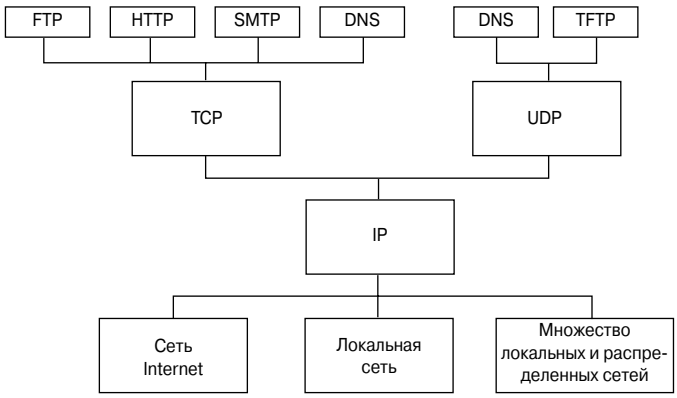


Рис. 21.14. Протоколы прикладного, транспортного и сетевого уровней

Протокол TCP должен использоваться там, где приложения должны гарантировать точную доставку пакетов, в нужной последовательности и без повторов. Однако при его использовании иногда возникает проблема, связанная с накладными расходами на обеспечение доставки пакетов. Не все приложения требуют гарантированной доставки пакета данных, поэтому некоторые используют более быстрый механизм без установления соединения, предоставляемый протоколом UDP. Стандарт UDP, описанный в документе RFC 768, представляет собой простой протокол, осуществляющий обмен сегментами без подтверждений и без гарантированной доставки. Например, для передачи файла конфигурации с сервера на маршрутизатор посредством сети Ethernet может использоваться протокол TFTP. В протоколе TFTP применяется эффективный транспортный протокол UDP, поскольку качество физических соединений обычно очень высоко и возможности подтверждения и повторной передачи, предусмотренные протоколом TCP, не нужны. Например, при передаче файла образа операционной системы IOS на маршрутизатор посредством протокола TFTP в задачу маршрутизатора входит пересчет контрольной суммы после того, как файл передан целиком; такая контрольная сумма позволяет убедиться в том, что файл был доставлен неповрежденным. Если файл был доставлен с ошибками, не целиком и т.п., то повторную его передачу можно инициировать только вручную.

В протоколе UDP не используется ни механизм скользящего окна, ни подтверждения. Поэтому средства уровня приложений должны предусматривать обнаружение ошибок. Протокол UDP предназначен для приложений, которые не должны составлять воедино последовательности сегментов.

Выше в этой главе на рис. 21.5 был показан формат сегмента в протоколе UDP. Поле порта-отправителя (*Source Port*) является необязательным и используется только при необходимости возврата информации узлу-отправителю. В поле порта-получателя (*Destination Port*) указывается приложение, которому протокол UDP должен передать данные. В поле порта-получателя (*Destination Port*) запроса системы DNS с узла на сервер DNS содержится число 53 — номер порта протокола UDP для системы DNS. В поле длины (*Length*) указывается количество октетов в сегменте протокола UDP. Контрольная сумма (*Checksum*) в протоколе UDP необязательна, но ею следует пользоваться для контроля целостности данных при передаче. С целью передачи по сети протокол UDP инкапсулируется в пакет IP.

После доставки сегмента по назначенному IP-адресу должен существовать механизм, позволяющий узлу-получателю определить целевое приложение сегмента. Именно для этого используются порты. Если узел использует службы TFTP и DNS, он должен быть в состоянии определить, какая служба нужна для полученных сегментов. Приложение, для которого доставлен сегмент протокола UDP, задается полем порта получателя (*Destination Port*) в заголовке протокола UDP.

Порты транспортного уровня

Порты транспортного уровня — это шестнадцатиразрядные числа, необходимые для идентификации конечных точек соединения. В результате такого метода адресации конкретное соединение сети идентифицируется последовательностью четырех чисел (адрес отправителя, порт отправителя, адрес получателя, порт получателя). В принципе, такая схема позволяет создавать между любыми двумя узлами уникальные соединения протокола UDP. И все же механизм UDP является ненадежным протоколом без установления соединения. Для поддержки приложений с установлением соединения, для которых требуются надежная передача потоков данных с восстановлением последовательности передаваемых сегментов, применяется протокол TCP. Как и протокол UDP, для определения конечных точек соединения протокол TCP использует порты.

Множественные сеансы связи между узлами

В наше время по сети одновременно перемещаются тысячи пакетов, предоставляющих сотни различных служб. Во многих случаях серверы поддерживают одновременно несколько разных служб, что порождает уникальные возможности адресации пакетов. Допустим, например, что сервер одновременно выполняет службы SMTP и World Wide Web (электронная почта и гипертекстовые документы). В таком случае клиент не может создать пакет, предназначенный для IP-адреса сервера, пользуясь одним лишь протоколом TCP, потому что протокол TCP выполняет функцию протокола транспортного уровня как для службы SMTP, так и для службы

World Wide Web. Чтобы обеспечить получение пакета соответствующей службой сервера, сеансу связи между узлами должен соответствовать номер порта. Если бы не было возможности разграничивать разные сеансы, клиент не смог бы одновременно посылать электронную почту и просматривать Web-страницы, используя один сервер. Именно поэтому необходим способ разграничения транспортных потоков.

Узлы, использующие набор протоколов TCP/IP, на транспортном уровне сопоставляют порты с определенными приложениями. Для поддержки разных сеансов, одновременно проходящих в сети, используются номера портов. Такие номера нужны при связи узла с сервером, предоставляющим разные службы. Для передачи информации на верхние уровни и протокол TCP, и протокол UDP используют номера портов. На рис. 21.15 показаны примеры номеров портов в протоколах TCP и UDP.

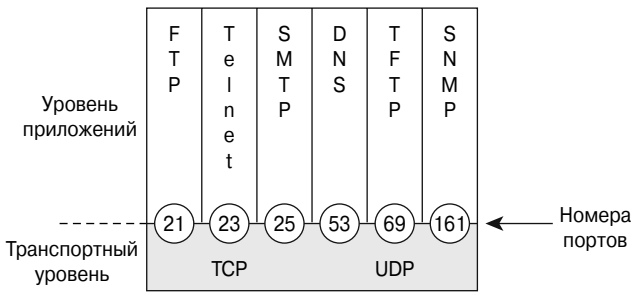


Рис. 21.15. Номера портов в протоколах TCP и UDP

Разработчики прикладного программного обеспечения договорились использовать зарезервированные номера портов, определенные в документе RFC 1700. Например, для любых сеансов, связанных с приложением FTP, используется стандартный номер порта 21. Сеансам, в которых не участвуют приложения с номерами зарезервированных портов, назначаются номера портов, случайно выбранные из некоторого диапазона. Эти номера портов служат в сегменте протокола TCP адресами отправителя и получателя. В табл. 21.1 перечислены зарезервированные номера портов в протоколах TCP и UDP.

Таблица 21.1. Зарезервированные номера портов в протоколах TCP и UDP

Десятичный номер	Дескриптор	Описание
0	-	Зарезервирован
1-4	-	Не присвоены
5	rje	Дистанционный ввод заданий *(Remote Job Entry — RJE)*
7	echo	Эхо
9	discard	Уничтожение пакетов
11	users	Активные пользователи
13	daytime	Время

Окончание табл. 21.1

Десятичный номер	Дескриптор	Описание
15	netstat	Кто есть, или состояние сети
17	quote	Цитата дня
19	chargen	Генератор символов
20	ftp-data	Служба FTP (данные)
21	ftp	Служба FTP
23	telnet	Соединение терминала
25	smtp	SMTP
37	time	Время
39	rlp	Протокол размещения ресурсов *(Resource Location Protocol — RLP)*
42	nameserver	Сервер имен узлов *(Host name server)*
43	nickname	Кто есть кто
53	domain	Служба DNS
67	bootps	Сервер удаленной загрузки
68	bootpc	Клиент удаленной загрузки
69	tftp	Служба TFTP
75	-	Любая конфиденциальная коммутируемая служба
77	-	Любая конфиденциальная служба терминала RJE
79	finger	Служба информации об активных пользователях
80	http	Протокол передачи гипертекста
123	ntp	Синхронизирующий сетевой протокол *(Network Time Protocol — NTP)*
133-159	-	Не присвоены
160-223	-	Зарезервированы
224-241	-	Не присвоены
242-255	-	Не присвоены

Номера портов разбиты на такие предопределенные диапазоны:

- номера ниже 255-ти — предназначены для открытых приложений и являются зарезервированными;
- номера от 255-ти до 1023-х предназначены для коммерческого использования компаниями и являются зарегистрированными;
- номера выше 1023-х — не регламентируются и носят название динамических, или частных.

Конечные системы используют номера портов для выбора соответствующих приложений. Как показано на рис. 21.16, номер исходного порта отправителя (1028) динамически назначается узлом отправителя. Обычно такой номер порта превышает величину 1023. Агентство по выделению портов сети Internet *(Internet Assigned Port Authority — IAPA)* контролирует номера портов в пределах от нуля до 1023-х.

Порты, предназначенные для служб

Для осуществления связи службам, исполняемым на узлах, должны быть присвоены номера портов. Когда удаленный узел делает попытку соединения со службой, ожидается, что эта служба работает с определенными протоколами транспортного уровня и на определенных портах. Некоторые порты, определенные в документе RFC 1700, называются *зарезервированными (well-known ports)*. Эти порты зарезервированы как в протоколе TCP, так и в протоколе UDP.

Зарезервированные порты могут определять приложения, выполняемые над протоколами транспортного уровня. Например, сервер, использующий службу FTP, перенаправляет от клиентов своему приложению FTP соединения TCP, используя порты 20 и 21. Таким образом, этот сервер может точно определить, какую службу требует клиент. Для правильного определения службы, которой следует перенаправить запрос клиента на обслуживание, и в протоколе TCP, и в протоколе UDP используются номера портов.

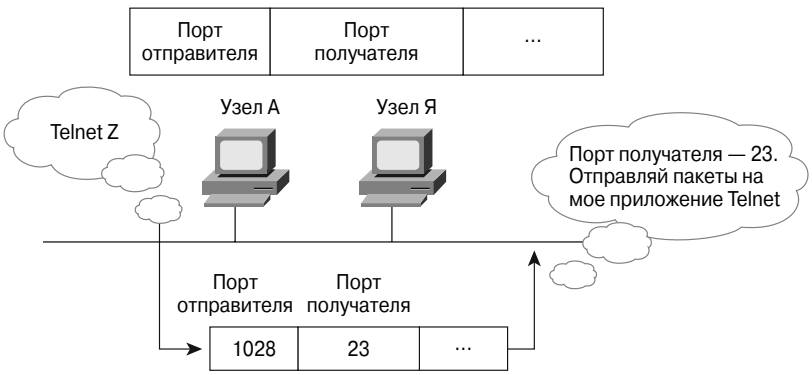


Рис. 21.16. Порты отправителей и получателей

Порты, предназначенные для клиентов

Для соединения клиента со службой на сервере должны быть указаны порты отправителя и получателя. В сегментах протоколов TCP и UDP есть соответствующие поля. Порты получателей, или порты, предназначенные для служб, обычно назначаются из числа зарезервированных портов. Порты-отправители, устанавливаемые клиентом, определяются динамически.

В общем случае клиент определяет порт-отправитель, назначая случайное число, превышающее 1023. Например, при попытке связаться с Web-сервером клиент использует протокол TCP и определяет порт получателя как порт с номером 80, выбирает порт отправителя, равный 1045-ти. Поступив на сервер, пакет попадает на транспортный уровень и в конечном счете передается Web-службе, которая связана с портом 80. Web-сервер отвечает на запрос клиента сегментом с портом-отправителем 80 и портом получателя 1045. Таким образом, чтобы определить, с каким процессом связан конкретный сегмент, клиенты и серверы используют порты. Если клиент открыл два сеанса с помощью браузера на разных серверах, в обоих сеансах используется порт получателя с номером 80. Но порт-отправителя для каждого сеанса будет другой: например, 1045 и 1048. Такое различие портов позволяет клиенту вести два разных сеанса.

Нумерация портов и зарезервированные порты

Номера портов в заголовках сегментов протоколов TCP и UDP выражаются двумя байтами. Эта шестнадцатиразрядная величина дает возможность использовать нумерацию портов в пределах от нуля до 65 535. Номера портов делятся на три категории:

- зарезервированные порты (well-known);
- зарегистрированные порты (registered);
- динамические, или частные, порты (dynamic, или private).

Первые 1023 порта относятся к зарезервированным портам. Как уже было сказано, они используются для зарезервированных служб сети Internet, например, FTP, Telnet, DNS и HTTP. Зарегистрированные порты, определяющие такие службы, как *Cisco-Net-Mgmt* и *протокол доступа к календарю (Calendar Access Protocol)*, размещены по адресам от 1024-х до 49 151. И, наконец, порты, имеющие номера от 49 152 и до 65 515, определяются как динамические, или конфиденциальные.

Пример множественных сеансов между узлами

Для ведения множества сеансов, которые могут происходить между узлами, используются номера портов. Номер порта и сетевой адрес образуют так называемый сокет (socket). Пара сокетов, каждый из которых соответствует своему узлу, образует уникальное соединение. Например, через порт 23 узел может вести сеанс Telnet и в то же время выходить в сеть, используя порт 80. IP-адрес узла совпадает с MAC-адресом, потому что пакеты доставляются с одного и того же узла. Но номера портов разные, т.к. используются разные протоколы и, соответственно, разные сокеты.

Практическое задание 21.2.5. Множественные сеансы между узлами и зарезервированные номера портов

В этом задании следует с помощью команды **`netstat`** проследить использование номеров зарезервированных портов множества сеансов на одном узле.

Сравнение MAC-, IP-адресов и номеров портов

MAC-, IP-адреса и номера портов часто путают. Но этой путаницы можно избежать, если интерпретировать адреса в соответствии с эталонной моделью взаимодействия открытых систем (моделью OSI). Номера портов расположены на транспортном уровне и обслуживаются сетевым уровнем. Сетевой уровень предоставляет логический адрес, т.е. адрес IP. После этого он обслуживается канальным уровнем, который назначает физический адрес, т.е. адрес MAC.

В качестве неплохого примера к разным типам адресов-идентификаторов можно привести обычное письмо. Адрес на конверте содержит имя, название улицы, город и страну. Такой адрес может быть сравнен с портом, MAC- и IP-адресами сетевых устройств, которые участвуют в передаче данных. Имя получателя письма на конверте можно сравнить с номером порта, название улицы будет соответствовать MAC-адресу, а город и страна — IP-адресу. В одну и ту же страну, один и тот же город и на одну и ту же улицу может быть отправлено множество писем одновременно, однако на них будут написаны разные фамилии. Например, в один и тот же дом могут прийти два письма: Ивану Петрову и Марии Петровой. В таком случае фамилии будут аналогом разных портов на одной и той же клиентской рабочей станции (в аналогии — квартире), и доставка писем будет соответствовать множественным сеансам на одном узле.

Дополнительная информация: набор протоколов TCP/IP и Internet-уровень

Протокол сети Internet (IP-протокол) является протоколом третьего уровня и отвечает за схему адресации, которая позволяет осуществлять во внутренних сетях и в сети Internet надежную маршрутизацию пакетов к адресатам. С помощью информации об IP-адресе в заголовке IP-пакетов маршрутизаторы определяют, на какой интерфейс следует направить пакет, чтобы доставить его по назначению. Протокол IP не предоставляет никаких служб, которые могли бы обеспечить доставку пакета адресату. Он считается ненадежным протоколом без установления соединения. Пакеты могут теряться по дороге, приходить в другой последовательности, передаваться быстрее, чем получатель способен принимать их. В протоколе IP не предусмотрены способы противодействия этим и другим проблемам, возникающим при доставке.

Internet-уровень стека TCP/IP полностью соответствует сетевому уровню модели OSI. Сетевой уровень отвечает за доставку пакетов по сети с помощью программной адресации.

Как показано на рис. 21.17, на Internet-уровне стека TCP/IP, который соответствует сетевому уровню модели OSI, работают несколько протоколов:

- *протокол IP* — обеспечивает адресацию в сети, он является негарантированным протоколом доставки дейтаграмм без установления соединения. Этот протокол не зависит от содержания дейтаграмм, но ищет возможности доставить дейтаграммы по назначению;
- *протокол ICMP* — обеспечивает функции управления и доставки информационных сообщений;
- *протокол ARP* — служит для определения адресов канального уровня (MAC) при известных адресах IP;
- *протокол RARP* — определяет сетевые адреса (IP) при известных адресах канального уровня (MAC).

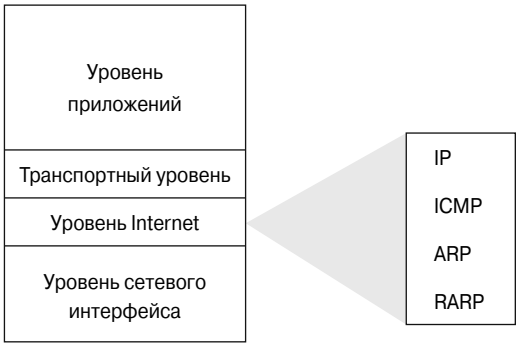


Рис. 21.17. Сетевой уровень модели TCP/IP

Механизм работы протокола ARP

Протокол ARP используется для сопоставления адреса MAC на подуровне известному адресу IP. При этом сопоставлении учитывается соединение, поскольку аппаратное обеспечение канального уровня не может принять фрейм, в котором адрес MAC не совпадает с адресом MAC этого аппаратного обеспечения (или не является *широковещательным адресом MAC — broadcast MAC address*). Чтобы определить адрес MAC для дейтаграммы, выполняется обращение к таблице, которая называется *кэшем преобразования ARP (ARP cache)*. На каждом узле сети (на маршрутизаторах, рабочих станциях, серверах и пр.) есть кэш ARP. Если в этой таблице адреса нет, ARP рассылает широковещательное сообщение о поиске станции назначения, которое получает каждая станция в сети. Если узел, подающий запрос, и узел назначения пользуются одной и той же средой передачи или кабелем, такой поиск называют *местным преобразованием ARP (local ARP)*. Как показано на рис. 21.18 перед преобразованием адресов необходимо обратиться к маске подсети. Тогда с помощью маски можно определить, находятся ли узлы в той же подсети.

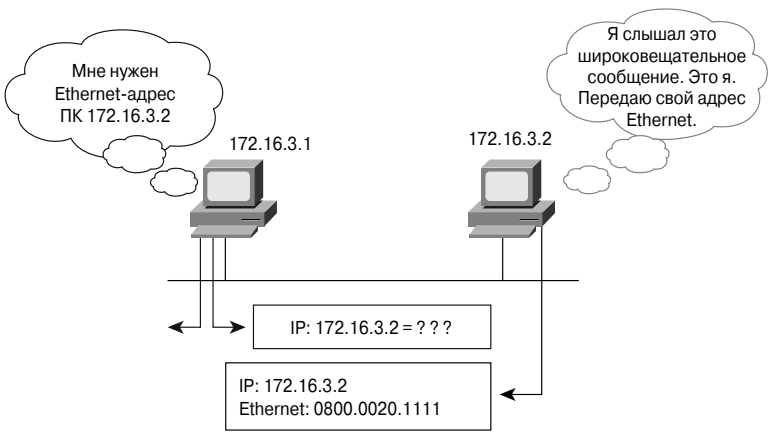


Рис. 21.18. Сетевой уровень модели OSI

Протокол RARP является протоколом стека TCP/IP, который позволяет преобразовать физический адрес (MAC), например, адрес в сети Ethernet, в IP-адрес. Следовательно, этот протокол выполняет функцию, обратную той, что выполняет протокол ARP. Таким узлам, как

бездисковые рабочие станции, в процессе загрузки часто могут быть известны только адреса их собственных аппаратных интерфейсов, или MAC-адреса. Свои IP-адреса они должны получать от внешнего источника. Обычно эту проблему с помощью протокола RARP разрешает сервер RARP.

Резюме

В этой главе были рассмотрены следующие ключевые понятия и определения:

- TCP представляет собой протокол транспортного уровня с установлением соединения. Он обеспечивает необходимый уровень качества обслуживания для процессов ненадежного протокола IP;
- TCP обеспечивает надежность, управление потоками и установление виртуального канала;
- для установления синхронизированного соединения между узлами в протоколе TCP используется трехэтапное квитирование;
- для динамического управления потоками данных предусмотрен изменяемый размер окна, реализуемый посредством механизма скользящего окна;
- восстановление узлом-получателем последовательности данных обеспечивается порядковыми номерами;
- UDP представляет собой протокол транспортного уровня без установления соединения;
- для распознавания приложений высшего уровня в протоколах UDP и TCP используются номера портов.

Для закрепления материала, изложенного в этой главе, воспользуйтесь относящимися к ней мультимедийными материалами, которые находятся на компакт-диске, предоставленном вместе с книгой.

Ключевые термины

Механизм скользящего окна (windowing) управляет потоками данных. Получатель сообщает отправителю, какого размера окно (сколько октетов) он способен обработать в данный момент. После этого отправитель отправляет получателю указанное количество октетов.

Отказ в обслуживании (DoS —denial-of-service) представляет собой тип сетевой атаки, призванной заблокировать сеть, завалив ее потоком бесполезного трафика.

Зарезервированные порты (well-known ports) определены документом RFC 1700 и зарезервированы и в протоколе TCP, и в протоколе UDP. Зарезервированные порты могут определять приложения, выполняемые над протоколами транспортного уровня.

Протокол ARP (Address Resolution Protocol — протокол преобразования адресов) — представляет собой протокол сети Internet, используемый для преобразования IP-адресов в MAC-адреса.

Протокол RARP (Reverse Address Resolution Protocol — протокол обратного преобразования адресов) представляет собой — протокол в стеке TCP/IP, предоставляющий возможность по известным MAC-адресам найти IP-адреса.

Протокол TCP (Transmission Control Protocol — протокол управления передачей) — протокол транспортного уровня с установлением соединения, который обеспечивает надежную дуплексную передачу. Протокол TCP относится к стеку TCP/IP.

Протокол UDP (User Datagram Protocol — протокол пользовательских дейтаграмм) — протокол транспортного уровня без установления соединения, относящийся к стеку TCP/IP. Протокол UDP представляет собой простой протокол обмена дейтаграммами без подтверждения, не предоставляющий гарантии доставки. При его использовании обработку ошибок и повторную передачу должны выполнять другие протоколы или, в частности, средства уровня приложений.

Управление потоками (flow control) — представляет собой процесс регулирования потоков данных между двумя устройствами, в результате которого устройство-получатель способно обработать все входящие данные.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, “Ответы на контрольные вопросы”.

1. Какое из приведенных ниже описаний дает представление о стеке протоколов TCP/IP?

   а) Это набор протоколов, который можно использовать для установления связи через любое количество взаимосвязанных сетей.

   б) Это набор протоколов, который позволяет связывать локальные вычислительные сети в распределенные вычислительные сети.

   в) Это набор протоколов, который предусматривает передачу данных по множеству сетей.

   г) Это набор протоколов, который позволяет взаимосвязанным сетям использовать различные устройства в распределенном режиме.

2. Какой из перечисленных протоколов относится к транспортному уровню?

   а) UCP.

   б) UDP.

   в) TDP.

   г) TDC.

3. Для чего нужны номера портов?

   а) Они позволяют отслеживать различные сеансы связи, которые одновременно осуществляются в сети.

б) Они используются отправителями для поддержания порядка в системе и для выбора нужного приложения.

в) Они используются конечными системами для динамического закрепления конечных пользователей за конкретными сеансами в зависимости от применяемых ими приложений.

г) Отправители генерируют их для прогнозирования адресов получателей.

4. Какое из приведенных ниже описаний дает представление о протоколе UDP?

а) Протокол, который выдает подтверждения как на некорректные, так и на правильные дейтаграммы.

б) Протокол, который обнаруживает ошибки и выдает отправителю запрос на повторную передачу.

в) Протокол, который обрабатывает дейтаграммы и при необходимости выдает запрос на повторную передачу.

г) Протокол, который осуществляет обмен дейтаграммами без подтверждения и без гарантии доставки.

5. Какой из уровней отвечает за передачу файлов, сообщений электронной почты, удаленный вход в систему и управление сетью?

а) Транспортный.

б) Уровень приложений.

в) Уровень Internet.

г) Сетевой.

6. Для чего нужны трехэтапное квитирование, процедура установления соединения и порядковые номера?

а) Чтобы обеспечить восстановление данных в случае возникновения проблем после их пересылки.

б) Чтобы определить, какое количество данных может одновременно принять станция-получатель.

в) Для обеспечения эффективного использования полосы пропускания.

г) Для преобразования двоичных ping-откликов в информацию верхних уровней.

7. Для чего служит механизм скользящего окна?

а) Он увеличивает размер окна, чтобы одновременно можно было передать большее количество данных и тем самым более эффективно использовать полосу пропускания.

б) Для приема данных размер окна изменяется по размеру каждой части дейтаграммы, что позволяет более эффективно использовать полосу пропускания.

в) Он предоставляет возможность устанавливать размер окна динамически в процессе развития сеанса протокола TCP, что позволяет более эффективно использовать полосу пропускания.

г) Он ограничивает входящие данные так, что каждый сегмент приходится пересылать по одному, а это является неэффективным способом использования полосы пропускания.

8. Какие протоколы используются сегментами протокола UDP для обеспечения надежности?

а) Протоколы сетевого уровня.

б) Протоколы уровня приложений.

в) Протоколы Internet-уровня.

г) Протоколы управления передачей.

9. Какое из приведенных ниже описаний относится к размеру окна?

а) Максимальный размер окна — это параметр, с которым программное обеспечение все еще способно быстро обрабатывать данные.

б) Размер окна — это число сообщений или байтов, которые могут быть переданы во время ожидания подтверждения.

в) Этот параметр описывает размер окна при пиковой нагрузке, который следует установить заблаговременно, чтобы была возможна передача данных.

г) Этот параметр описывает размер окна, открываемого на мониторе, который не всегда совпадает с размером монитора.

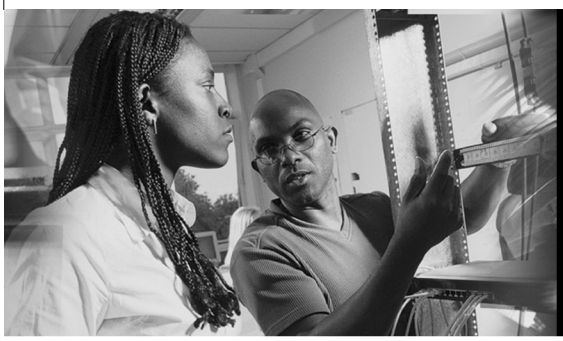
10. Какую роль играет протокол ARP?

а) Завершает исследование адреса назначения на третьем уровне.

б) Используется для сопоставления IP-адресов с неизвестными MAC-адресами.

в) Используется для сопоставления неизвестных IP-адресов с MAC-адресами.

г) Рассылает широковещательное сообщение для поиска IP-адреса маршрутизатора.



ГЛАВА 22

Списки управления доступом

В этой главе...

- описано назначение списков управления доступом и рассказано о цели их применения;
- описано, каким образом списки управления доступом обеспечивают безопасность и средства контроля сети;
- объясняется, как следует рассчитывать шаблоны масок и как их использовать;
- описано, как создать и использовать стандартные, расширенные и именованные списки управления доступом, перечислены отличия между ними и приведены примеры типичных сценариев, в которых каждый тип списка может быть использован;
- рассказывается, как списки управления доступом связаны со структурами на основе брандмауэров.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

список управления доступом, с. 934,

установка пакетов в очередь, с. 937,

битовая корзина, с. 939,

стандартный список управления доступом, с. 948,

расширенный список управления доступом, с. 952,

именованный список управления доступом, с. 959,

брандмауэр, с. 963,

внешний маршрутизатор, с. 964,

внутренний маршрутизатор, с. 964,

граничный маршрутизатор, с. 965.

Прочитав эту главу, вы научитесь использовать стандартные и расширенные списки управления доступом, которые служат средством контроля трафика, и узнаете о том, как списки управления доступом могут применяться для обеспечения безопасности.

В главе приведены основные принципы использования списков управления доступом, а также рассмотрены команды и конфигурации, необходимые для их создания. В последней части главы приведены примеры стандартных и расширенных списков управления доступом и описано, как их применять на интерфейсах маршрутизаторов.

Обратите внимание на относящиеся к данной главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Введение в списки управления доступом

Сетевой администратор должен уметь запрещать несанкционированный доступ к сети и в то же время обязан обеспечить доступ к сети авторизированных пользователей. Несмотря на то что средства безопасности, такие, как пароли, средства установления обратного вызова и физические устройства безопасности, достаточно полезны, им часто не хватает гибкости при фильтрации потока данных и специализированных управляющих средств, которые чаще всего предпочитают администраторы. Например, бывают ситуации, когда сетевой администратор готов предоставить пользователям локальной сети выход в сеть Internet, но при этом не хочет разрешать пользователям сети Internet, находящимся вне такой локальной сети, входить в сеть предприятия средствами протокола telnet.

ВНИМАНИЕ!

Следует помнить, что списки ACL интенсивно используют ресурсы центрального процессора (CPU) маршрутизатора. Каждый[1] поступающий на устройство пакет должен быть обработан центральным процессором при использовании списков доступа.

Маршрутизаторы предоставляют администраторам основные возможности фильтрации, такие, как блокирование потока данных из сети Internet с использованием *списков управления доступом (Access Control List — ACL)*. Список управления доступом представляет собой последовательный набор разрешающих или запрещающих директив, которые относятся к адресам или протоколам верхнего уровня.

В процессе чтения этой главы следует помнить, что правила списка ACL, которые принадлежат одному и тому же списку управления доступом, всегда содержат

[1] *В действительности, каждый ли пакет будет обработан с участием центрального процессора или без него, зависит от нескольких факторов: используемого метода перенаправления пакетов, типа списка управления доступом и конкретного аппаратного решения. — Прим. ред.*

один и тот же номер-идентификатор списка. Например, представим себе такой набор списков и правил:

- список управления доступом 1
  - правило списка ACL 1,
  - правило списка ACL 1,
  - правило списка ACL 1,
  - правило списка ACL 1;
- список управления доступом 2
  - правило списка ACL 2,
  - правило списка ACL 2,
  - правило списка ACL 2,
  - правило списка ACL 2,
  - правило списка ACL 2;
- список управления доступом 3
  - правило списка ACL 3,
  - правило списка ACL 3,
  - правило списка ACL 3.

В приведенной структуре списков ACL правило, номер которого совпадает с номером списка, относится к определенному нумерованному списку. Сами правила выполняются в процессе отработки списка последовательно.

Администратору и техническому специалисту необходимо уметь правильно конфигурировать списки управления доступом и знать, где их следует разместить в сети. Основные функции списков управления доступом включают в себя:

- фильтрацию внутренних пакетов;
- защиту внутренней сети от несанкционированного доступа;
- ограничение доступа к портам виртуального терминала.

Списки управления доступом (ACL) представляют собой набор инструкций, применяемых к интерфейсу маршрутизатора. Они указывают маршрутизатору, какие пакеты следует принять, а какие — отбросить. Решение о том, как поступить с пакетом, может быть основано на определенных критериях, таких, как адреса отправителя и получателя или номер порта TCP/UDP.

Списки управления доступом позволяют администратору управлять потоками данных и сканировать определенные пакеты. Любые потоки данных, которые проходят через интерфейс маршрутизатора, проверяются на соответствие условиям списка.

Списки управления доступом могут быть созданы для всех маршрутизируемых сетевых протоколов, таких, например, как Internet-протокол (Internet Protocol — IP) или протокол межсетевого пакетного обмена (Internetwork Packet Exchange — IPX),

с целью фильтрации пакетов по мере их поступления на маршрутизатор. Для списков ACL может быть установлена конфигурация, позволяющая управлять доступом к сети или подсети.

Алгоритм списков управления доступом при фильтрации потока данных принимает решение о том, направить пакет далее или заблокировать его на интерфейсе. Каждый пакет исследуется на соответствие условиям, которые указаны в списке; в качестве условий могут выступать адреса отправителя и получателя, идентификатор протокола верхнего уровня или другая информация.

Список ACL должен составляться для каждого отдельного протокола. Иными словами, для *каждого* используемого на интерфейсе маршрутизатора протокола должен быть составлен список, который будет регулировать трафик именно *на этом* интерфейсе. (Отметим, что в некоторых протоколах списки управления доступом называются *фильтрами*). Например, если интерфейс маршрутизатора используется для передачи IP-, AppleTalk- и IPX-трафика, то необходимо будет сконфигурировать, по меньшей мере, три списка управления доступом. Как именно следует конфигурировать списки ACL, как правильно выбрать диапазон и указать номер списка, рассказывается в этой главе. Списки могут быть использованы в качестве гибкого средства фильтрации пакетов, поступающих на интерфейс маршрутизатора или отправляемых с него (рис. 22.1).

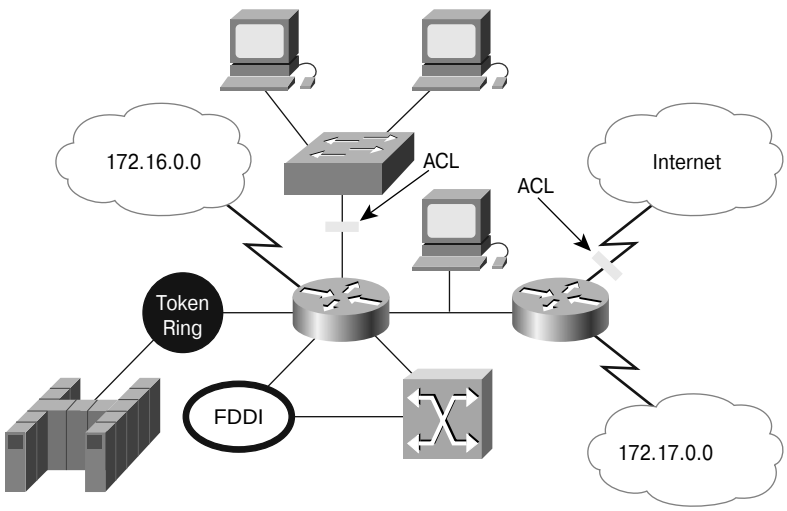


Рис. 22.1. Пример использования списков управления доступом

Введение в списки управления доступом

Для создания списков управления доступом существует множество причин; некоторые из них перечислены ниже.

ВНИМАНИЕ!

Правило, которое следует помнить: можно использовать один список ACL для одного интерфейса и для одного направления.

- Списки ACL можно использовать для ограничения потока данных в сети и повышения ее производительности. В частности, списки могут быть использованы для того, чтобы некоторые пакеты какого-либо протокола обрабатывались маршрутизатором ранее других. Такая функция называется *установкой очередности (queuing)* и используется для того, чтобы маршрутизатор не обрабатывал пакеты, которые в данный момент не являются жизненно необходимыми. Установка пакетов в очередь ограничивает поток данных в сети и уменьшает вероятность перегрузки.
- Списки ACL можно использовать для управления потоком данных. Например, с помощью списков можно ограничить или уменьшить количество сообщений об изменениях в сети. Такие ограничения используются для предотвращения распространения информации об отдельных сетях на всю сеть.
- Списки ACL можно использовать для обеспечения базового уровня защиты от несанкционированного доступа. Например, списки доступа позволяют разрешить одному узлу доступ к некоторому сегменту сети, а другому закрыть доступ к этой же области. На рис. 22.2 показано, что узлу А разрешен доступ к сети пользователей, а узлу Б такой доступ запрещен. Если на маршрутизаторе не установлен список управления доступом, то все пакеты, проходящие через него, поступают во все сегменты сети.
- Списки ACL можно использовать для указания данных, которые будут направляться далее или блокироваться на интерфейсе маршрутизатора. Например, можно разрешить маршрутизацию трафика электронной почты и в то же время заблокировать весь поток данных протокола telnet.

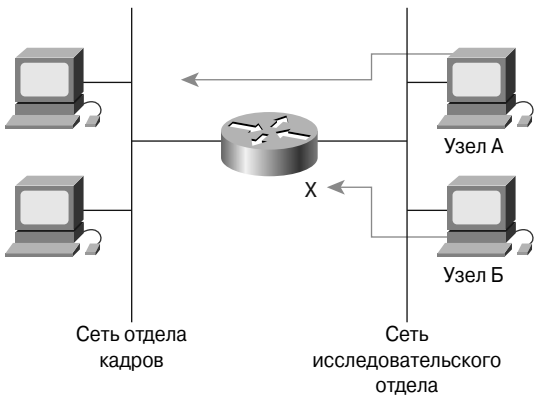


Рис. 22.2. Пример ограничения сетевого трафика

Дополнительная информация: конфигурирование списков ACL, порядок следования записей

Порядок следования записей необходимо учитывать при создании списка управления доступом. Принимая решение о дальнейшей отправке пакета или его блокировке, межсетевая операционная система Cisco (Cisco Internetwork Operational System — IOS) проверяет его соответствие всем директивам в том порядке, в каком они записаны. Пакеты последовательно проверяются на соответствие записям до тех пор, пока не будет найдено соответствие одному из правил. Если такое соответствие обнаружено, то остальные директивы списка не рассматриваются, и к пакету применяется указанное в списке действие.

Например, если было указано правило, которое разрешает передачу всех данных, то все последующие директивы не проверяются. Если требуется внести дополнительные директивы, то нужно удалить весь список и заново создать его с новыми записями. Поэтому при изменении списков доступа целесообразнее всего отредактировать конфигурацию маршрутизатора с помощью текстового редактора, а затем переслать ее на устройство посредством простейшего протокола передачи файлов (Trivial File Transfer Protocol — TFTP) или воспользоваться средствами передачи файлов терминального приложения, например, встроенной возможностью программы HyperTerminal.

Каждая добавленная запись заносится в конец списка. Таким образом, невозможно удалить в нумерованном списке отдельные директивы после того, как они были созданы, а можно удалить только весь список полностью.

Использование списков управления доступом

Для каждого протокола, данные которого необходимо фильтровать, и для каждого интерфейса необходимо создать список управления доступом. В некоторых протоколах создается один список для фильтрации входных данных и другой — для выходных.

После того как пакет будет проверен на соответствие заданному условию с помощью директивы списка доступа, ему может быть разрешено или запрещено использование интерфейса; сам список подключается к интерфейсу с помощью так называемой группы доступа.

Операционная система Cisco IOS проверяет пакет и заголовки верхних уровней для списков доступа, как показано на рис. 22.3.

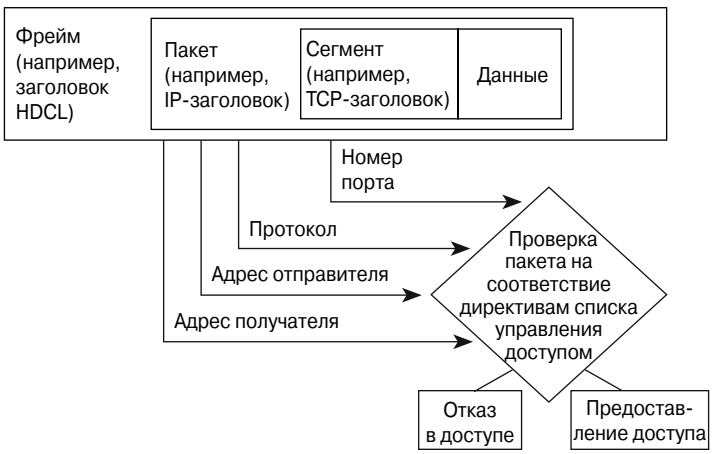


Рис. 22.3. Проверка пакетов и заголовков верхних уровней

Презентация: списки управления доступом
Списки ACL предоставляют базовые средства контроля трафика. В этой презентации перечислены предпосылки использования списков управления доступом и этапы их конфигурирования. Презентация позволит научиться различать две разновидности списков ACL, расширенные и стандартные списки, а также поможет разобраться в том, какие именно списки в каких случаях лучше всего использовать.

Принцип работы списков управления доступом

Список управления доступом представляет собой набор директив, которые определяют то, как пакеты

- поступают на входной интерфейс маршрутизатора,
- доставляются внутри маршрутизатора,
- пересылаются далее через выходной интерфейс маршрутизатора.

Начальная стадия процесса установления связи не зависит от того, используются ли списки управления доступом или нет (рис. 22.4). Когда пакет поступает на интерфейс, маршрутизатор определяет, куда его направить — на маршрутизатор или на мост (т.е. являются ли пакеты маршрутизируемыми или коммутируемыми). Если пакет по какой-либо причине не может быть обработан маршрутизатором или мостом, он отбрасывается. Далее операционная система проверяет, связан ли со входным интерфейсом какой-либо список доступа. Если список есть, то операционная система сверяет параметры пакета с записями такого списка ACL. Если пакет соответствует разрешающему правилу и подвергается маршрутизации, то в таблице маршрутизации выполняется поиск сети-получателя, определяется метрика маршрута или состояние и интерфейс, через который следует отправить пакет. Список управления доступом не фильтрует пакеты, которые возникают внутри маршрутизатора, но фильтрует пакеты из иных источников.

Далее маршрутизатор проверяет, находится ли интерфейс получателя в группе списка управления доступом. Если его там нет, то пакет может быть направлен на интерфейс получателя непосредственно; например, при использовании интерфейса E0, который не связан со списками управления доступом, пакет отправляется непосредственно через такой интерфейс.

Директивы списка исполняются в последовательном логическом порядке. Если заголовок пакета соответствует директиве списка, то остальные директивы пропускаются. Если условие директивы выполнено, пакет передается далее или отбрасывается в соответствии с конфигурацией. Если заголовок пакета не соответствует ни одной директиве списка, то к нему применяется стандартное правило, размещенное в конце списка, которое запрещает передачу любых пакетов. Даже если такая директива не отображается в последней строке списка управления доступом, она стандартно там присутствует. В примере, который проиллюстрирован на рис. 22.5, пакет соответствует условию первой директивы и ему отказано в доступе. Он отбрасывается, соответствие пакета последующим условиям не проверяется. Для уничтожения пакета используется *битовая корзина (bit bucket)*. Если пакет не соответствует условию

первой директивы, он проверяется на соответствие второй директиве из списка управления доступом, и т.д.

Списки ACL позволяют контролировать, каким пользователям разрешен доступ к конкретной сети. Условия в списке контроля доступа позволяют:

- просмотреть адреса определенных узлов для того, чтобы разрешить или заблокировать им доступ к некоторой части сети;
- разрешить или запретить доступ пользователям только к определенным видам приложений, таким, как службы FTP и HTTP.

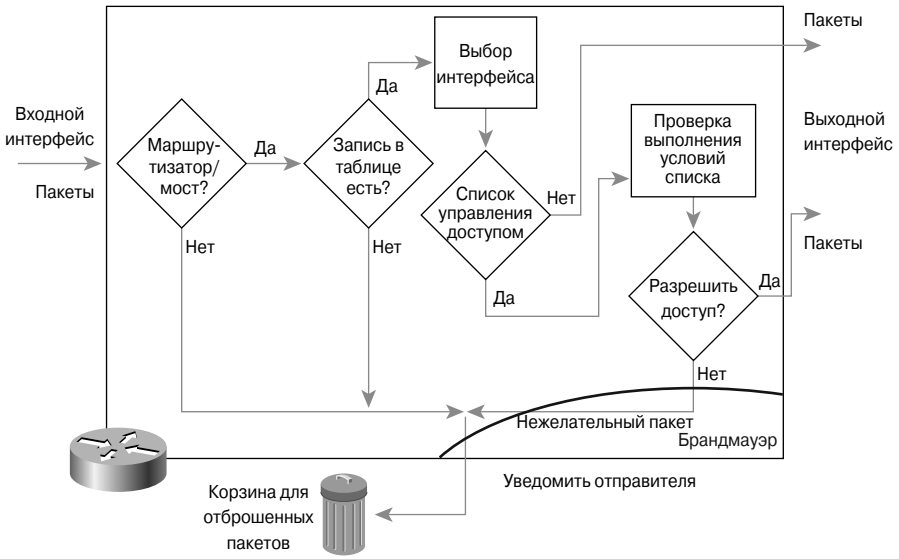


Рис. 22.4. Принцип работы списков управления доступом

Конфигурирование списков управления доступом

Списки ACL создаются в режиме глобальной конфигурации устройства. Существует великое множество разных типов списков управления доступом: стандартные, расширенные, списки протокола IPX, списки AppleTalk и многие другие. При создании списков ACL в маршрутизаторе каждому списку следует назначить уникальный номер. Такой номер идентифицирует тип списка и не должен выходить за границы диапазона номеров, который выделен для определенной разновидности списков.

После того как администратор переводит режим командной строки в нужный и принято решение о том, из какого диапазона следует выбрать номер списка, он последовательно вводит директивы списка ACL, начиная с ключевого слова **`access-list`** и заканчивая правильными параметрами, как показано в примере 22.1. Создание списка управления доступом — это только половина дела. Вторая, и не менее важная часть процесса, — это привязка списка к интерфейсу.

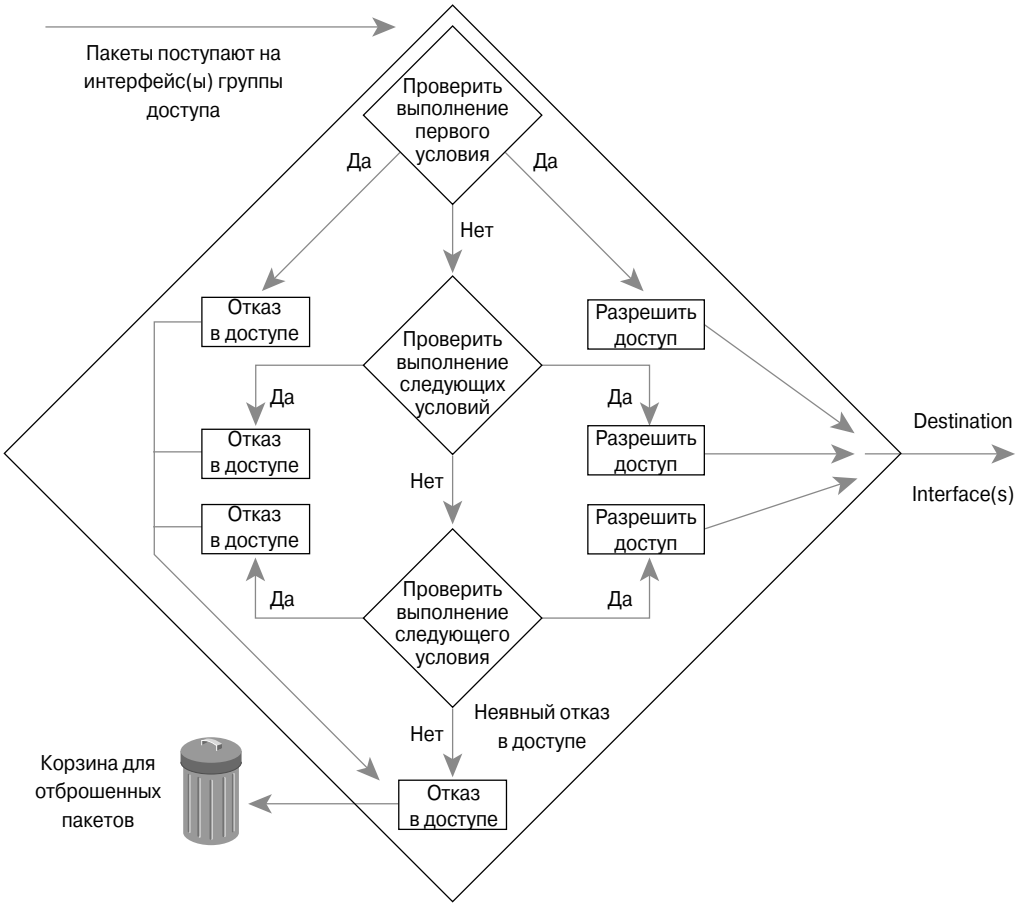


Рис. 22.5. Список ACL: проверка на соответствие условиям и неявное правило в конце

Списки ACL могут быть привязаны к одному и более интерфейсам и могут фильтровать как входные, так и выходные потоки данных. Привязка списка к интерфейсу (интерфейсам) осуществляется посредством команды **`access-group`** (пример 22.1). Команда **`access-group`** вводится в режиме конфигурирования интерфейса. Список управления доступом привязывается к интерфейсу во входном или выходном направлении: для входящего или исходящего трафика. Чтобы определить, в каком направлении должен воздействовать список ACL на проходящие через интерфейс потоки данных, следует "взглянуть на интерфейс изнутри маршрутизатора", т.е. представить себе, что вы находитесь внутри устройства. Такой подход поможет разобраться в потоках трафика во многих ситуациях, когда необходимо понять, какие потоки данных в каком направлении передаются. С точки зрения "наблюдателя внутри маршрутизатора", трафик, который входит из внешнего мира внутрь устройства через интерфейс, может быть отфильтрован входным списком

управления доступом; соответственно, поток данных, который направлен из устройства во внешнюю сеть через интерфейс, может быть отфильтрован выходным списком. После того как нумерованный список ACL создан, его следует привязать к нужному интерфейсу. Чтобы изменить порядок следования директив в нумерованном списке управления доступом, необходимо удалить весь список с помощью команды **no access-list** *номер списка* и создать его заново.

На практике команды списков управления доступом представляют собой длинные символьные строки. Основные задачи, решение которых описано в этом разделе, включают в себя следующие действия:

- необходимо сконфигурировать список управления доступом в режиме глобальной конфигурации маршрутизатора;
- следует назначить номер списку управления доступом в диапазоне от 1 до 99, если требуется создать стандартный список для протокола IP;
- следует назначить номер списку управления доступом в диапазоне от 100 до 199, если требуется создать расширенный список ACL для протокола IP;
- при создании списка ACL необходимо тщательно отбирать необходимые директивы и соблюдать их логическую последовательность. В списке должны быть указаны разрешенные IP-протоколы; все данные других протоколов должны быть запрещены;
- необходимо выбрать IP-протоколы, которые следует проверять; все остальные протоколы проверяться не будут. В дальнейшем для большей точности можно будет также указать порт получателя;
- после того как будет создан необходимый список контроля доступа, его следует привязать к определенному интерфейсу.

Несмотря на то что каждый протокол выдвигает свои специфические требования и правила, выполнение которых необходимо для фильтрации трафика, в целом создание списков управления доступом требует выполнения всего двух основных действий, которые указаны ниже.

Этап 1. Создать список доступа ACL.

Этап 2. Применить список доступа на конкретном интерфейсе.

Списки управления доступом применяются к одному или нескольким интерфейсам и выполняют фильтрацию входящих или исходящих потоков данных, в зависимости от установленной конфигурации. Списки для исходящего трафика обычно более эффективны, поэтому предпочтительнее использовать именно их. Маршрутизатор, в котором сконфигурирован список ACL для входящего трафика, должен проверять каждый пакет на его соответствие условиям списка перед тем, как отправить пакет на выходной интерфейс.

Присвоение уникального номера каждому списку управления доступом

В процессе конфигурирования маршрутизатора каждому списку управления доступом необходимо присвоить индивидуальный номер; при назначении номера необходимо принимать во внимание диапазон номеров, который зарезервирован для данного протокола или стека. В примере 22.1 показаны стандартные списки управления доступом с номерами 1 и 2, которые привязываются к интерфейсу Ethernet 0.

Пример 22.1. Применение списков управления доступом к интерфейсу

```
access-list 1 permit 5.6.0.0 0.0.255.255
access-list 1 deny 7.9.0.0 0.0.255.255
!
access-list 2 permit 1.2.3.4
access-list 2 deny 1.2.0.0 0.0.255.255
!
interface ethernet 0
ip address 1.1.1.1 255.0.0.0
!
ip access-group 1 in
ip access-group 2 out
```

В табл. 22.1 перечислены наиболее часто используемые протокольные номера списков контроля доступа.

Таблица 22.1. Протокольные номера списков ACL

Протокол и тип списка	Диапазон номеров
Стандартные списки IP	1–99
Расширенные списки IP	100–199
Протокол AppleTalk	600–699
Стандартные списки IPX	800–899
Расширенные списки IPX	900–999
Протокол IPX SAP (Service Advertising Protocol — протокол извещения о службах)	1000–1099

Интерактивная презентация: создание списков ACL
В этой презентации подробно рассмотрен процесс создания списков управления доступом.

Использование битов инвертированной маски

Инвертированная маска (wildcard mask) представляет собой 32-битовую величину, которая разделена на четыре октета, каждый из которых состоит из восьми битов. Если в какой-либо позиции маски стоит бит, равный нулю, то соответствующий бит

адреса должен быть проверен; если же в какой-либо позиции бит равен единице, то соответствующий бит адреса должен быть проигнорирован (рис. 22.6).

Рис. 22.6. Проверка битов инвертированной маски

Инвертированная маска, как и маска подсети, тесно связана с IP-адресом. В инвертированной маске используются нули и единицы, для того чтобы указать, как следует трактовать соответствующие биты IP-адреса.

Инвертированная маска используется для указания одного или нескольких адресов, которые будут проверяться на соответствие условиям списка контроля доступа. Термин *использование инвертированной маски (wildcard masking)* обозначает процесс побитового сравнения и подстановки значений битов адреса[2].

Несмотря на то что инвертированная маска списков управления доступом и маска подсети представляют собой 32-битовые величины, выполняемые ими функции значительно отличаются. Нули и единицы в маске подсети определяют сеть, подсеть и номер узла. Биты инвертированной маски указывают, будет ли проверяться соответствующий бит.

Итак, нули и единицы в инвертированной маске указывают списку управления доступом на необходимость проверять или не проверять соответствующие биты в IP-адресе. На рис. 22.7 проиллюстрировано применение инвертированной маски.

Предположим, необходимо проверить IP-адрес подсети, которому может быть разрешен или блокирован доступ. Предположим также, что этот адрес относится к классу B (т.е. первые два октета представляют собой номер сети), а следующие 8 битов обозначают номер подсети (третий октет предназначен для номера подсети). Если требуется разрешить доступ всем пакетам с номерами подсетей от 172.30.16.0

[2] *По-английски* wildcard *на профессиональном жаргоне игроков в карты обозначает* джокер. *Сам компьютерный термин связан с карточной игрой покер, в которой джокер может заменять любую карту. Аналогично определенное значение бита инвертированной маски позволяет подставлять любой бит адреса без его проверки. — Прим. ред.*

до 172.30.31.0, то следует использовать инвертированную маску, которая показана на рис. 22.7.

Сначала проверяются первые два октета (172.30) адреса с использованием соответствующих нулевых битов в инвертированной маске.

Поскольку индивидуальные адреса узлов не представляют интереса (правильный идентификатор узла не содержит в конце адреса 0.0), в шаблоне маски не учитывается последний октет, о чем свидетельствуют биты со значением, равным единице, в правой части инвертированной маски.

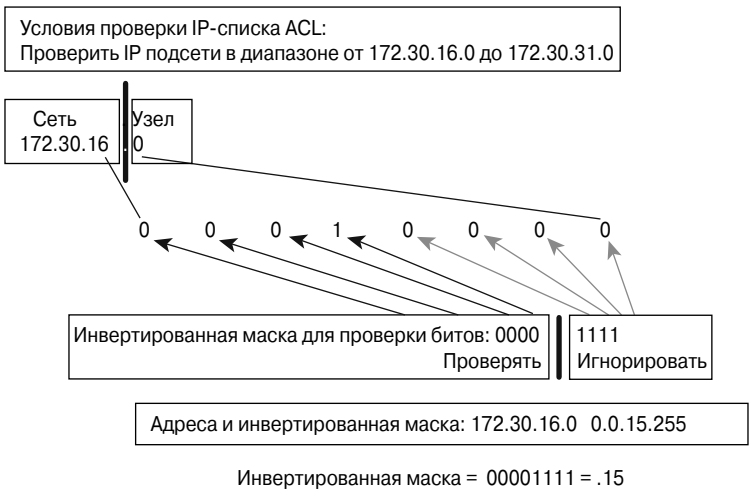


Рис. 22.7. Пример использования инвертированной маски

В третьем октете инвертированная маска равна 15-ти (в бинарном виде — 00001111), а IP-адрес равен 16-ти (в бинарном виде — 00001000). Первые четыре нуля шаблона маски указывают маршрутизатору на необходимость проверки первых четырех битов IP-адреса (т.е. шаблона 0001). Поскольку последние четыре бита не принимаются во внимание, все числа в интервале от 16 (00010000) до 31 (00011111) будут отвечать условию, поскольку они все начинаются с шаблона 0001.

Последние (наименьшие значащие) четыре бита в третьем октете инвертированной маски во внимание не принимаются, они могут быть равны как нулям, так и единицам.

В рассмотренном выше примере маска указывает маршрутизатору на необходимость поиска соответствия первых 4-х битов в IP-адресе шаблону, остальные 4 бита полностью игнорируются. Поэтому если в списке ACL указан адрес 172.30.16.0 с инвертированной маской 0.0.15.255, он соответствует подсетям с номерами от 172.30.16.0 до 172.30.31.0. Другие подсети не отвечают условиям рассмотренной маски.

Использование шаблона any

Работа с десятичным представлением битов шаблона может показаться утомительной[3]. Во многих случаях ключевые слова (или зарезервированные шаблоны) значительно упростят работу со списками ACL. Прежде всего, такие ключевые слова уменьшают количество символов, которое приходится набирать на клавиатуре при записи условий проверки для отдельных адресов. Одним из таких шаблонов является ключевое слово **any** (переводится как *любой*). Например, если требуется разрешить доступ для всех адресов получателей, можно указать маску 0.0.0.0 (рис. 22.8); кроме этого, список управления доступом должен игнорировать (т.е. пропускать их без проверки) любые значения битов адреса, поэтому все биты инвертированной маски должны быть равны единице (т.е. 255.255.255.255).

Рис. 22.8. Шаблон ***any***

Для указания операционной системе Cisco IOS описанного выше условия можно также использовать ключевое слово **any**. Вместо того чтобы набирать на клавиатуре 0.0.0.0 255.255.255.255, достаточно указать простое и короткое ключевое слово **any**.

Например, вместо использования строки

```
Router(config)# access-list 1 permit 0.0.0.0 255.255.255.255
```

можно просто набрать

```
Router(config)# access-list 1 permit any
```

[3] *Существует несколько простых эмпирических методов расчета инвертированной маски. Если известна маска подсети, то от каждого октета нужно отнять 255, в результате будет получена инвертированная маска. Например, нужно рассчитать инвертированную маску для подсети в сети класса B с маской 255.255.224.0. Если отнять от каждого октета 255 (по модулю), инвертированная маска будет равна 0.0.31.255. Другой метод проще всего применять для сетей класса C. Он подразумевает, что специалист знает количество узлов в подсети; от общего количества узлов необходимо отнять единицу, в результате будет получено значение последнего октета инвертированной маски. Например, в подсети с маской 255.255.255.240 есть 16 адресов (с учетом адреса подсети и широковещательного адреса). Отняв от 16-ти единицу, мы получим последний октет, результирующая инвертированная маска будет равна 0.0.0.15. — Прим. ред.*

Использование шаблона host

Второй случай, когда можно использовать ключевое слово в списке ACL, — это ситуация, когда необходимо соответствие всех битов адреса одного узла заданному шаблону. Предположим, требуется заблокировать доступ конкретному узлу. Чтобы указать один узел, надо полностью ввести его IP-адрес (например, 172.30.16.29; рис. 22.9), а затем указать, что в списке должны быть проверены все биты адреса, т.е. инвертированная маска должна состоять только из нулей (0.0.0.0).

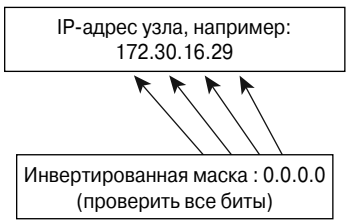


Рис. 22.9. Шаблон ***host***

Можно использовать ключевое слово **host**, которое укажет операционной системе Cisco IOS, что нужно проверять только один полный адрес. В приведенном ниже примере показано, что вместо ввода длинной строки **172.30.16.29 0.0.0.0** перед адресом можно записать ключевое слово **host**.

Например, вместо строки

```
Router(config)# access-list 1 permit 172.30.16.29 0.0.0.0
```

можно записать

```
Router(config)# access-list 1 permit host 172.30.16.29
```

Проверка списков управления доступом

Команда **show ip interface** отображает информацию об интерфейсах и показывает, установлены ли на них списки управления доступом. Результат выполнения этой команды приведен в примере 22.2. Обратите внимание на строки 9 и 10: для исходящего трафика интерфейса Ethernet 0 установлен список управления доступом с номером 10, для исходящих потоков данных списков нет.

Пример 22.2. Результат выполнения команды show ip interface

```
Router> show ip interface
Ethernet0 is up, line protocol is up
Internet address is 192.54.22.2, subnet mask is 255.255.255.0
Broadcast address is 255.255.255.255
Address determined by nonvolatile memory
MTU is 1500 bytes
```

```
Helper address is 192.52.71.4
Secondary address 131.192.115.2, subnet mask 255.255.255.0
Outgoing ACL 10 is set
Inbound ACL is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachables are never sent
ICMP mask replies are never sent
IP fast switching is enabled
Gateway Discovery is disabled
IP accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Router>
```

Команда **show access-lists** отображает содержимое всех списков управления доступом. Если после двух указанных ключевых слов ввести имя или номер списка управления доступом в качестве параметра, то будет отображено содержимое конкретного списка ACL.

Списки управления доступом

Посредством списков управления доступом маршрутизаторы предоставляют простые средства фильтрации потоков данных, например, возможность блокирования Internet-трафика. Список ACL представляет собой упорядоченный набор выражений на основе ключей **permit** (разрешить) и **deny** (заблокировать), которые применяются к адресам протоколов верхних уровней. В текущем разделе подробно рассматриваются стандартные и расширенные списки управления доступом и методы их применения в качестве средства сетевого трафика. В нем также обсуждается вопрос использования списков ACL в качестве механизма обеспечения безопасности в сети.

Стандартные списки ACL

Стандартный список управления доступом позволяет проверять и сравнивать адреса отправителей пакетов с директивами, как показано на рис. 22.10.

Стандартные списки управления доступом используются тогда, когда необходимо заблокировать или разрешить доступ всему набору протоколов (íàïðèìåð, IP) на основании адреса сети, подсети или узла.

Например, для пакетов, поступивших на интерфейс `E0` или `Fa0/0`, проверяются адреса отправителя и протоколы. Затем они сравниваются с директивами списка управления доступа. Если соответствие найдено, выполняется указанное действие (разрешение или запрет). Если пакеты соответствуют разрешающему правилу (**permit**), они перенаправляются через маршрутизатор к выходному интерфейсу,

который логически связан со списком управления доступом. Если же пакеты соответствуют запрещающему правилу (**deny**), они отбрасываются.

Полный синтаксис директивы стандартного списка ACL имеет вид:

```
Router(config)# access-list access-list-number {permit | deny |
remark} source [source-wildcard] [log]
```

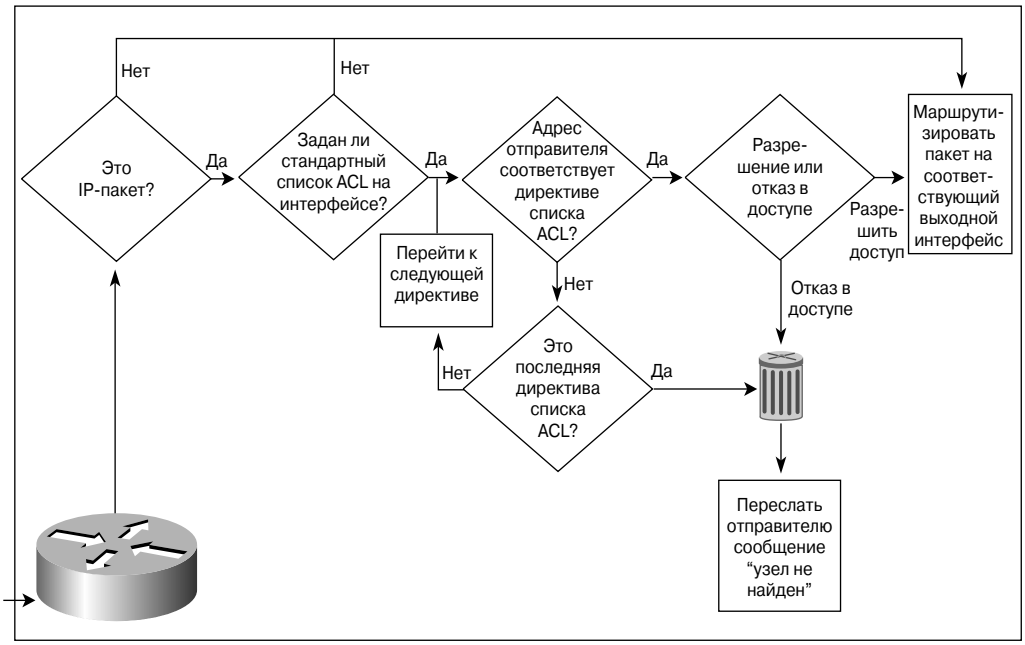


Рис. 22.10. Принцип работы стандартных списков управления доступом

Ключевое слово **remark** используется для внесения в список комментария, который впоследствии поможет разобраться в списке управления доступом. Длина такой строки-комментария не может превышать ста символов.

Например, с первого взгляда тяжело сказать, для чего именно нужна такая запись:

```
access-list 1 permit 171.69.2.88
```

Если же в списке управления доступом присутствует комментарий, то разобраться, к чему именно относится определенная директива, будет значительно проще.

```
access-list 1 remark Permit only Howard workstation though
ACL 1 171.69.2.88
access-list 1 permit 171.69.2.88
```

(Комментарий гласит: "Разрешить доступ посредством списка ACL 1 только рабочей станции Говарда 171.69.2.88".)

Для удаления стандартного списка управления доступом используется форма этой команды с ключевым словом **no**:

```
Router(config)# no access-list number
```

В табл. 22.2 приведено описание параметров, используемых для создания директивы стандартного списка контроля доступа.

Стандартная версия команды **access-list** списка доступа в режиме глобальной конфигурации задает стандартный список управления доступом с номером в диапазоне от 1 до 99. В примере 22.3 показан стандартный список доступа, который содержит 4 директивы; все директивы входят в список доступа с номером 2. Следует помнить, что даже если пакеты не отвечают ни одному из правил (т.е. записям или директивам) списка доступа, они попадают под неявное правило в конце списка доступа ACL, которое запрещает передачу всех пакетов (это правило не отображается в конфигурации).

Пример 22.3. Директивы стандартного списка управления доступом

```
access-list 2 deny 172.16.1.1
access-list 2 permit 192.168.1.0 0.0.0.255
access-list 2 deny 172.16.0.0 0.0.255.255
access-list 2 permit 10.0.0.0 0.255.255.255
```

В первой строке списка управления доступом указано, что инвертированная маска не используется (обратите внимание, что она там отсутствует). В подобной ситуации, когда не указана маска, используется инвертированная маска со стандартным значением 0.0.0.0. Данная директива списка ACL запретит доступ с одного IP-адреса — 172.16.1.1.

Вторая строка разрешает доступ с адресов из сети 192.168.1.0, т.е. с любого адреса, который начинается с комбинации 192.168.1.

Третья строка-директива запрещает доступ из сети 172.16.0.0, а четвертая разрешает передавать пакеты с любого адреса, который начинается с 10., т.е. из сети 10.0.0.0.

Команда **ip access-group** используется для привязки созданного списка управления доступом к интерфейсу. Отметим, что для каждого порта, протокола и направления допускается использовать только один список. Команда имеет следующий формат:

```
Router(config)# ip access-group номер списка {in | out}
```

Таблица 22.2. Параметры стандартного списка управления доступом

Параметр	Описание
number	Номер списка управления доступом. Представляет собой целое десятичное число в диапазоне от 1 до 99 или от 1300 до 1999
deny	Пакету будет отказано в доступе, если он соответствует этой записи
permit	Пакету будет разрешен доступ, если он соответствует этой записи
source	Номер сети или адрес узла, с которого отправлен пакет. Устройство-отправитель можно указать двумя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; ■ использовать ключевое слово **any** для обозначения отправителя вместо записи `0.0.0.0 255.255.255.255`
source-wilcard	(Необязательный параметр) Инвертированная маска отправителя. Инвертированную маску устройства-отправителя можно указать двумя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; если какие-либо биты нужно игнорировать, в них следует записать единицы; ■ использовать ключевое слово **any** для обозначения отправителя вместо записи `0.0.0.0 255.255.255.255`
log	(Необязательный параметр) Журнал. Параметр указывает, что нужно выводить информационные сообщения в системном журнале (logging message) для пакета, отвечающего записи списка. Журнал впоследствии можно вывести на консоль. (Уровень сообщений, выводимых на консоль, задается командой **logging console**.) Информационное сообщение включает в себя: номер списка управления доступом, адрес отправителя и количество пакетов, указывает, была ли разрешена передача пакета. Такое сообщение генерируется для первого пакета, удовлетворяющего условию, а затем генерируется с пятиминутным интервалом; при этом сообщается количество пакетов, которым было разрешено или отказано в доступе за предыдущий пятиминутный интервал. С помощью команды **ip access-list log-update** можно указать пороговое количество сообщений для генерирования системного журнала, вместо того чтобы ждать истечения пятиминутного интервала. Более подробная информация о команде **ip access-list log-update** размещена на Web-сайте корпорации Cisco в разделе `www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/cbkixol.htm`. Системная служба может пропускать или отбрасывать сообщения, если устройство перегружено или когда больше одного системного сообщения обрабатывается за секунду. Такое поведение предотвращает отказ или перегрузку маршрутизатора из-за большого количества системных сообщений, поэтому системные службы не рекомендуется использовать как средства учета в сети или как средство подсчета точного количества соответствий в списках доступа ACL

Практическое задание 22.2.1a. Конфигурирование стандартных списков управления доступом
В этой лабораторной работе необходимо сконфигурировать стандартный список ACL, который запретит или разрешит определенные типы трафика.

Практическое задание 22.2.1b. Стандартные списки управления доступом
В этой лабораторной работе необходимо спланировать, сконфигурировать и применить стандартные списки управления доступом, которые разрешат или запретят передачу отдельных пакетов. Список ACL также необходимо проверить, чтобы определить, был ли достигнут желаемый результат.

Расширенные списки управления доступом

Расширенные списки управления доступом (extended access control list — extended ACL) используются чаще, чем стандартные, поскольку они обеспечивают бо́льшие возможности контроля. Расширенный список управления доступом проверяет как адрес отправителя, так и адрес получателя. Список может также проверять конкретные протоколы, номера портов и другие параметры. Процесс обработки трафика маршрутизатором для проверки пакетов на соответствие правилам расширенных списков управления доступом проиллюстрирован на рис. 22.11.

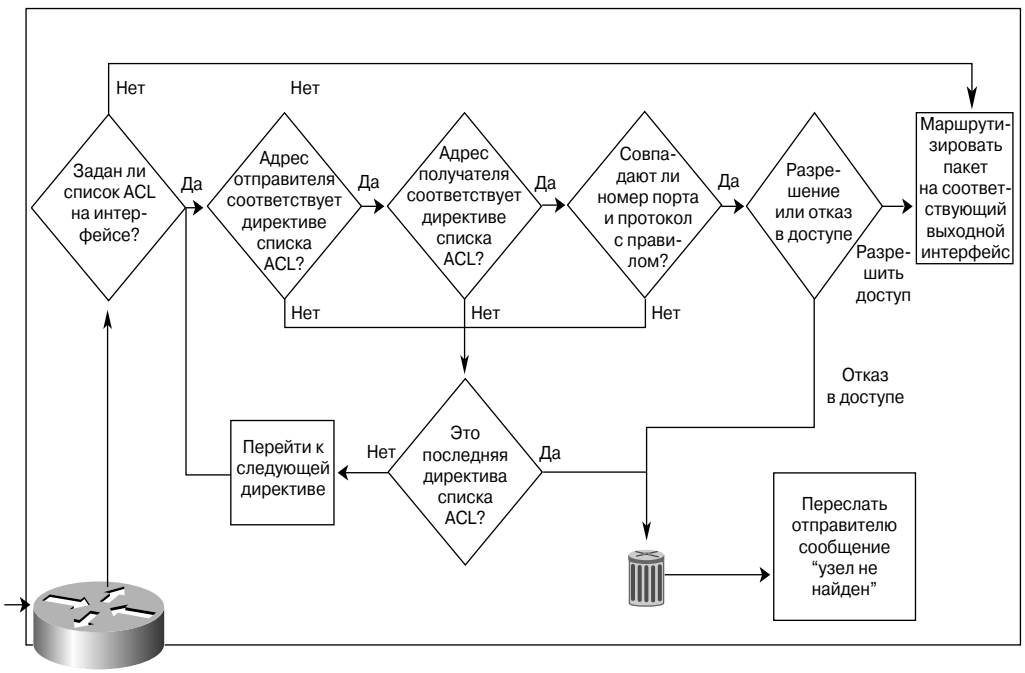


Рис. 22.11. Принцип работы расширенного списка управления доступом

Отправка пакета может быть разрешена или же может быть отказано в передаче в зависимости от того, откуда был переслан пакет и куда направлен, какой протокол, адрес порта и тип приложения при этом были использованы. Расширенные списки управления доступом, например, позволяют пересылать трафик электронной почты из интерфейса `Fa0/0` в интерфейс `S0/0` и в то же время могут запрещать передачу файлов и потоки данных от Web-сайтов. Когда маршрутизатор уничтожает пакеты, некоторые протоколы посылают эхо-сообщения отправителю, уведомляющие, что получатель недоступен.

Расширенные списки управления позволяют более точно контролировать и управлять пакетами, нежели стандартные. Стандартные списки управления доступом предназначены для того, чтобы запрещать весь набор или стек протоколов; расширенные списки позволяют точно указать, какой из протоколов необходимо разрешить или запретить. Например, с помощью такого списка ACL можно разрешить трафик HTTP, но запретить доступ к ресурсам по протоколу FTP.

Полный формат команды **`access-list`** для расширенного списка контроля доступа имеет следующий вид:

```
Router(config)# access-list access-list-number [dynamic dynamic-name
[timeout minutes]] {permit | deny} protocol source [source-wildcard
destination destination-wildcard] [precedence precedence] [tos tos]
[log | log-input] [ time-range time-range-name] established
[fragments]
```

Ключевое слово **`no`** в начале команды используется для удаления расширенного списка управления доступом. Например, чтобы удалить список, следует ввести команду с параметром **`no`** в начале:

```
Router(config)# no access-list access-list-number
```

Полная команда расширенного списка управления доступом может быть очень длинной, часто она превышает ширину окна терминала. Параметры расширенных списков доступа и множество дополнительных опций, которые в примере синтаксиса команды опущены, описаны в табл. 22.3.

Таблица 22.3. Параметры расширенного списка доступа

Параметр	Описание
access-list-number	Номер списка доступа. Представляет собой десятичное число в диапазоне от 100 до 199 или от 2000 до 2699
dynamic *dynamic-name*	(Необязательный параметр) Идентифицирует список управления доступом как динамический список ACL. Обычно этот параметр используется для реализации защиты типа замка (lock-and-key). (Более подробную информацию по данному вопросу можно найти в книге *Cisco IOS Security Configuration Guide*)

Продолжение табл. 22.3

Параметр	Описание
timeout *minutes*	(Необязательный параметр) Указывает абсолютный интервал в минутах, в течение которого временная запись списка контроля доступа может существовать в динамическом списке ACL. Стандартно такой интервал бесконечен, и данные могут передаваться в любой момент времени. (Более подробную информацию по этому вопросу можно найти в книге *Cisco IOS Security Configuration Guide*)
deny	Запрещает доступ, если условие выполнено
permit	Разрешает доступ, если условие выполнено
protocol	Имя или номер протокола сети Internet. В качестве параметра может использоваться одно из ключевых слов: **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **pim**, **tcp**, **udp** или целое число в диапазоне от 0 до 255, соответствующее номеру Internet-протокола. Для проверки любых Internet-протоколов (включая ICMP, TCP и UDP) следует использовать ключевое слово **ip**. Некоторые протоколы позволяют добавить уточняющие параметры в список
source	Номер сети или адрес узла, с которого отправлен пакет. Устройство-отправитель можно указать тремя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; ■ использовать ключевое слово **any** для обозначения любого отправителя вместо записи `0.0.0.0 255.255.255.255`;использовать ключевое слово **host** для обозначения единственного адреса отправителя вместо записи инвертированной маски в виде `0.0.0.0`
source-wildcard	Инвертированная маска отправителя. Если в какой-либо позиции маски стоит бит, равный нулю, то соответствующий бит адреса должен быть проверен; если же в какой-либо позиции бит равен единице, то соответствующий бит адреса должен быть проигнорирован. Инвертированную маску устройства-отправителя можно указать тремя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; биты адреса, которым соответствуют единичные биты в маске, не будут проверяться; ■ использовать ключевое слово **any** для обозначения любого отправителя вместо записи `0.0.0.0 255.255.255.255`; ■ использовать ключевое слово **host** для обозначения единственного адреса отправителя вместо записи инвертированной маски в виде `0.0.0.0`.

Продолжение табл. 22.3

Параметр	Описание
	Биты инвертированной маски со значением 1 не обязательно должны быть последовательно (т.е. непрерывно) записаны в шаблоне отправителя. Например, инвертированная маска для некоторого адреса отправителя `0.255.0.64` вполне приемлема
destination	Номер сети или адрес узла, которому предназначен пакет. Устройство-получатель можно указать тремя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; ■ использовать ключевое слово **any** для обозначения любого получателя вместо записи `0.0.0.0 255.255.255.255`;использовать ключевое слово **host** для обозначения единственного адреса получателя вместо записи инвертированной маски в виде `0.0.0.0`
destination-wildcard	Инвертированная маска получателя. Инвертированную маску устройства-получателя можно указать тремя способами: ■ использовать 32-битовую величину в точечно-десятичном формате, состоящем из четырех частей; биты адреса, которым соответствуют единичные биты в маске, не будут проверяться; ■ использовать ключевое слово **any** для обозначения любого получателя вместо записи `0.0.0.0 255.255.255.255`;использовать ключевое слово **host** для обозначения единственного адреса получателя вместо записи инвертированной маски в виде `0.0.0.0`
precedence *precedence*	(Необязательный параметр) Пакеты могут быть отфильтрованы по уровню приоритета (precedence), который задается целым числом от 0 до 7. Такая возможность используется в механизмах обеспечения качества обслуживания (Quality of Service — QoS) в сетевых устройствах
tos *tos*	(Необязательный параметр) Пакеты могут быть отфильтрованы по типу обслуживания (Type of Service — ToS), который задается целым числом от 0 до 15. Такая возможность используется в механизмах обеспечения качества обслуживания (Quality of Service — QoS) в сетевых устройствах
log	(Необязательный параметр) Журнал. Параметр указывает, что нужно выводить информационные сообщения в системном журнале (logging message) для пакета, отвечающего записи списка; журнал впоследствии можно вывести на консоль. (Уровень сообщений, выводимых на консоль, задается командой **logging console**.) Информационное сообщение включает в себя: номер списка управления доступом, адрес отправителя и количество пакетов, указывает, была ли разрешена передача пакета. Оно генерируется для первого пакета, удовлетворяющего условию, а затем генерируется с пятиминутным интервалом; при этом

Продолжение табл. 22.3

Параметр	Описание
	сообщается количество пакетов, которым было разрешено или отказано в доступе за предыдущий пятиминутный интервал. С помощью команды **ip access-list log-update** можно указать пороговое количество сообщений для генерирования системного журнала, вместо того чтобы ждать истечения пятиминутного интервала. Более подробная информация о команде **ip access-list log-update** размещена на Web-сайте корпорации Cisco в разделе `www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/cbkixol.htm`. Системная служба может пропускать или отбрасывать сообщения, если устройство перегружено или когда за одну секунду обрабатывается более одного системного сообщения. Такое поведение предотвращает отказ или перегрузку маршрутизатора из-за большого количества системных сообщений. Поэтому системные службы не рекомендуется использовать как средства учета в сети или как средство подсчета точного количества соответствий в списках доступа ACL
log-input	(Необязательный параметр) Включает входной интерфейс и MAC-адрес отправителя или номер виртуального канала (Virtual Circuit — VC) в сообщения системного журнала
time-range *time-range-name*	(Необязательный параметр) Задает время срабатывания записи списка ACL. Параметры временного интервала (имя и ограничения) задаются отдельной конфигурационной командой **time-range**
icmp-type	(Необязательный параметр) ICMP-пакеты могут быть отфильтрованы по типу ICMP-сообщений. Тип указывают с помощью номера в диапазоне от 0 до 255
icmp-code	(Необязательный параметр) ICMP-пакеты могут быть отфильтрованы по коду ICMP-сообщений. Код сообщения указывают с помощью номера в диапазоне от 0 до 255
icmp-message	(Необязательный параметр) ICMP-пакеты могут быть отфильтрованы по имени типа ICMP-сообщений или символьному имени-параметру кода ICMP-сообщения
igmp-type	(Необязательный параметр) IGMP-пакеты могут быть отфильтрованы по типу IGMP-сообщений. Тип указывают с помощью номера в диапазоне от 0 до 15
operator	(Необязательный параметр) Используется для сравнения портов отправителя и/или получателя. Возможные варианты включают в себя ключи **lt** (less than — меньше, чем), **gt** (больше, чем), **eq** (равно), **neq** (не равно) и **range** (т.е. порты, которые входят в диапазон). Если оператор расположен после адреса и инвертированной маски отправителя, он задает порт отправителя. Если оператор расположен после адреса и инвертированной маски получателя, он задает порт получателя.

Окончание табл. 22.3

Параметр	Описание
	Оператор диапазона **range** требует указания двух номеров портов. Для всех остальных операторов должен быть указан один номер порта
port	(Необязательный параметр) Задает в десятичном формате номера или символьные имена TCP- или UDP-портов. Порт — это номер в диапазоне от 0 до 65 535. Символьное имя TCP-порта может быть использовано только при фильтрации протокола из стека TCP. Символьное имя UDP-порта может использоваться только при фильтрации UDP-протоколов
established	(Необязательный параметр) Используется только для TCP-протоколов: пропускает пакеты лишь установленного соединения. TCP-дейтаграммы с флагом ACK, FIN, PSH, RST или установленным управляющим URG-битом будут соответствовать данной записи списка управления доступом. Первая дейтаграмма, которая отправляется при установке TCP-соединения, не отвечает условию, которое задано данным ключевым словом
fragments	(Необязательный параметр) Этот параметр применяется для последующих (т.е. всех, кроме первого) фрагментов пакетов; фрагменты могут быть разрешены или запрещены к передаче

В одном списке управления доступом может быть указано несколько директив. Каждая из записей списка должна содержать один и тот же *номер* списка доступа, чтобы относиться к одному и тому же списку, как показано в примере. 22.4. В одном списке управления доступом может быть указано столько директив, сколько требуется. Количество директив ограничено только доступной памятью маршрутизатора. Чем больше записей содержится в каждом списке управления доступом, тем сложнее будет поддерживать и управлять списками ACL в маршрутизаторе. В примере 22.3 используются три последовательные директивы, которые указывают, что telnet-, ftp-пакеты и пакеты данных протокола FTP разрешено передавать от любых узлов подсети 172.16.6.0 в любую сеть.

Пример 22.4. Директивы расширенного списка управления доступом

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

Расширенные списки управления доступом являются практически универсальным инструментом и, по существу, позволяют использовать практически любые опции и параметры, которые характерны для любого используемого протокола. Порядок следования записей в списке может быть различным и зависит от используемого протокола. Основные применяемые на практике протоколы перечислены ниже.

- Протокол управляющих сообщений в сети Internet (Internet Control Message Protocol — ICMP).
- Межсетевой протокол управления группами (Internet Group Management Protocol — IGMP).
- Протокол управления передачей (Transmission Control Protocol — TCP).
- Протокол пользовательских дейтаграмм (User Data Protocol — UDP).

В коротких разделах ниже описаны вариации расширенных списков управлением доступом в зависимости от используемого протокола.

Дополнительная информация: конфигурирование расширенных списков управления доступом для различных протоколов

Конфигурирование расширенных списков управления доступом для протокола ICMP

Списки ACL для протокола ICMP имеют следующий синтаксис:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard*[*icmp-type* [*icmp-code*] | *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Конфигурирование расширенных списков управления доступом для протокола IGMP

Списки ACL для протокола IGMP имеют следующий синтаксис:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard*[*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Конфигурирование расширенных списков управления доступом для протокола TCP

Списки ACL для протокола TCP имеют следующий синтаксис:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Конфигурирование расширенных списков управления доступом для протокола UDP

Списки ACL для протокола UDP имеют следующий синтаксис:

access-list *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]

Стандартные значения параметров расширенных списков ACL

В расширенном списке управления доступом в конце стандартно помещается неявная запись, которая запрещает любой доступ (**deny**). Следует помнить, что стандартно сконфигурированный список (т.е. список без единой пользовательской записи) запрещает все!

В конце директивы расширенного списка управления доступом можно указать необязательный параметр — номер порта TCP или UDP, который позволяет более точно контролировать потоки данных, проходящие через устройство (рис. 22.12).

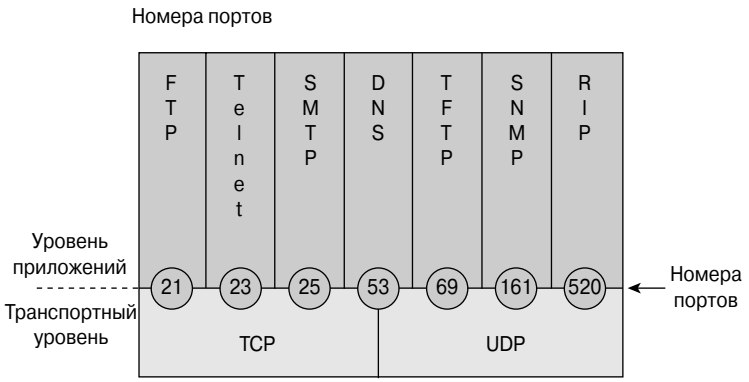


Рис. 22.12. Номера портов протоколов транспортного уровня и соответствующих приложений

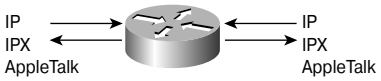
В табл. 22.4 перечислены наиболее часто используемые номера портов UDP и TCP.

Таблица 22.4. Некоторые зарезервированные номера портов TCP и UDP

Десятичное число	Ключевое слово	Описание
0	Нет	Зарезервирован
1-4	Нет	Не назначены
5	RJE	Удаленные задания
7	ECHO	Эхо
9	DISCARD	Уничтожение пакета
11	USERS	Активные пользователи
13	DAYTIME	Дата и время
15	NETSTAT	Список активных соединений
17	QUOTE	Цитата дня
19	CHARGEN	Генератор символов
20	FTP-DATA	Протокол FTP (данные)
21	FTP	Протокол FTP
23	TELNET	Терминальное соединение
25	SMTP	Протокол SMTP
53	DOMAIN	Служба DNS
69	TFTP	Протокол TFTP
80	HTTP	Гипертекстовый протокол (WWW)

Команда **ip access-group** используется для того, чтобы привязать существующий расширенный список доступа к интерфейсу. Только один список доступа может быть установлен на одном интерфейсе, в одном направлении и для одного протокола, как показано на рис. 22.13. Формат команды следующий:

```
Router(config-if)# ip access-group access-list-number {in | out}
```



Один список в одном направлении,
для одного порта и для одного протокола

Рис. 22.13. Правила использования списков управления доступом

Практическое задание 22.2.1a. Конфигурирование расширенных списков управления доступом

В этой лабораторной работе необходимо спланировать, сконфигурировать и применить расширенные списки управления доступом, которые разрешат или запретят передачу отдельных пакетов. Список ACL также необходимо проверить, чтобы определить, был ли достигнут желаемый результат.

Практическое задание 22.2.1b. Расширенные списки управления доступом

В этой лабораторной работе необходимо сконфигурировать расширенный список ACL, который запретит или разрешит определенные типы трафика из определенной сети в другую сеть, от узла в определенную сеть и из сети к определенному узлу.

Использование именованных списков управления доступом

Именованные списки управления доступом впервые были представлены в операционной системе Cisco IOS 11.2; они позволяют обращаться к стандартным и расширенным спискам управления доступом посредством символьной строки — имени списка. Именованным спискам управления доступом присущи следующие преимущества:

- в символьном имени можно указать краткое интуитивно понятное описание списка;
- исключен лимит в 99 стандартных и 100 расширенных списков управления доступом;
- администратор может изменять списки управления доступом без их удаления и повторного введения.

Именованные списки управления доступом создаются с помощью команды **ip access-list**. Синтаксис именованных списков управления доступом выглядит следующим образом:

```
ip access-list {extended | standard} name
```

Такая команда переведет устройство в режим конфигурирования именованного списка ACL:

```
Router(config-std-nacl)#
```

или

```
Router(config-ext-nacl)#
```

В режиме конфигурирования списка доступа можно указать одно или несколько условий (так называемых директив) для разрешения или блокирования доступа. При конфигурировании именованного списка доступны следующие опции:

```
Router(config-std-nacl)#permit | deny
{source [source-wildcard]| any [log]
```

или

```
Router(config-ext-nacl)#permit | deny protocol source
source-wildcard [operator [ port]] destination destination-wildcard
[ operator [ port]] [established] [precedence precedence] [tos tos]
[log] [time-range time-range-name]
```

Операнд разрешения или запрета (**permit** или **deny**) указывает маршрутизатору, какие действия следует выполнять, когда пакеты будут проверяться на соответствие другим критериям, указанным в директиве списка управления доступом, т.е. отправить или отбросить пакет. В примере 22.5 показано, как применять именованный список управления доступом.

Пример 22.5. Директивы именованного списка управления доступом

```
! Создание именованного списка ACL:
Rt(config)# ip access-list extended server-access
Rt(config-ext-nacl)# permit tcp any host 131.108.101.99 eq smtp
Rt(config-ext-nacl)# permit udp any host 131.108.101.99 eq domain
Rt(config-ext-nacl)# deny ip any any log
Rt(config-ext-nacl)# ^Z
! Привязка именованного списка ACL к интерфейсу:
Rt(config)# interface fastethernet0/0
Rt(config-if)# ip access-group server-access out
Rt(config-if)# ^Z
```

В приведенном выше примере списку доступа присваивается имя “server-access” (“доступ к серверу”); потом список доступа применяется к интерфейсу `Fast Ethernet 0/0`. Данный список доступа предоставляет возможность пользователям обратиться только к почте и службе DNS; все прочие запросы будут отклонены.

Именованный список управления доступом позволяет удалять отдельные директивы, но новые записи могут быть добавлены только в конец списка, как показано в примере 22.6.

Пример 22.6. Конфигурирование именованного списка управления доступом

```
router# configure terminal
Enter configuration commands, one per line.
router(config)# ip access-list extended test
router(config-ext-nacl)# permit ip host 2.2.2.2 host 3.3.3.3
router(config-ext-nacl)# permit tcp host 1.1.1.1 host 5.5.5.5 eq www
router(config-ext-nacl)# permit icmp any any
router(config-ext-nacl)# permit udp host 6.6.6.6 10.10.10.0
0.0.0.255 eq domain
router(config-ext-nacl)# ^Z
1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-1
router# show access-list
Extended IP access list test
    permit ip host 2.2.2.2 host 3.3.3.3
    permit tcp host 1.1.1.1 host 5.5.5.5 eq www
    permit icmp any any
    permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq domain
router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# ip access-list extended test
!--- Команда, приведенная ниже, удаляет запись в именованном списке ACL.
router(config-ext-nacl)# no permit icmp any any
!--- Команда, приведенная ниже, добавляет запись в именованном
   списке ACL.
router(config-ext-nacl)# permit gre host 4.4.4.4 host 8.8.8.8
router(config-ext-nacl)# ^Z
1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-1
router# show access-list
Extended IP access list test
    permit ip host 2.2.2.2 host 3.3.3.3
    permit tcp host 1.1.1.1 host 5.5.5.5 eq www
    permit udp host 6.6.6.6 10.10.10.0 0.0.0.255 eq domain
    permit gre host 4.4.4.4 host 8.8.8.8
```

Перед тем как начинать внедрение и конфигурирование именованных списков контроля доступа, следует учесть такие две особенности:

- именованные списки управления доступом несовместимы с операционной системой Cisco IOS версии ниже 11.2;
- одни и те же названия не могут быть использованы для разных списков управления доступом. Например, нельзя определить стандартный и расширенный списки управления доступом с одним и тем же именем George (Джордж).

Последовательность команд, показанных в примере 20.7, используется для указания имени стандартного списка управления доступом “Internetfilter” и имени расширенного списка управления доступом “marketing_group”. Далее используются команды конфигурирования интерфейса e0/5, которые задают IP-адрес. и затем оба списка управления доступом применяются к данному интерфейсу (Ethernet 0/5).

Пример 22.7. Именованные списки управления доступом

```
. . .
ip access-list standard Internetfilter
permit 1.2.3.4
deny any
ip access-list extended marketing_group
permit tcp any 171.69.0.0 0.255.255.255 eq telnet
deny tcp any any
deny udp any 171.69.0.0 0.255.255.255 lt 1024
deny ip any log
interface Ethernet0/5
ip address 2.0.5.1 255.255.255.0
ip access-group Internetfilter out
ip access-group marketing_group in
```

Практическое задание 22.2.3a. Именованные списки управления доступом
В этой лабораторной работе необходимо спланировать, сконфигурировать и применить именованные списки управления доступом, которые разрешат или запретят передачу отдельных пакетов. Список ACL также необходимо проверить и определить, был ли достигнут желаемый результат.

Практическое задание 22.2.3b. Простейшие расширенные списки управления доступом для создания зоны DMZ
В этой лабораторной работе необходимо создать несложный расширенный список для зоны DMZ (DeMilitarized Zone — демилитаризованная зона)[4].

Практическое задание 22.2.3c. Использование разнообразных функций списков управления доступом (усложненная лабораторная работа)
В этой лабораторной работе необходимо создать несколько списков ACL, которые будут использованы для контроля потоков данных из сети Internet на нескольких маршрутизаторах.

Правила размещения списков управления доступом

Как мы уже говорили, списки управления доступом используются для контроля потоков данных путем фильтрации пакетов и уничтожения нежелательных потоков. От того, где размещен список, зависит эффективность его применения. Если список размещен в нужном месте, он не только фильтрует пакеты, но также может существенно повысить быстродействие сети. Для фильтрации потоков данных список управления доступом должен находиться в том месте, где он больше всего будет влиять на трафик и производительность сети.

Предположим, основная цель политики предприятия состоит в том, чтобы запретить telnet- и FTP-трафик на маршрутизаторе A и к порту E1 маршрутизатора Г для

[4] *Применительно к сетевой инфраструктуре предприятия обозначает "нейтральную" пограничную подсеть, отделенную сетевыми брандмауэрами и от публичных, и от внутренних сетей. — Прим. ред.*

соответствующей коммутируемой локальной сети, как показано на рис. 22.14. В то же время все остальные потоки данных должны проходить беспрепятственно. Добиться поставленной цели можно несколькими способами. Рекомендуется подход, связанный с использованием расширенного списка управления доступом, который выполняет проверку как адреса отправителя, так и адреса получателя. Один расширенный список управления доступом следует разместить на интерфейсе To0 маршрутизатора А, тогда пакеты не пройдут через Ethernet-интерфейс маршрутизатора А и далее через последовательные интерфейсы маршрутизаторов Б и В и не попадут на маршрутизатор Г. Такая конфигурация уменьшит трафик в сети между маршрутизаторами А и Г. Потоки данных в обратном направлении (т.е. те потоки, в которых адреса отправителя и получателя поменяны местами относительно уже установленного списка контроля доступа) остались разрешены в маршрутизаторах.

Рекомендуется размещать список управления доступом как можно ближе к отправителю данных, трафик которого нужно запретить. Стандартные списки не проверяют адрес получателя, поэтому стандартный список необходимо размещать как можно ближе к получателю трафика. Например, если нужно запретить передачу данных от маршрутизатора А маршрутизатору Г, стандартный список следует разместить на интерфейсе Fa0/0 маршрутизатора Г.

ВНИМАНИЕ!

Списки управления доступом могут замедлить выполнение маршрутизатором процессов маршрутизации. Устройству приходится считывать больше информации из пакета и запускать алгоритм поиска и сравнения еще до того, как пакет может быть передан процессу маршрутизации.

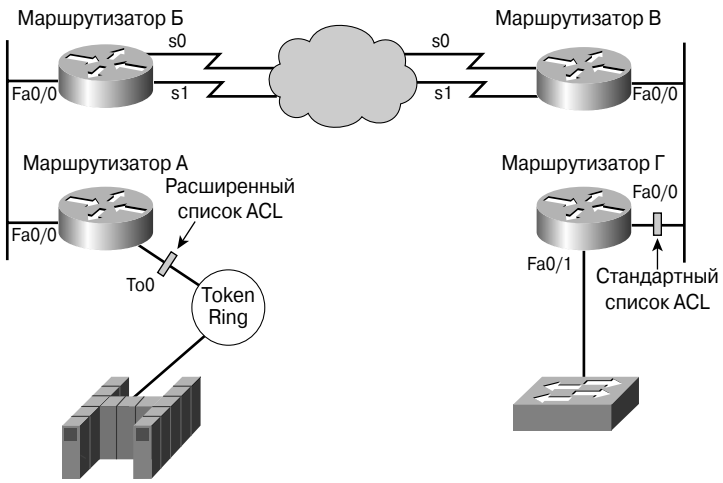


Рис. 22.14. Правила размещения списков управления доступом

В расширенных конфигурациях доступна специализированная функция, которая называется Turbo ACL. Она позволяет компилировать список управления доступом и намного ускоряет процесс поиска в списке. Опция Turbo ACL немного повышает эффективность работы алгоритма поиска, а также позволяет намного быстрее и эффективнее анализировать список управления доступом.

Интерактивная презентация: правила размещения списков ACL
В этой презентации подробно описаны правила размещения списков управления доступом.

Брандмауэры

Брандмауэр — это обычно компьютер или сетевое оборудование, которое является связующим звеном между пользователем и внешним миром и защищает внутреннюю сеть от вторжений. В большинстве случаев вторжение происходит из глобальной сети Internet или из тысяч удаленных сетей, которые она связывает. Обычно сетевой брандмауэр состоит из нескольких устройств, которые функционируют совместно, защищая сеть и предотвращая нежелательный или нелегальный доступ к ресурсам извне. Структура простого брандмауэра проиллюстрирована на рис. 22.15.

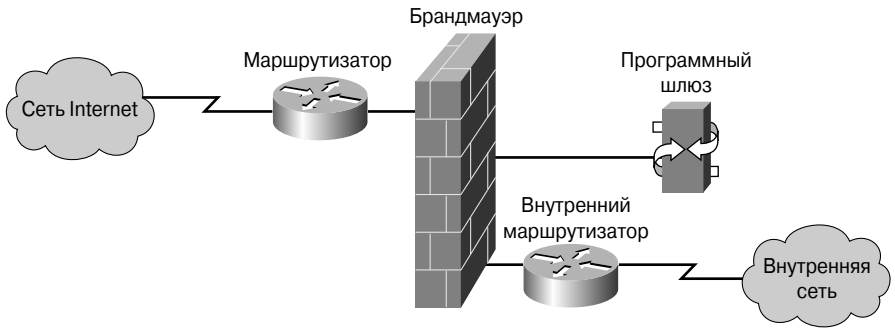


Рис. 22.15. Структура брандмауэра

В инфраструктуре, построенной с использованием брандмауэра, маршрутизатор, который соединен с сетью Internet, называется *внешним (exterior router)*. Внешний маршрутизатор перенаправляет все входящие пакеты на программный шлюз (application gateway[5]). Маршрутизатор, который соединен с внутренней сетью организации, называется *внутренним (interior)*. Внутренний маршрутизатор принимает пакеты только от шлюза. Таким образом, шлюз контролирует предоставление сетевых служб и доступа как во внутреннюю сеть, так и из нее. Например, только некоторым пользователям может быть предоставлено право работы в сети Internet или только определенным приложениям разрешено устанавливать соединение между

[5] *Часто этим термином обозначают систему, выполняющую преобразование из одного естественного формата в другой. — Прим. ред.*

внутренним и внешним узлами. Если единственным допустимым приложением является электронная почта, то на маршрутизаторе должно быть установлено соответствующее ограничение и через этот маршрутизатор должны проходить только пакеты, связанные с почтовой службой. Такой подход позволяет защищать не только шлюз и предотвращать его переполнение неавторизированными пакетами, но и обеспечить высокий уровень безопасности внутренней сети.

Использование списков управления доступом совместно с брандмауэрами

Рекомендуется использовать списки управления доступом на маршрутизаторах, которые исполняют роль брандмауэров (firewall) и размещаются между внутренней сетью и внешней, такой, как сеть Internet. Брандмауэр создает точку изолирования сети, в результате чего внешний трафик не оказывает воздействия на внутреннюю сеть и логику ее работы. Списки управления доступом могут также использоваться на маршрутизаторах, расположенных между двумя сегментами или частями сети, для управления входящими и исходящими потоками данных, трафиком между сетями или потоками данных от некоторого участка одной из подсетей.

Для обеспечения большей безопасности сети всегда следует устанавливать минимальную конфигурацию с использованием списков контроля доступа на *граничных маршрутизаторах (border routers)*, т.е. маршрутизаторах, расположенных на границах сети, называемых также *маршрутизаторами-брандмауэрами*. Такой подход в большей степени изолирует частную сеть от внешней или от менее контролируемой части сети, обеспечивая приемлемый и достаточно высокий уровень защиты.

На граничных маршрутизаторах списки управления доступом могут быть созданы для каждого сетевого протокола, который используется на интерфейсах маршрутизатора. При этом конфигурацию списка и сам граничный маршрутизатор можно настроить так, что входные, выходные или и те, и другие потоки данных будут фильтроваться на заданном интерфейсе.

Ограничение доступа к виртуальным терминалам

Стандартные и расширенные списки управления воздействуют на пакеты, которые следуют через маршрутизатор. Они не блокируют доступ пакетам данных, которые создаются внутри маршрутизатора. Например, стандартно расширенные списки ACL, которые применяются в исходящем направлении и рассчитаны на telnet-трафик, не предотвращают telnet-сеансов, которые инициируются на маршрутизаторе.

Кроме физических интерфейсов, таких, как Fa0/0 и S0/0, у каждого маршрутизатора есть так называемые виртуальные порты, которые называют линиями vty. У маршрутизатора обычно есть 5 линий vty, которые пронумерованы цифрами от 0 до 4, как показано на рис. 22.16. В целях повышения безопасности администратор может разрешить или запретить доступ посредством виртуальных терминальных линий к маршрутизатору, вместо того чтобы запрещать определенные типы трафика от маршрутизатора к получателям. Так, например, администратор может сконфигурировать списки управления доступом, которые разрешают терминальное подключение

к маршрутизатору для управления устройством и устранения неисправностей, но соответствующие службы могут быть запрещены в остальной части сети.

Ограничение vty-доступа обычно не используется в качестве механизма управления потоками данных; такая функция необходима для повышения уровня защиты сети. Терминальное подключение использует протокол telnet и позволяет установить *нефизическое* соединение с маршрутизатором, поэтому существует только одна разновидность vty-списка управления доступом. Одинаковые ограничения должны быть использованы для всех виртуальных линий, потому что невозможно заранее сказать, к какой именно линии присоединится пользователь.

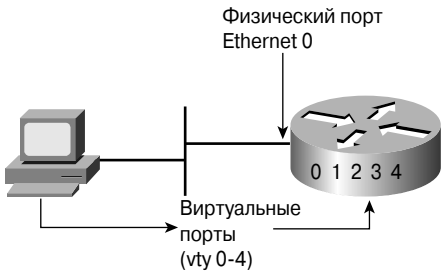


Рис. 22.16. Ограничение доступа к линиям vty при помощи списков управления доступом

Несмотря на то что список управления доступом для виртуальных терминалов выглядит точно так же, как и любой другой список ACL (для физического интерфейса устройства), для привязки vty-списка к терминальной линии используется команда **access-class** вместо **access-group**. Как создать и применить список доступа к виртуальным терминалам, показано в примере 22.8.

Пример 22.8. Ограничение доступа к виртуальным терминалам при помощи списков ACL

```
! Создадим стандартный список управления доступом:
!
Rt1(config)# access-list 2 permit 172.16.1.0 0.0.0.255
Rt1(config)# access-list 2 permit 172.16.2.0 0.0.0.255
Rt1(config)# access-list 2 deny any
! Применим список к линиям:
Rt1(config)# line vty 0 4
Rt1(config)# login
Rt1(config)# password secret
Rt1(config)# access-class 2 in
```

При использовании списков ACL для ограничения доступа к линиям виртуальных терминалов следует помнить следующие правила:

- именованные или нумерованные списки можно использовать для управления доступом к физическому интерфейсу;

- только нумерованный список доступа может быть использован для линий виртуальных терминалов;
- одинаковые ограничения должны быть установлены для всех виртуальных линий терминалов, потому что пользователь может попытаться присоединиться к любой из них.

Практическое задание 22.2.6. Ограничение доступа к линиям виртуальных терминалов
В этой лабораторной работе необходимо создать несколько списков ACL, которые будут использованы для контроля потоков данных из сети Internet на нескольких маршрутизаторах.

Резюме

В этой главе были рассмотрены следующие ключевые понятия:

- существуют два основных типа списков управления доступом: стандартные и расширенные;
- именованные списки управления доступом позволяют идентифицировать список доступа по имени вместо номера;
- списки управления доступом могут быть сконфигурированы для всех маршрутизируемых сетевых протоколов;
- списки управления доступом обычно используются на маршрутизаторах, выполняющих роль брандмауэров, которые размещены между внутренней и внешней сетью, такой, как Internet;
- списки управления доступом также используются для ограничения доступа к виртуальным терминалам маршрутизаторов;
- в маршрутизаторе корпорации Cisco списки управления доступом выполняют несколько функций, в частности, они обеспечивают безопасность устройства;
- списки управления доступом используются для управления трафиком;
- для некоторых протоколов на одном интерфейсе могут быть установлены два списка управления доступом: один — во входящем, другой — в исходящем направлении;
- при использовании списков управления доступом после проверки пакета на соответствие директиве списка пакету может быть разрешено или запрещено использование некоторого интерфейса. Для привязки списка к интерфейсу используется команда **`access-group`**;
- биты инвертированной маски (нули и единицы) указывают способ обработки соответствующего бита IP-адреса.

Обратите внимание на относящиеся к главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложены в данной главе.

Ключевые термины

Битовая корзина (bit bucket) используется для уничтожения отброшенных (или уничтоженных) маршрутизатором пакетов.

Брандмауэр (firewall) — одно или более сетевых устройств, таких, как маршрутизаторы или серверы доступа, предназначенных для создания буферной зоны между соединенными открытыми и частными сетями. Для обеспечения безопасности частных сетей в брандмауэре используются списки управления доступом и другие методы.

Внешний маршрутизатор (exterior router) — в структуре брандмауэра это маршрутизатор, который подсоединен к сети Internet. Он перенаправляет все входящие пакеты на программный шлюз для их дальнейшей обработки и анализа.

Внутренний маршрутизатор (interior router) — это маршрутизатор, который подсоединен ко внутренней сети. Внутренний маршрутизатор разрешает трафик только от программного шлюза. Шлюз контролирует сетевые потоки данных в обоих направлениях: как из внешней сети во внутреннюю, так и из внутренней наружу.

Граничный маршрутизатор (border router) — устройство, размещенное на границе сети и обеспечивающее функции защиты некоторой частной области сети от внешних сетей или от слабо контролируемых областей сети.

Именованный список управления доступом (named ACL) — это стандартный или расширенный список управления доступом, в котором вместо номера используется имя.

Очередь (queue) — механизм, позволяющий задать с помощью списков управления доступом такой принцип обработки трафика, что определенные потоки данных, например, на основании номера протокола, будут отправлены прежде всех остальных. Очередность является настраиваемым механизмом, который позволяет указать, по какому именно признаку следует передавать некоторые данные раньше: например, трафик можно разделить по адресам, по протоколам и т.п.

Расширенный список управления доступом (Extended Access Control List — Extended ACL) — список управления доступом, который позволяет проверять адреса отправителя и получателя, а также другие критерии, установленные в правилах расширенного списка управления доступом.

Список управления доступом (Access Control List — ACL) — способ контроля или ограничения трафика сети, который отвечает различным критериям, установленным определенными правилами.

Стандартный список управления доступом (Standard Access Control List — Standard ACL) — список управления доступом, осуществляющий фильтрацию на основе сравнения адреса отправителя пакетов с заданными в нем правилами.

Контрольные вопросы

Чтобы проверить, насколько хорошо вы усвоили темы и понятия, описанные в этой главе, ответьте на предлагаемые вопросы. Ответы на них приведены в приложении Б, "Ответы на контрольные вопросы".

1. Наиболее распространенными функциями списков ACL является фильтрация пакетов внутри маршрутизатора, которая предполагает защиту внутренних сетей от неавторизованного или нелегального доступа извне или из сети Internet, и функция ограничения доступа к виртуальным терминалам маршрутизатора?

а) Да.

б) Нет.

2. Аббревиатура ACL означает:

а) Accessibility Control List (список управления доступностью).

б) Accountability Control list (список управления ответственностью).

в) Assessment Control List (список управления оценками).

г) Access Control List (список управления доступом).

3. Какой тип списка управления доступом (ACL) позволяет использовать в своих правилах только IP-адреса отправителей?

а) Расширенный.

б) Именованный.

в) Стандартный.

г) Маршрутизаторный.

4. Какой список управления доступом (ACL) позволяет использовать в своих правилах IP-адреса отправителей, IP-адреса получателей и другие параметры?

а) Расширенный.

б) Именованный.

в) Стандартный.

г) Маршрутизаторный.

5. Какой из указанных ниже списков управления доступом (ACL) позволяет использовать в качестве идентификатора название вместо числа?

а) Расширенный.

б) Именованный.

в) Стандартный.

г) Маршрутизаторный.

6. Где предпочтительнее всего размещать расширенные списки управления доступом (ACL)?

   а) В сети Internet.

   б) В магистральных каналах сети.

   в) Как можно ближе к отправителям трафика.

   г) Ни в одном из перечисленных выше мест.

7. Какая команда используется для того, чтобы привязать список управления доступом к виртуальному терминалу?

   а) **ip access-list**.

   б) **ip access-class**.

   в) **ip access-group**.

   г) **access-class**.

8. С помощью какой команды можно точно определить, установлен ли на интерфейсе список ACL?

   а) **show running-config**.

   б) **show ip protocols**.

   в) **show ip interface**.

   г) **show ip network**.

9. Какую из указанных ниже команд нужно использовать, если необходимо разрешить передачу потоков данных на основании адресов получателей или определенного типа протокола?

   а) `Router# **access-list** *access-list-number* {**permit** | **deny**} {*test conditions*}.`

   б) `Router(config)# **access-list** *access-list-number* {**permit** | **deny**} {*test conditions*}.`

   в) `Router(config-if)# **access-list** *access-list-number* {**permit** | **deny**} {*test conditions*}.`

   г) Все указанные команды неправильны.

10. Стандартный IP-список управления доступом запрещает или разрешает маршрутизацию пакета в зависимости от того, с какого IP-адерса был отправлен пакет, а также в зависимости от того, какой стек протоколов или протокол используется?

    а) Да.

    б) Нет.

11. За счет какого из указанных ниже факторов список управления доступом повышает безопасность сети?

а) Содержимое поля данных пакета.

б) Сеть-, узел- или подсеть-получатель пакета.

в) Сеть-, узел- или подсеть-отправитель пакета.

г) Тип сетей, через которые маршрутизируются пакеты.

12. В каком сетевом оборудовании устанавливаются списки управления доступом для повышения безопасности сети?

а) В концентраторе.

б) В маршрутизаторе.

в) На мосту.

г) На коммутаторе.

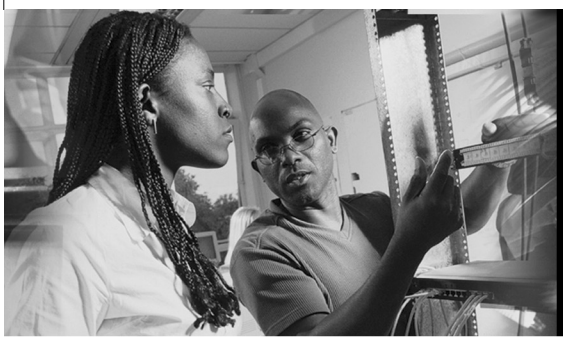
13. Что именно выполняет следующий список управления доступом: **`access-list 1 permit 204.211.19.162 0.0.0.0`**?

а) Запрещает передачу данных только из определенной сети.

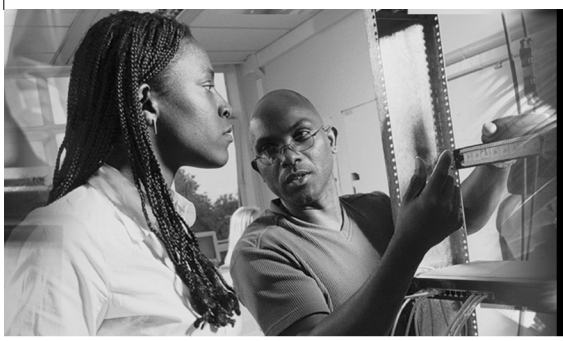
б) Разрешает передачу данных только для определенного узла.

в) Разрешает передачу данных только из определенной сети.

г) Не выполняет ничего из перечисленного в пунктах а–в.



ЧАСТЬ III
ПРИЛОЖЕНИЯ



ПРИЛОЖЕНИЕ А

Структурированная кабельная система

В этом приложении...

- описаны основные понятия структурированной кабельной системы;
- описаны правила и стандарты построения кабельных систем для разработки и установки масштабируемых сетей;
- рассмотрены подсистемы структурированной кабельной сети, точки демаркации, подробно описаны телекоммуникационные узлы и различные их разновидности;
- рассмотрены стандарты Ассоциации промышленности средств связи (Telecommunications Industry Association — TIA), Ассоциации электронной промышленности (Electronics Industries Association — EIA), Европейского Комитета по стандартизации электротехнических средств (European Committee for Electrotechnical Standardization) и всемирно известной Международной организации по стандартизации (International Organization for Standardization — ISO);
- перечислены специальные требования к кабельной системе в рабочей зоне;
- описано, как выполнять электротехнические работы, и перечислены правила безопасности при работе с электрическими приборами;
- описаны правила безопасности при работе со стремянкой и требования к одежде монтажника;
- перечислены основные инструменты, с которыми приходится сталкиваться прокладчику кабеля, а также основные электроизмерительные приборы и кабельные тестеры;
- указаны основные этапы установки структурированной кабельной системы и их привязка к типовому проекту сети;
- приведено описание бизнес-процессов и описана их взаимосвязь с кабельной структурой.

Ключевые определения главы

Ниже перечислены основные определения главы, полные расшифровки терминов приведены в конце:

структурированная кабельная система, с. 977,
телекоммуникационный узел, с. 977,
точка демаркации, с. 977,
магистральное соединение, с. 978,
демарк, с. 981,
ассоциация промышленности средств связи, с. 982,
ассоциация электронной промышленности, с. 982,
коммутационная панель, с. 985,
соединительный кабель, с. 988,
главный коммутационный узел, с. 990,
промежуточный коммутационный узел, с. 990,
горизонтальный кабельный узел, с. 990,
кабельная система, с. 991,
горизонтальная кабельная система, с. 991,
многопортовый блок розеток, с. 994,
комитет CENELEC, с. 1000,
закон о технике безопасности и гигиене труда, с. 1006,
справочник по безопасности материалов, с. 1006,
лаборатория по технике безопасности, с. 1006,
национальные электротехнические нормативы, с. 1007,
мультиметр, с. 1010,
кабельная подставка, с. 1024,
инструментальный барабан, с. 1025,
кабельный канал, с. 1032,
динамический рефлектометр, с. 1055.

В этом приложении основное внимание уделено следующим вопросам:

- структурированные кабельные системы, их стандарты и условные обозначения;
- личная безопасность;
- инструментарий монтажника;
- процесс развертывания кабельной системы;
- финальный этап построения сети;
- коммерческие вопросы;
- практические примеры.

Обратите внимание на относящиеся к этой главе интерактивные материалы, которые находятся на компакт-диске, предоставленном вместе с книгой: электронные лабораторные работы (e-Lab), видеоролики, мультимедийные интерактивные презентации (PhotoZoom). Эти вспомогательные материалы помогут закрепить основные понятия и термины, изложенные в главе.

Структурированные кабельные системы, их стандарты и условные обозначения

Структурированной кабельной системой (structured cabling system) называют упорядоченную телекоммуникационную инфраструктуру, которая соответствует стандартам и начинается в *точке демаркации* (demarcation point), проходит через различные *телекоммуникационные узлы* и составляет *рабочую область* (work area). Такая система должна предполагать возможность расширения в дальнейшем.

К наиболее важным вопросам, связанным со структурированной кабельной системой, можно отнести:

- правила построения структурированной кабельной системы;
- подсистемы кабельной системы;
- масштабируемость структуры;
- точки демаркации;
- телекоммуникационные узлы и серверные комнаты;
- размещение рабочих областей;
- магистральные, промежуточные и горизонтальные соединения;
- соблюдение стандартов Ассоциации промышленности средств связи (Telecommunications Industry Association — TIA), Ассоциации электронной промышленности (Electronics Industries Association — EIA);
- соблюдение стандартов Международной организации по стандартизации (International Organization for Standardization — ISO);
- соблюдение стандартов и сводов правил США;
- учет новых стандартов.

Правила построения кабельной системы локальных сетей

Структурированная кабельная система — это систематизированный подход к прокладке кабеля. Этим термином обозначают метод упорядоченного развертывания физической основы сети, которая проста и понятна как монтажникам, так и сетевым администраторам и другим техническим специалистам, которым приходится иметь с ней дело.

Ниже перечислены основные требования, которых следует придерживаться при реализации проектов структурированных кабельных систем, чтобы сделать их максимально эффективными и удобными.

- **Следует стремиться к завершенности решения**. Оптимальное решение для физической структуры сети включает в себя все компоненты, которые используются для соединения устройств, размещения кабеля, управления каналами и идентификации соединений.

- **Необходимо учитывать возможность расширения структуры в будущем**. Общее количество развернутых соединений должно быть выбрано с учетом запросов, которые могут возникнуть позднее. Витая пара категорий 5e и 6 или оптоволоконные соединения должны быть использованы везде, где это возможно, поскольку потребность в высококачественной инфраструктуре может возникнуть в любой момент. Физическая инфраструктура сети должна быть рассчитана как минимум на десятилетний срок службы.
- **Сеть не должна зависеть от устройств и технологий одного производителя**. Несмотря на то что закрытые технологии или фирменные стандарты могут стоить дешевле на первом этапе построения сети, дальнейшее их сопровождение может обойтись в значительную сумму. Нестандартные системы определенного производителя могут значительно усложнить и даже сделать невозможным процессы изменения, усовершенствования и расширения сети в дальнейшем.

Дополнительная информация: правила построения структурированной кабельной системы

За дополнительной информацией по вопросам, касающимся правил развертывания структурированных кабельных систем, обратитесь на Web-сайт `www.panduit.com` и найдите в нем документ под названием *Rules of Structured Cabling (Правила построения структурированной кабельной системы)*.

Подсистемы структурированной кабельной системы

Структурированную кабельную систему обычно подразделяют на семь подсистем (рис. А.1). Каждая подсистема выполняет определенные функции и обеспечивает передачу обычных и голосовых данных по физическим носителям.

Наиболее важными подсистемами являются следующие:

- точка демаркации (demarcation point или demarc);
- *телекоммуникационный узел* (Telecommunications Room — TR);
- *магистральные соединения*, которые часто называют *вертикальной* кабельной системой;
- распределительная кабельная система, зачастую носящая название *горизонтальной*;
- рабочая область;
- серверные помещения;
- административные помещения.

Точкой демаркации (demarc) называют узел, в котором кабель провайдера службы подключается к кабельной системе организации или здания.

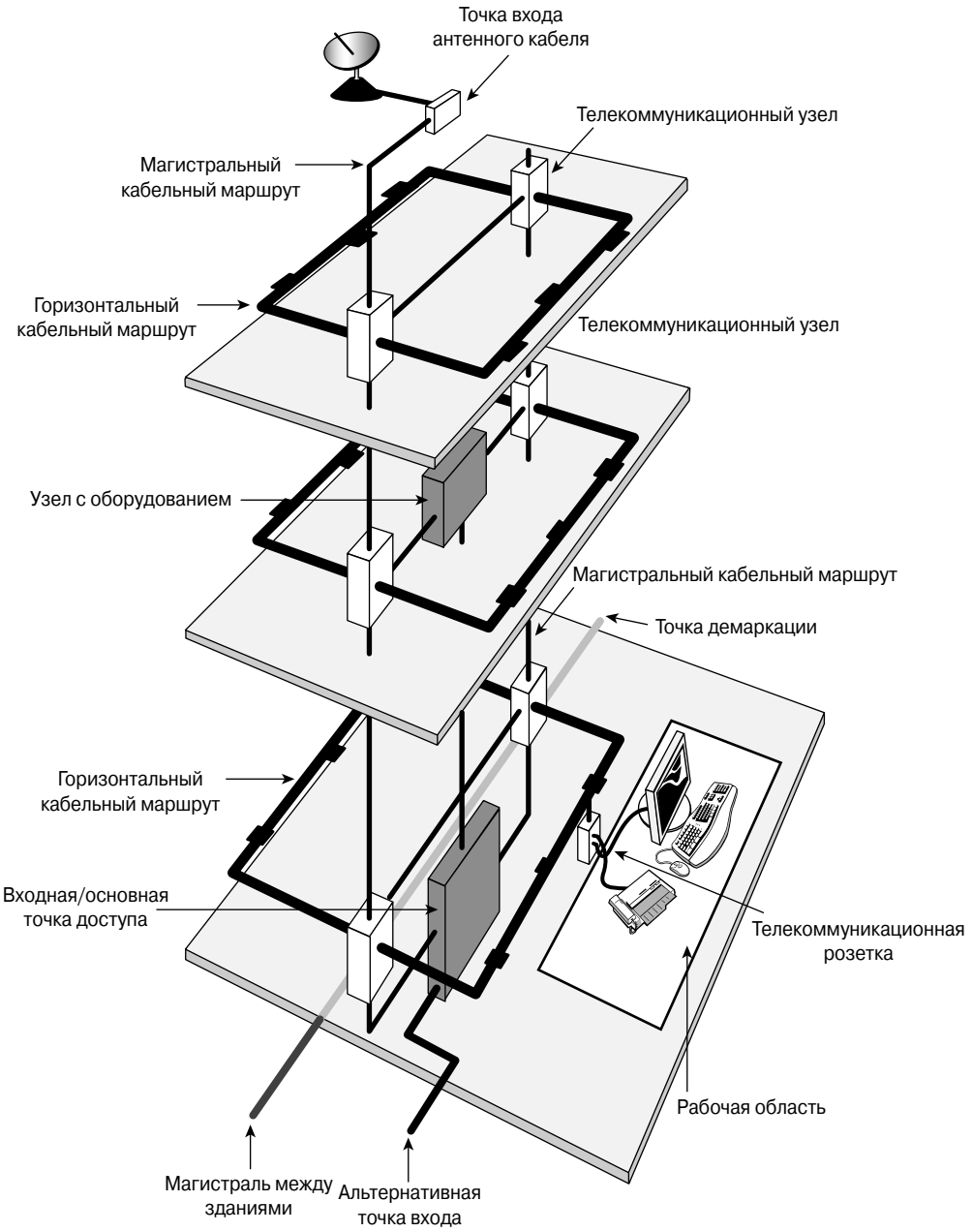


Рис. А.1. Подсистемы структурированной кабельной системы

Магистральной кабельной системой обычно называют кабели, которые соединяют точку демаркации и серверную комнату, а также служат для подключения к серверной комнате телекоммуникационных узлов здания или организации. Горизонтальной кабельной системой называют кабели, которые проложены от телекоммуникационных узлов к рабочим областям. Телекоммуникационные узлы обеспечивают подключение горизонтальных кабельных систем к магистральным.

Перечисленные выше подсистемы составляют структурированную кабельную систему, которая по своей природе является распределенной. Средства управления такой системой обычно ограничены возможностями активного оборудования (ПК, коммутаторы, концентраторы и др.). Разработка логичной и структурированной физической основы сети, в которой кабель проложен согласно стандартам (т.е. "правильно"), защищен и его легко идентифицировать, а соединения правильно подключены, — это наиболее важная проблема, от успешного решения которой зависит производительность сети и простота дальнейшего ее расширения.

Масштабируемость кабельной системы

Локальная сеть (Local Area Network — LAN), которая может быть увеличена в размере с течением времени, называется масштабируемой. Для любого технического специалиста очень важно планировать такую особенность заранее, в процессе оценки количества кабелепроводов и соединений в рабочей области.

Более того, на сегодняшний день общепринято прокладывать избыточное количество кабельных соединений в рабочей области на случай дальнейшего расширения инфраструктуры, как, например, принято монтировать дополнительный кабель к каждому рабочему месту "на всякий случай".

Масштабируемость магистральной кабельной структуры

Чтобы определить количество избыточных медных кабелей для магистрали, прежде всего подсчитайте требуемое общее количество соединений и добавьте некоторый "запас", обычно — около 20%.

Одним из методов резервирования производительности на будущее является установка волоконно-оптических кабелей и соответствующего оборудования в магистральной сети. За счет обновления модулей оптического оборудования (которые, например, содержат лазеры других моделей) можно достичь более высокой производительности без замены кабеля.

Масштабируемость рабочей области

Очевидным кажется тот факт, что к каждому рабочему месту необходимо провести два кабеля: один — для голосовой связи (телефон) и второй — для передачи данных. Тем не менее, некоторым устройствам может понадобиться одно из этих соединений для нормальной работы. Дополнительные соединения могут потребоваться сетевым принтерам, факс-аппаратам, портативным компьютерам или просто зашедшим "в гости" пользователям.

Рекомендуется использовать настенные розетки с несколькими портами, вместо того чтобы просто устанавливать на конце кабеля разъем для подключения к сетевой карте. Разъемы или порты обязательно нужно промаркировать (или использовать разноцветные разъемы), чтобы легко было идентифицировать номер и тип соединения. Стандарты администрирования сетей требуют, чтобы каждое соединение было промаркировано на обоих концах для облегчения поиска и устранения неисправностей.

Все большую популярность приобретает *технология передачи голоса через Internet-протокол* (Voice over Internet Protocol — VoIP). Она позволяет специализированным телефонам использовать сети передачи данных при установлении звонка. Несомненным преимуществом этой технологии является то, что она позволяет сэкономить значительные средства за счет замены междугородних звонков службами передачи голоса по компьютерным сетям. Другие сетевые устройства, как, например, принтеры и компьютеры, могут быть включены непосредственно в такой IP-телефон, который в таком случае будет играть роль концентратора или коммутатора в рабочей области. Даже если известно точное количество рабочих мест, всегда следует оставлять избыточные кабельные соединения, невзирая на тот факт, например, что IP-телефония и потоки видео могут быть переданы по уже существующим компьютерным кабелям.

Для того чтобы учесть дальнейшее расширение сети, например, в офисе какой-либо фирмы, рекомендуется к каждой розетке подводить как минимум один запасной кабель. При реструктуризации предприятия количество работников может удвоиться или даже утроиться. В таком случае именно рабочие области могут быть основной проблемой администратора, особенно если к каждому существующему рабочему месту подведен всего один кабель. Правильное решение, в котором учтена возможность дальнейшего роста, показано на рис. А.2.

Точка демаркации

Точкой демаркации (demarc — *демарк*) называют интерфейс, в котором кабельная система провайдера подключается к магистральной проводке здания (рис А.3). Она представляет собой границу между сферами ответственности провайдера и потребителя. В большинстве существующих сетей такая точка размещена внутри или рядом с точкой присутствия (Point of Presence — POP) других коммунальных служб, таких, как енерго- или водоснабжение.

Провайдер службы несет ответственность за все, что происходит на участке от точки демаркации до своего оборудования. Все, что находится между точкой демаркации и конечными системами пользователей в здании, — это головная боль потребителя.

Местные телефонные компании обычно требуют, чтобы сегмент кабеля от точки входа в здание до распределительного узла не превышал 15 м[1] и был защищен от электрических помех. Обычно такой кабель устанавливается и сопровождается провайдером службы.

[1] *49,2 фута.*

Рис. А.2. Масштабируемое решение

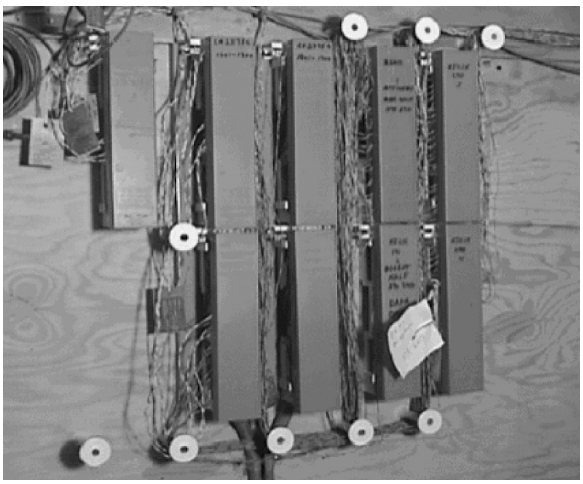


Рис. А.3. Точка демаркации

Ассоциация промышленности средств связи (Telecommunications Industry Association — TIA) и *Ассоциация электронной промышленности* (Electronics Industries Association — EIA) совместно разрабатывают и публикуют индустриальные стандарты. Следует придерживаться таких стандартов при прокладке и сопровождении кабеля как для телефонной связи, так и для передачи данных, чтобы быть уверенным в том, что кабель смонтирован правильно, соответствует требованиям безопасности и обеспечивает необходимую производительность.

В стандарте TIA/EIA-569-A указаны правила, относящиеся к демаркационным узлам и телекоммуникационным шкафам, например, размер, структура и местоположение такого узла рассчитываются, исходя из размеров здания. Если этаж здания имеет площадь большую 2000 м^2, рекомендуется разместить кабельный узел в отдельном помещении, доступ в которое ограничен.

Ниже перечислены наиболее важные условия, которые необходимо выполнить при выборе местоположения точки демаркации.

- На каждые 20 м^2 пола[2] должно приходиться около 1 м^2 свободного места для настенных розеток.
- Стены, пол и потолок помещения, где размещены узлы и телекоммуникационное оборудование, должны быть изготовлены из огнеупорного материала или покрыты двумя слоями огнеупорной краски.
- Настенные панели, кожухи или сами распределительные узлы должны быть покрашены в оранжевый цвет.

Телекоммуникационные узлы и серверные комнаты

Когда кабель проложен до точки демаркации здания, необходимо смонтировать кабельный сегмент от точки входа до телекоммуникационного оборудования потребителя, а именно — в серверное помещение или комнату (Equipment Room — ER). Серверная комната, или просто серверная, — это "сердце" сети передачи данных и голоса. Обычно это достаточно просторное помещение, в котором размещено множество монтажных шкафов, сетевые серверы, маршрутизаторы, коммутаторы, мини-АТС, бесперебойные источники питания, спутниковые приемники, модемы, высокоскоростное Internet-оборудование и многое другое. Все требования к серверным комнатам описаны в стандарте TIA/EIA-569-A.

На крупных предприятиях к серверной комнате могут быть подключены меньшие по размеру телекоммуникационные узлы или комнаты (Telecommunication Rooms — TR), которые могут быть разбросаны по всему зданию (рис. А.4).

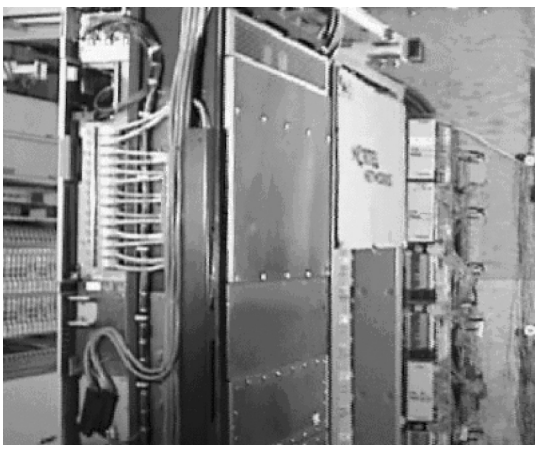


Рис. А.4. Серверная

[2] *215,3 фута*.

Концентратор или коммутационная панель (patch panel) телекоммуникационного узла (TP) могут быть размещены в навесном шкафу с замком, обычном монтажном шкафу или просто в отдельном блоке общего шкафа с оборудованием (рис. А.5).

Рис. А.5. Монтажный шкаф компании Panduit

При размещении телекоммуникационного узла следует руководствоваться следующими правилами:

- если используется навесной монтажный шкафчик, его следует крепить к внешней обшивке (конечно же, с учетом ее жесткости!) таким образом, чтобы он был устойчив. Основное требование к подвеске шкафчика при этом — она должна позволять отклонить шкаф не менее чем на 48 см[3] от стены, чтобы предоставить доступ монтажникам и ремонтным работникам как к обратной стороне шкафа, так и к стене;
- если используется обычный монтажный шкаф, то спереди и сзади от него должно быть свободное место (1 м[4]), чтобы было удобно при необходимости перекоммутировать кабели. Для повышения устойчивости конструкции используется специальная квадратная монтажная пластина (длиной 55,9 см[5]), которая привинчивается к полу;

[3] *18,2 дюйма.*
[4] *3 фута.*
[5] *22 дюйма.*

- если узел, *коммутационная панель* или концентратор размещаются в стойке с оборудованием (с замком и дверью), необходимо, чтобы перед стойкой было свободное пространство (минимум 76,2 см[6]). Обычно такие стойки имеют стандартные размеры: 1,8×0,74×0,66 м[7].

Оборудование необходимо размещать в монтажном шкафу с особой осторожностью. Перед установкой оборудования нужно определить требования к питанию, расположение кабелей и то, насколько просто будет дотянуться до нужного блока или оборудования. Например, коммутационную панель не следует располагать в верхней части монтажного шкафа, поскольку по мере наполнения шкафа оборудованием придется часто переключать соединения, и свисающие сверху провода, несомненно, будут мешать администратору. Удобство использования — это основной принцип размещения оборудования в стойках и монтажных шкафах.

Масштабируемость является еще одним важным моментом, который необходимо учитывать в процессе размещения оборудования. В монтажном шкафу после размещения всех компонентов должно остаться свободное пространство, которое в перспективе может быть использовано для дополнительных коммутационных панелей. В телекоммуникационном узле или серверной комнате после установки всего оборудования должно оставаться свободное место на тот случай, если в перспективе придется поставить еще один или даже больше монтажных шкафов.

Правильное размещение оборудования, монтажных стоек и коммутационных панелей в телекоммуникационном узле позволит легко изменить, нарастить или реорганизовать структуру сети. Этот момент является самым принципиальным в проектировании физической структуры сети и рабочих областей.

Рабочие области

Зона, которая обслуживается одним телекоммуникационным узлом, называется *рабочей областью*. В большинстве случаев рабочая область занимает целый этаж здания или его часть, как показано на рис. А.6.

Максимальное расстояние от конечной точки телекоммуникационного узла до настенной розетки области не должно превышать 90 м[8]. Такой 90-метровый участок в горизонтальной кабельной системе часто называют постоянным соединением. В каждой рабочей области должно быть как минимум два сегмента кабеля: один — для передачи голоса, другой — для передачи данных. Как было сказано выше, также необходимо учитывать возможность дальнейшего расширения сети и появления дополнительных служб.

Максимальное расстояние на практике будет меньше указанного выше, потому что кабель не может быть проложен на полу или непосредственно под ним. Обычно кабель размещают в кабелепроводах, которые крепятся к стенам, или в декоративных коробах. Такие кабелепроводы формируют маршрут прокладки кабеля и медных

[6] *28,6 дюйма.*
[7] *216,5 × 5,9 ×2,4 фута.*
[8] *295 футов.*

проводников между рабочими станциями и *пленумом*[9]. Из общей протяженности кабеля в горизонтальной плоскости необходимо вычесть удвоенную длину кабеля в вертикальном направлении (поскольку два одинаковых по длине кабеля используются для того, чтобы достичь потолка).

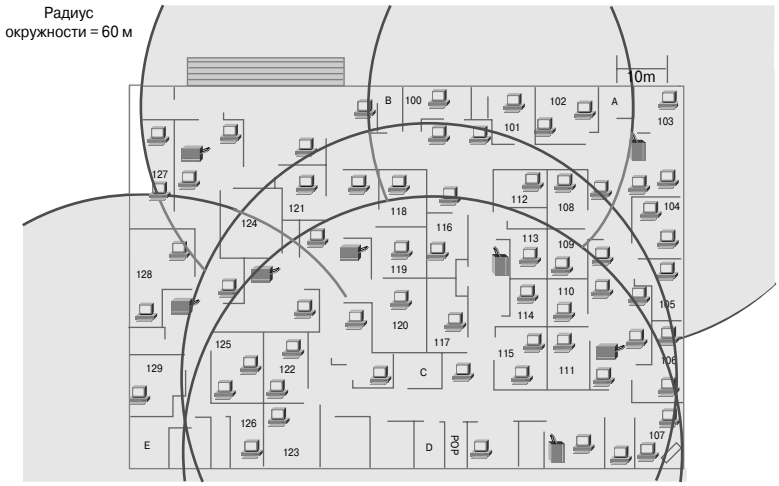


Рис. А.6. Рабочие области

Стандарт TIA/EIA-568-B определяет, что соединительный кабель длиной до 5 м[10] включительно может быть использован для подключения телекоммуникационных устройств к коммутационной панели, а кабель длиной до 5 м может быть использован для подключения компьютера или телефона к настенной розетке. Такие дополнительные 10 метров совместно с длиной постоянного соединения (permanent link) в сумме дают максимальную длину горизонтального кабеля. Согласно стандарту, максимальная длина сегмента кабеля равна ста метрам — 90 м горизонтального кабеля плюс 10 м двух сегментов соединительного кабеля (patch cord).

И, наконец, маршрут прокладки кабеля до конечной точки не может быть идеально прямым. Активное телекоммуникационное оборудование стоит достаточно дорого и требует определенных климатических условий, определенного уровня влажности, сетевых трансформаторов питания, специфического освещения. Такие требования также могут налагать серьезные ограничения на доступную длину кабельного сегмента и постоянного соединения. Все перечисленное, несомненно, значительно уменьшает длину кабельного сегмента и диаметр рабочей области. Фактически, если учесть все требования, радиус кабельного сегмента будет лежать в диапазоне от 60-ти до 70-ти метров (сравните со значением 100 м, которые указаны в

[9] Пленумом *зачастую называется небольшое пространство между фальшпотолком и собственно перекрытием, используемое во многих зданиях для вентиляции и прокладки сетевого кабеля; иногда такое название носят ниши в стенах и потолке. — Прим. ред.*

[10] *16,4 фута.*

стандарте!). На практике обычно считается, что радиус рабочей области составляет примерно 100 м.

Обслуживание рабочей области

Обслуживание кабельной системы производится в тех случаях, когда необходимо внести какие-либо изменения. Значительно проще просто перекоммутировать кабель в кабельном узле или включить другое устройство в настенную розетку, чем проложить заново участок кабеля непосредственно от аппаратного обеспечения к точке назначения и создать новую замкнутую цепь. Соединительные кабели также могут использоваться для того, чтобы подключить сетевое оборудование к коммутационной панели в кабельном узле. Максимальная длина соединительного кабеля, согласно стандарту TIA/EIA-568-B.1, составляет 5 м.

Единый план разводки кабеля должен быть использован для всех подключений к коммутационной панели (patch panel). Все гнезда такой панели и разъемы должны быть распаяны (запрессованы или, как говорят на жаргоне, "обжаты") согласно этому плану. Если для распайки розеток и разъемов используется стандарт T568A, то для портов коммутационной панели следует применить стандарт T568B. Аналогично, если для розеток используется план T568B, то для портов коммутационной панели следует применить стандарт T568A.

Коммутационные панели можно использовать для подключения посредством неэкранированной витой пары (Unshielded Twisted-Pair — UTP), экранированной витой пары (Shielded Twisted-Pair — STP) или волоконно-оптического кабеля. Наиболее часто используется кабель UTP. В таких коммутационных панелях установлены розетки стандарта RJ-45, а на конце кабеля присутствует разъем RJ-45.

На большинстве предприятий не предпринимаются никакие усилия, чтобы ограничить неавторизированный доступ к кабельной системе. Злоумышленник может подключить свое устройство соединительным кабелем или установить в сети дополнительный концентратор. Чтобы избежать такой ситуации, производители разрабатывают специализированные автоматизированные коммутационные панели, которые имеют функцию мониторинга сети и значительно облегчают инициализацию, перестройку и расширение кабельной инфраструктуры, а также позволяют отслеживать изменения в топологии. Такие коммутационные панели обычно имеют светодиодные индикаторы, которые указывают на то, что данный кабель необходимо отключить. Дополнительные индикаторы могут указывать порт, в который далее кабель необходимо включить. Эта функция будет полезна тем администраторам, опыт работы которых с кабельными системами ограничен; она облегчит им внесение изменений в кабельную структуру.

Механизм, подобный описанному выше, используется в том случае, если необходимо определить, был ли отключен какой-либо соединительный кабель, либо в том случае, если необходимо отследить подключение кабеля. Неавторизированное подключение и отключение кабеля может быть записано в журнал системных событий и при необходимости может генерировать сигнал тревоги. Например, если десяток кабелей был отключен от коммутационной панели, и произошло это в полтретьего

ночи, возможно, вашу компанию ограбили, и у многих пользователй с утра не будет персональных компьютеров!

Типы соединительных кабелей

Соединительные кабели (рис. А.7) могут быть распаяны по-разному. Чаще всего используется кабель, который называется *прямым* (straight-through), потому что распайка контактов на обоих концах одинакова. Иными словами, контакт 1 одного конца кабеля подключен к контакту 1 другого, контакт с номером 2, соответственно, подключен к контакту 2 второго конца кабеля, и т.д. Этот тип кабеля используется для подключения персонального компьютера к сетевому концентратору.

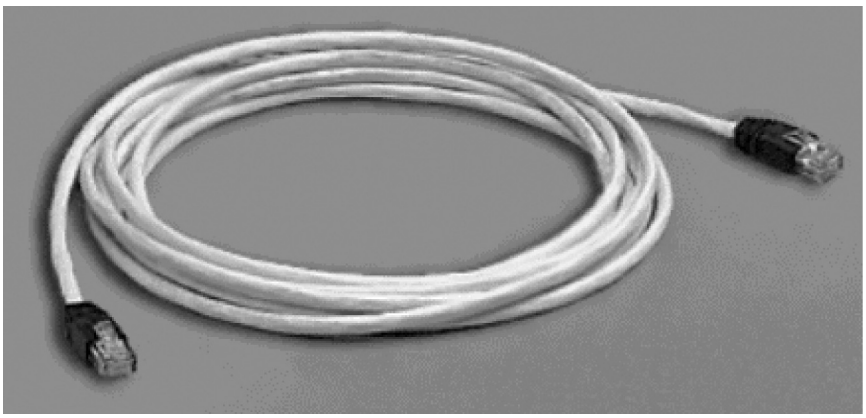


Рис. А.7. Соединительный кабель

При подключении концентратора к другому телекоммуникационному устройству зачастую используется перекрещенный кабель (crossover). В таком кабеле на одном конце используется стандарт распайки T568A, а на другом — T568B.

Практическое задание А.1. Определение типа распайки
В этой лабораторной работе описаны стандарты T568A, T568B и RJ-45 USOC, правила распайки, а также описано, как правильно запрессовать в разъем кабель категории 5e.

Приспособления для укладки кабеля

Кабельные направляющие необходимы для правильной прокладки кабеля, они обеспечивают аккуратный вид кабельной системы и позволяют поддерживать стандартный минимальный угол изгиба проводника. Кабелепроводы и направляющие облегчают добавление и удаление сегментов кабеля и любые изменения кабельной структуры. В телекоммуникационных узлах используются различные приспособления для укладки кабеля. Сетчатые кабелепроводы используются в тех местах, где необходимо развернуть облегченную структуру. Монтажные стойки используются в том случае, если конструкция узла должна быть рассчитана на значительные нагрузки.

Различные типы кабелепроводов используются для того, чтобы прокладывать кабель внутри стен, над подвесными потолками, под полом и даже в том случае, если кабель необходимо защитить от воздействия вредной внешней среды. Различные приспособления для укладки кабеля используются в монтажных шкафах для того, чтобы кабель был размещен упорядоченно и красиво (рис. А.8).

Рис. А.8. Кабельный монтажный шкаф для вертикальной и горизонтальной кабельных систем компании Panduit

Головные, промежуточные и горизонтальные кабельные узлы

В большинстве сетей используется более одного телекоммуникационного узла. Вполне очевидно, что сети крупного и среднего размера могут охватывать несколько этажей и даже несколько зданий. В таком случае на каждом этаже должен быть развернут телекоммуникационный узел, как показано на рис. А.9. Кроме того, как уже обсуждалось выше, среда передачи данных ограничена определенным предельным расстоянием из-за затухания и деградации сигнала, поэтому телекоммуникационные узлы должны быть размещены с определенным интервалом в локальной сети. Такие узлы обеспечивают подключение к концентраторам и коммутаторам локальной сети и гарантируют необходимый уровень производительности и чистоты сигнала. В телекоммуникационных узлах размещается различное оборудование, которое используется для усиления и восстановления сигнала: повторители, концентраторы, мосты и коммутаторы.

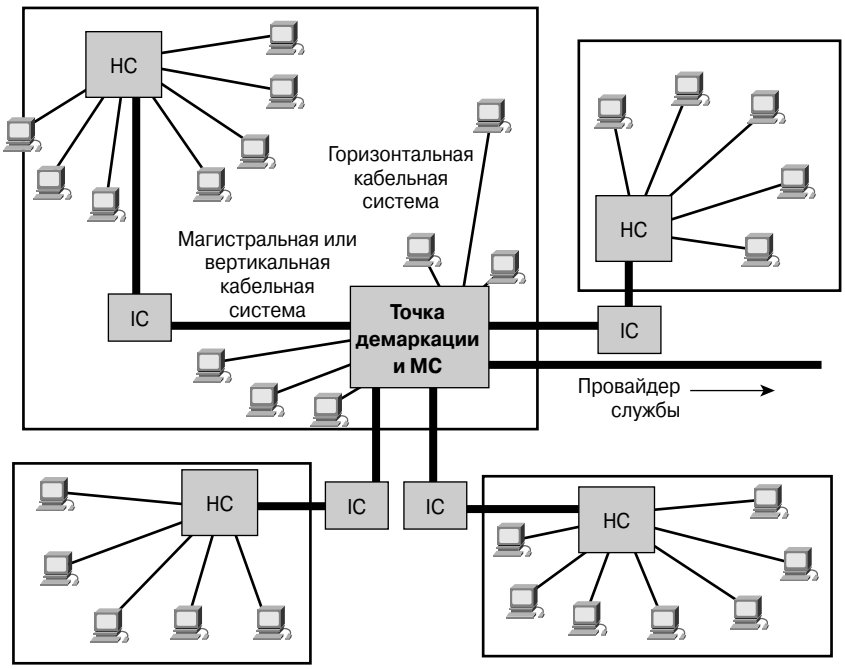


Рис. А.9. Головные, промежуточные и горизонтальные кабельные узлы

Телекоммуникационные узлы различают по выполняемым ими функциям. Первичный узел называют *главным коммутационным узлом* (Main Cross-connect — MC). Такой узел — основа сети. Главный коммутационный узел представляет собой точку кабельной структуры, откуда монтажники прокладывают магистральный кабель, и в нем обычно размещена большая часть активного оборудования сети. *Промежуточный коммутационный узел* (Intermediate Cross-connect — IC) — это узел, который подключен к главному и в котором размещено оборудование здания или территориальной сети. *Горизонтальный кабельный узел* (Horizontal Cross-connect — HC) обеспечивает соединения между горизонтальной и магистральной кабельной системами для одного этажа или небольшого здания.

Главный коммутационный узел

Главный коммутационный узел представляет собой центральную точку концентрации крупного здания или территориальной сети. Фактически такой узел является первичным. Обычно для такого узла выделяется отдельное помещение, в котором размещены средства контроля остальных телекоммуникационных узлов (промежуточных и горизонтальных). В некоторых случаях в этот узел также заводятся внешние каналы провайдеров службы, и он выполняет функцию точки демаркации.

Все промежуточные и горизонтальные кабельные узлы подключены к главному по звездообразной топологии. Магистральная кабельная система, зачастую называемая *вертикальной*, используется для подключения промежуточных и горизонтальных кабельных узлов, расположенных на других этажах здания. Согласно стандартным требованиям, главный коммутационный узел должен быть размещен на одном из промежуточных этажей многоэтажного здания; точка демаркации при этом может быть размещена на первом этаже или в подвале.

Если сеть соединяет несколько зданий, в одном из них обычно размещают главный коммутационный узел. Во всех остальных зданиях устанавливается "упрощенный" вариант главного узла, который называется *промежуточным* и объединяет все горизонтальные кабельные узлы в одном здании. Промежуточные кабельные узлы позволяют расширить магистральную кабельную систему вплоть до горизонтальных узлов за счет усиления и восстановления сигнала. В структурированной кабельной системе организации может существовать только один главный коммутационный узел. К главному узлу подключены промежуточные, к промежуточным узлам — горизонтальные кабельные узлы. Между главным коммутационным узлом и любым горизонтальным, согласно стандартам, может быть размещен только один промежуточный узел.

Магистраль (жирная линия на рис. А.9) соединяет главный и промежуточные коммутационные узлы. В территориальной сети промежуточные узлы являются узлами уровня здания, а горизонтальные узлы обслуживают рабочие области. Горизонтальная кабельная система показана на рис. А.9 тонкими линиями.

Горизонтальный коммутационный узел

Горизонтальным коммутационным узлом называют телекоммуникационный узел уровня рабочей области. Как и любой другой коммутационный узел, он обычно представляет собой монтажный шкаф, в котором установлена коммутационная панель или блок и, что необязательно, некоторые сетевые устройства: повторители, концентраторы и коммутаторы. Такой узел может быть размещен как в отдельном шкафу, так и просто занимать отдельный блок в общей монтажной стойке. Поскольку с горизонтальным узлом связаны все кабели, проложенные к рабочим станциям, он может представлять собой точку максимальной концентрации кабельного хозяйства. Например, в здании, сеть которого насчитывает 1000 рабочих станций, горизонтальная кабельная система может состоять из 2000 и даже 3000 отдельных соединительных кабелей к рабочим местам.

Горизонтальная кабельная система включает в себя медные и оптоволоконные кабели, которые используются в качестве среды передачи данных на участке между коммутационным узлом и рабочими станциями. Горизонтальная система включает в себя кабели, которые проложены (внутри горизонтальных кабелепроводов) между настенными телекоммуникационными розетками (или любыми другими разъемами, используемыми в рабочей области) и портами или перемычками коммутационной панели горизонтального коммутационного узла.

Как уже упоминалось выше, кабель, который проложен между главным коммутационным узлом и любым другим, называется магистральным. Чем отличается горизонтальная кабельная система от магистральной, четко описано в соответствующих стандартах.

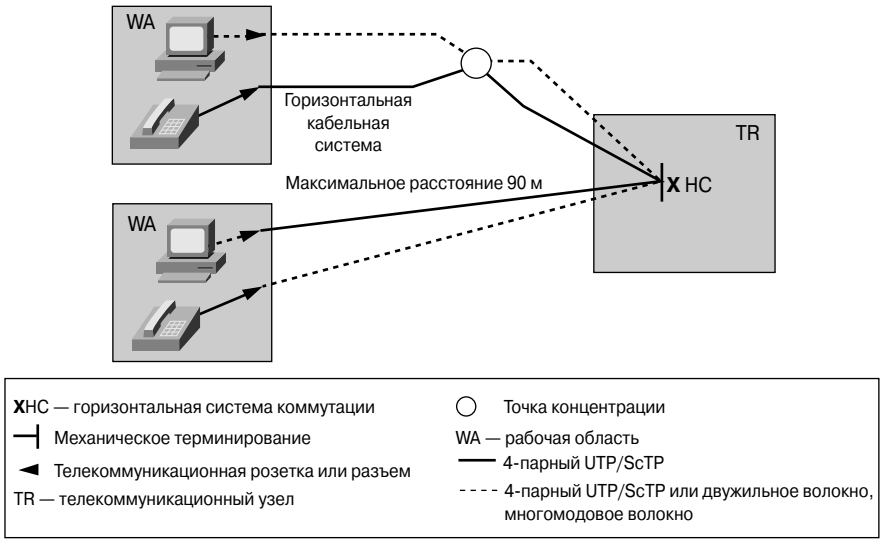


Рис. А.10. Горизонтальная кабельная система и ее условные обозначения

Практическое задание А.2. Установка кабеля категории 5e в коммутационную панель
Выполнив эту лабораторную работу, вы выучите, как устанавливать кабель категории 5e в коммутационную панель телекоммуникационного узла, а также научитесь работать с обжимным инструментом и инструментом для обрезки и очистки кабеля.

Магистральная кабельная система

Кабель, который соединяет главный коммутационный узел и любой другой, называется магистральным. Его отличия от горизонтального кабеля перечислены в стандартах, которые относятся к структурированной кабельной системе. Магистральную кабельную систему (и кабели) зачастую называют вертикальной. Магистральная кабельная система состоит из магистрального кабеля или кабелей, промежуточных и главного коммутационного узлов, механических заглушек и перемычек, которые используются для объединения разных сегментов магистрального кабеля. Кабели, которые непосредственно относятся к магистральной системе, перечислены ниже.

- Кабельные соединения между коммутационными узлами одного этажа (кабели между горизонтальным и промежуточным, между промежуточным и главным коммутационными узлами).
- Вертикальные соединения (кабельные спуски) между коммутационными узлами разных этажей (от главных узлов к промежуточным).

- Кабели между телекоммуникационными узлами и точкой демаркации.
- Кабели между зданиями в крупной территориальной сети.

Максимальная длина сегмента в данной магистральной системе зависит от типа кабеля и от того, как именно он используется. Предположим, необходимо соединить горизонтальный и главный коммутационный узлы с помощью одномодового оптоволокна; в таком случае максимальная длина магистрального сегмента будет равна 3000 м[11]. При определенных условиях сегмент нужно будет разделить на два участка, например, если необходимо соединить сначала горизонтальный коммутационный узел с промежуточным, а затем — промежуточный коммутационный узел с главным. В данном случае максимальная длина сегмента между горизонтальным и промежуточным коммутационным узлами не должна превышать 300 м[12]. Следовательно, предельная длина магистрального сегмента между промежуточным и главным коммутационным узлами не должна превышать 2700 м[13].

Магистраль на основе оптоволоконного кабеля

Оптические среды являются наиболее эффективным средством построения магистрали сети. Главное преимущество оптоволокна заключается в том, что оно не подвержено воздействию радиочастотных наводок и промышленного электромагнитного шума. Кроме того, оптический кабель производится из диэлектрических веществ, поэтому в нем не может быть паразитных токов или замыкания проводников на заземление. Оптоволоконный кабель обеспечивает большие скорости передачи данных и имеет более широкую полосу пропускания. Следует отметить, что магистральная сеть, которая основана на современном оптическом кабеле, может быть усовершенствована до более высокой производительности путем замены конечного оборудования. Эта особенность делает оптоволокно еще более привлекательным с точки зрения экономии денежных средств.

Оптическому кабелю в качестве магистральной среды присуще еще одно несомненное преимущество: максимальная длина сегмента у него значительно больше, чем у медного. Предельная длина участка многомодового оптического кабеля составляет 2000 м, одномодового — вплоть до 3000 м. В действительности, максимальное расстояние, на которое можно передать сигнал по оптоволокну, значительно больше указанного (например, максимальное расстояние для одномодового волокна превышает 100 км для определенного оборудования), но в данном разделе соответствующие вопросы будут опущены, поскольку они выходят за рамки изучения технологий локальных сетей.

[11] *9842,4 фута.*
[12] *984 фута.*
[13] *8855 футов.*

Точки концентрации и многопортовые блоки розеток

Если в здании есть фальшпол или подвесной потолок, в свободном пространстве можно разместить коммутационную панель. Такие панели называют точками концентрации, или *многопортовыми блоками розеток (Multiuser Telecommunications Outlet Assemblies — MUTOA)*.

Дополнительные спецификации горизонтальной кабельной системы в рабочих областях были включены в стандарт TIA/EIA-568-B.1, который описывает данные кабельные приспособления и дополнительные аксессуары. Горизонтальная кабельная система в структуре, в которой есть точки концентрации и многопортовые блоки розеток, описывает открытую планировку рабочих помещений, т.е. без обеспечения физической безопасности инфраструктуры (рис. A.11). Она обеспечивает высокую гибкость и экономичность установленной сети в незащищенных офисах, где часто приходится перекоммутировать и реконфигурировать сетевую структуру.

Вместо того чтобы каждый раз прокладывать новый горизонтальный сегмент кабеля, в помещениях устанавливаются точки концентрации и многопортовые блоки розеток, что позволяет при каких-либо перестановках (в том числе и мебели) и перемещении пользователей легко и быстро подключиться к ближайшему коммутационному узлу. Единственный кабель, который придется заменить, — это кабель, протянутый от розетки рабочего места пользователя к точке концентрации или многопортовому блоку в нужном помещении. Более длинный кабель от точки концентрации к коммутационному узлу при этом останется нетронутым.

Многопортовый блок розеток — это приспособление, которое за счет модульной структуры позволяет перемещать и добавлять устройства без дополнительной прокладки кабеля. *Соединительные кабели* могут быть использованы для подключения пользователей в рабочей области к такому многопортовому блоку (рис. A.12). Блок необходимо размещать в легкодоступном месте, он не может быть вмонтирован в монтажный шкаф или встроен в подвесной потолок или пол. Аналогично многопортовый блок не может быть встроен в мебель, за исключением того случая, когда мебель сама встроена в стены, пол или потолок здания.

Для многопортовых блоков стандарт TIA/EIA-568-B.1 описывает следующие параметры:

- как минимум один многопортовый блок необходимо установить для каждого набора офисной мебели;
- не более 12-ти рабочих областей могут быть подключены к одному блоку;
- соединительные кабели рабочей области должны быть промаркированы на обоих концах;
- максимальная длина соединительного кабеля составляет 22 м[14].

[14] *72,2 фута.*

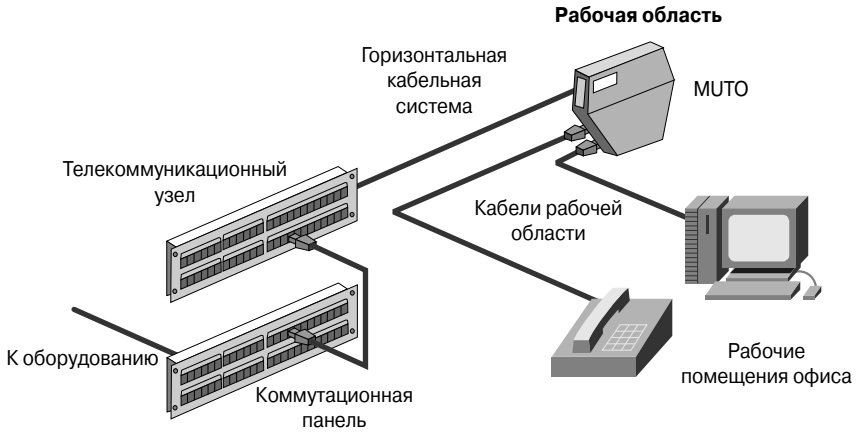


Рис. А.11. Типичный многопортовый блок

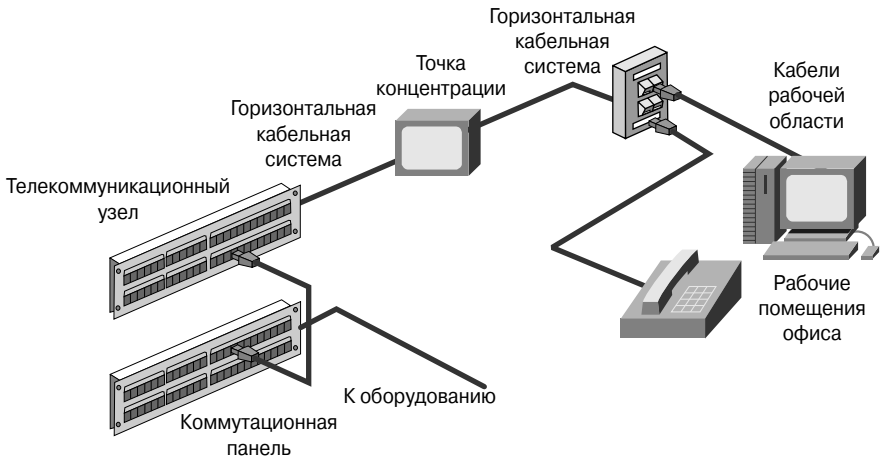


Рис. А.12. Типичная точка концентрации

Точка концентрации похожа на многопортовый блок, но содержит меньшее число разъемов. Обычно она представляет собой стационарное приспособление, установленное в стену, ниши потолка или мебель в рабочей области. Необходимо обеспечить свободный доступ к такой точке, чтобы для подключения к сети не приходилось передвигать какие-либо приспособления, оборудование или тяжелую мебель. Основное отличие точки концентрации от многопортового блока заключается в том, что рабочие станции и другое оборудование, которое находится в рабочей области, не подключается к такой точке напрямую. Оборудование подсоединяется к точке концентрации через настенную телекоммуникационную розетку.

Стандарт TIA/EIA-569 описывает следующие параметры точек концентрации:

- для каждого набора офисной мебели необходимо устанавливать как минимум две точки;
- к каждой точке концентрации можно подключить не более 12-ти рабочих областей;
- максимальная длина соединительного кабеля ограничена — он должен быть не длиннее пяти метров[15].

Как для точек концентрации, так и для многопортовых блоков в стандарте TIA/EIA-568-B.1 рекомендуется, чтобы расстояние до оборудования телекоммуникационного узла было не менее 15-ти метров. Соблюдение этого требования позволит уменьшить влияние перекрестных наводок и минимизировать искажения за счет отражения сигнала.

Стандарты и правила структурированной кабельной системы

Стандартом называется набор правил или процедур, которые либо широко используются, либо являются официально утвержденными спецификациями и служат шаблоном или эталоном. Стандарты могут принимать множество форм. Они могут быть созданы одним-единственным производителем оборудования или могут быть индустриальными стандартами, в которых определяются правила совместимости между продуктами различных компаний.

Стандарты структурированной кабельной системы можно разделить на три класса:

- стандарты, которые описывают среды передачи данных, а также принципы размещения горизонтальной и магистральной кабельных систем;
- стандарты, описывающие физические соединения между оборудованием, спецификации соединительных интерфейсов;
- базовые принципы дизайна, согласованные и универсальные правила дизайна, которые отвечают определенному плану.

Многие компании, организации и даже правительственные комитеты указывают, какие именно кабели необходимо использовать. В дополнение к таким организациям местные, окружные и государственные агентства издают спецификации, требования и правила маркировки.

Зачем нужны стандарты? Сеть, построенная согласно стандартам, будет великолепно работать и взаимодействовать со стандартными сетевыми устройствами. Долгосрочная производительность и инвестиции в сетевую инфраструктуру зачастую занижаются теми дизайнерами сетей, которые не знают основных стандартов или придерживаются необязательных или незавершенных стандартов.

[15] *16,4 фута.*

Необходимо понимать, что стандарты постоянно развиваются, и различные организации периодически пересматривают их, для того чтобы они были наиболее современными, отражали все новейшие технологии и соответствовали все более и более высоким требованиям к сетям передачи голоса и данных. По мере того, как новые технологии постепенно включаются в стандарты, устаревшие исключаются или смещаются на более низкий уровень. В большинстве случаев уже существующие сети могут включать технологии, от которых уже отказались, или стандарты, которые сегодня уже не используются. Зачастую такая ситуация не требует немедленного вмешательства, но в перспективе устаревшие участки необходимо будет заменять более новыми и быстрыми технологическими решениями.

Обычно стандарты разрабатывают или сопровождают международные организации, которые стремятся придать им наиболее универсальную форму. Такие организации, как IEEE, ISO и IEC[16], отвечают за основные стандарты. Организации по стандартизации зачастую состоят из представителей многих государств, каждый из которых отвечает за соответствие стандарта национальным требованиям.

Во многих странах внутренние национальные стандарты являются шаблоном для государственных агентств, областных, районных и муниципальных органов, которые внедряют их в свои законы и постановления. Далее они передаются определенным местным органам, поэтому всегда стоит консультироваться в муниципальных учреждениях перед тем, как приступать к развертыванию инфраструктуры сети. Во многих странах местные законы и постановления имеют бо́льший приоритет относительно общенациональных, а общенациональные являются более приоритетными, нежели международные. К стандартам применяется точно такой же подход, как к законам.

Ассоциация промышленности средств связи и Ассоциация электронной промышленности

Ассоциация промышленности средств связи (Telecommunications Industry Association — TIA) и Ассоциация электронной промышленности (Electronics Industries Association — EIA) — это коммерческие международные организации, которые совместно разрабатывают и издают стандарты, описывающие структурированные кабельные системы для передачи голоса и данных в локальных сетях (рис.А.13).

ВНИМАНИЕ!

За более подробной информацией об ассоциациях TIA и EIA обратитесь на Web-сайты `www.tiaonline.org` и `www.eia.org`.

[16] *International Electrotechnical Commission — Международная электротехническая комиссия, МЭК. — Прим. ред.*

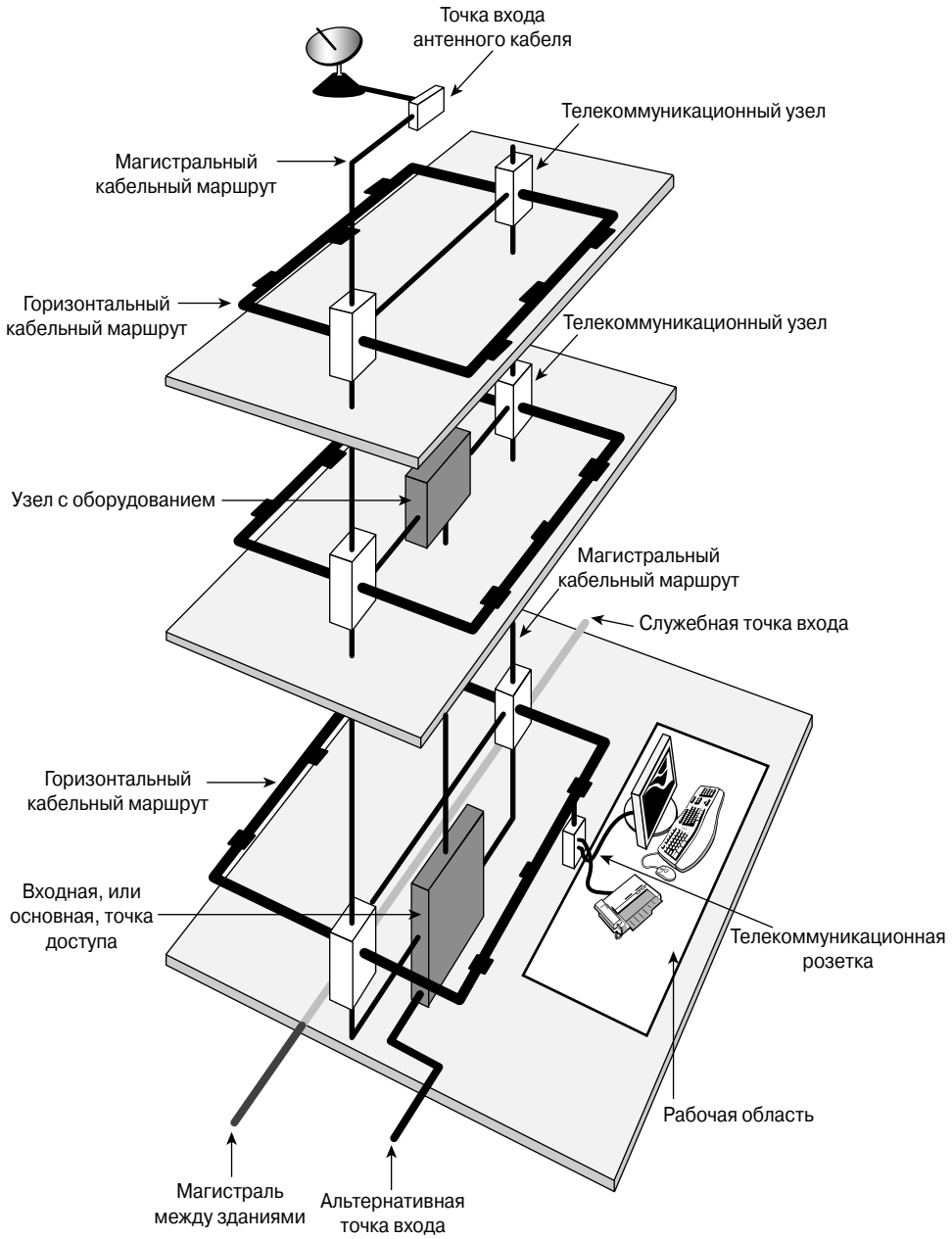


Рис. А.13. Стандарты TIA/EIA для здания

Обе ассоциации аккредитованы национальным Институтом стандартизации США (American National Standards Institute — ANSI, раздел 6.2.7) как организации, которые занимаются разработкой открытых стандартов для большого числа телекоммуникационных продуктов. Такое утверждение означает, что после окончания разработки спецификации и стандарты часто маркируются как ANSI/TIA/EIA. В состав TIA/EIA входит множество комитетов и подкомитетов, которые занимаются разработкой стандартов и правил для оптоволоконных соединений, оборудования, размещаемого в узле потребителя, для сетевого оборудования, для беспроводных и спутниковых средств связи.

Несмотря на то что стандартов существует великое множество, можно выделить наиболее часто используемые специалистами по укладке кабеля спецификации (рис. А.14).

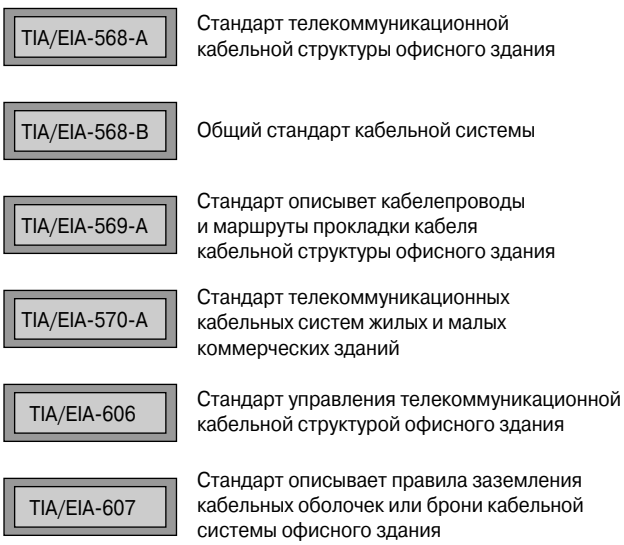


Рис. А.14. Стандарты TIA/EIA для структурированной кабельной системы

- Спецификация TIA/EIA 568-A представляет собой стандарт телекоммуникационной кабельной структуры офисного здания. Она описывает минимальные требования к кабельной системе, рекомендуемую топологию и ограничения по длине кабелей, указывает спецификации среды передачи данных и производительность каналов между сетевым аппаратным обеспечением, а также задает параметры используемых разъемов и правила их распайки.
- Спецификация TIA/EIA 568-B представляет собой общий стандарт кабельной системы. В этом стандарте указаны компоненты и передаточные характеристики сетевой среды. В стандарте TIA/EIA 568-B.1 описана “обобщенная” кабельная телекоммуникационная структура офисного здания, которая способна взаимодействовать с различным оборудованием разных производителей.

Стандарт TIA/EIA 568-B.1.1 является приложением, в котором описано применение восьмипроводной неэкранированной витой пары (Unshielded Twisted-Pair — UTP) и экранированной витой пары (Screened Twisted-Pair — ScTP), а также указаны радиусы изгиба соединительного кабеля обоих типов. В стандарте TIA/EIA 568-B.1.1 описаны компоненты кабельной системы, моделирование процессов передачи и кабельных систем, указаны измерительные процедуры, которые используются для проверки кабелей. Спецификация TIA/EIA 568-B.2.1 является приложением, в котором перечислены требования к кабельным системам на основе витой пары категории 6. В стандарте TIA/EIA 568-B.3. описаны компоненты и передаточные функции оптоволоконных кабельных систем.

- Спецификация TIA/EIA 569-A представляет собой стандарт, описывающий кабелепроводы и маршруты прокладки кабельной структуры офисного здания. Она описывает оборудование, принципы дизайна и методы построения опорных структур для прокладки кабеля как внутри, так и за пределами зданий.
- Спецификация TIA/EIA 606-A представляет собой стандарт управления телекоммуникационной кабельной структурой офисного здания и содержит правила маркировки кабелей. Именно в этом стандарте указано, что каждая конечная точка или порт оборудования должны быть промаркированы уникальным идентификатором. В этом стандарте также перечислены требования к документации по сети и описано, как поддерживать записи в административных журналах в актуальном состоянии.
- Спецификация TIA/EIA 607-A является стандартом, который описывает правила заземления кабельных оболочек или брони кабельной системы офисного здания. Она учитывает особенности различных типов оборудования многих производителей, в частности, указывает общепринятые методы безопасной установки устройств в серверной комнате потребителя. В этом стандарте четко описаны стандартные точки заземления в здании, конфигурации заземления телекоммуникационного оборудования, требования к стандартной оснастке офиса, которые позволят обеспечить стабильную и безопасную работу сетевых устройств.

Европейский Комитет по стандартизации электротехнических средств

Комитет *CENELEC (European Committee for Electrotechnical Standardization — Европейский комитет электротехнической стандартизации)* был основан в Бельгии в 1973 году как некоммерческая организация. Его основной задачей является разработка электротехнических стандартов для Европы. Комитет сотрудничает с 35000 технических экспертов из 19-ти европейских стран и издает стандарты, которые предназначены именно для европейского рынка телекоммуникаций. Он был официально зарегистрирован как Европейская организация по стандартизации указом 83/189/EEC Европейской комиссии. Многие из стандартов CENELEC соответствуют кабельным стандартам ISO с минимальными отличиями.

ВНИМАНИЕ!

За более подробной информацией о комитете CENELEC обратитесь на Web-сайт `www.cenelec.org`.

Несмотря на то что Комитет и Международная электротехническая комиссия (International Electrotechnical Commission — IEC) работают на разных уровнях процесса стандартизации, их деятельность достаточно сильно связана. Эти две организации фактически определяют то, как будут выглядеть электротехнические стандарты в Европе. Как именно взаимодействуют обе организации, было описано в так называемом Дрезденском Акте, который был подписан обеими участвующими сторонами в Дрездене в 1996 г. Предпосылкой этого соглашения было желание ускорить процесс выпуска и адаптации международных стандартов, а также необходимость в более интенсивной разработке новых спецификаций, которые будут учитывать самые последние требования активно растущего рынка телекоммуникаций. Такое объединение, несомненно, способствует более рациональному использованию ресурсов. Стоит отметить, что предпочтительнее, конечно, рассматривать все стандарты на международном уровне, независимо от того, будут ли они использоваться в Европе, США, Японии или где-либо еще.

Международная организация по стандартизации

Международная организация по стандартизации (International Organization for Standardization — ISO) является международным органом, в который входят представители более 140 стран. Так, например, Национальный Институт Стандартизации США (American National Standards Institute — ANSI) является членом этой организации. ISO является негосударственной организацией, основная задача которой состоит в разработке стандартов и всего, что связано с этим процессом. В процессе работы организации создаются международные соглашения, которые публикуются как международные стандарты.

Организация ISO выпустила множество популярных компьютерных стандартов, наиболее известным среди которых является модель взаимодействия открытых систем (Open Systems Interconnection — OSI) — стандартная структура, используемая для разработки и установки компьютерных сетей.

Стандарты и правила в США

Для внедрения некоторых сетевых проектов может потребоваться разрешение, которое будет гарантией того, что работа выполнена правильно. Чтобы узнать, какие именно документы или разрешения могут понадобиться, обратитесь в местные административные органы.

Например, для того чтобы получить копии нормативных документов, которые содержат требования к строящимся или построенным зданиям, придется обратиться в соответствующие местные государственные организации. Все нормативные акты, документы Совета строительных организаций Америки (Council of American Building

Officials — CABO), инструкции Международной конференции строительных министерств (International Conference of Building Officials — ICBO), акты Союза строительных министерств и нормативных организаций (Building Officials and Code Administrators — BOCA), Южного международного конгресса строительных нормативных организаций (Southern Building Code Congress International — SBCCI), акты международного нормативного Совета (International Code Council — ICC) и другие, имеющие юридическую силу в Соединенных Штатах Америки, могут быть куплены в представительстве Международной конференции строительных министерств (International Conference of Building Officials — ICBO) или, при отсутствии такового, заказаны непосредственно на Web-сайте этой организации.

Общепринято, что нормативные акты проверяются, утверждаются и соблюдаются местными законодательными органами. Обычно такие документы включаются в областные или окружные нормы, и контроль над их соблюдением делегируется местным или городским организациям. Стандарты и нормативные акты, в которых указаны строительные противопожарные или электротехнические нормы, являются наиболее ярким примером таких документов. Подобным образом, например, правила техники безопасности на производстве ранее были делом местных законодательных и исполнительных органов. Из-за несоответствия стандартам или недостаточного контроля со стороны вышестоящих организаций такие разрозненные требования послужили основой для национальных стандартов. Поэтому, когда такие стандарты утверждаются на уровне штата и контролируются на соответствующем уровне, нижестоящие организации вынуждены их выполнять во избежание юридических проблем[17].

Следует помнить, что несоблюдение местных норм и стандартов может привести к тому, что организации придется заплатить достаточно крупные штрафы в будущем и, следовательно, это значительно увеличит затраты на сопровождение телекоммуникационной структуры.

Некоторые нормы и правила по-разному соблюдаются городскими, окружными органами или инстанциями уровня штата. Т.е. проект сети, которая развернута в городе, попадает под юрисдикцию городских органов; проект такой же сети в пригороде должен соответствовать нормативным актам окружных инстанций, а правила у них могут отличаться. Например, нормы противопожарной безопасности могут в определенной местности быть установлены местным строительным комитетом, в другой — пожарной службой.

Несмотря на то что местные инстанции проверяют и требуют выполнения определенных норм, иногда они не издают их в печатном виде. Часто за них это делают организации по стандартизации. Например, национальный стандарт электротехнической безопасности (National Electrical Code — NEC), который издан организацией по стандартизации, написан таким образом, что звучит как постановление правительства.

[17] *В данном случае описана ситуация, характерная в США, но нехарактерная для большинства стран, в частности, Европы. Так, например, за одно и то же преступление виновный по законам одного штата может получить высшую меру наказания, по законам другого — достаточно длительный срок тюремного заключения. — Прим. ред.*

Такая форма позволяет местным административным органам принять или не принять его посредством голосования. Конечно, подобного рода события происходят достаточно редко, и государственные органы не торопятся с ратификацией новых версий. Обязательно перед тем, как разрабатывать проект сети, уточните, какая именно версия данного стандарта утверждена местными инстанциями.

ВНИМАНИЕ!

Во многих станах существуют нормы и законы, аналогичные описанным выше. Знание местных стандартов и стандартов, принятых в разных странах, понадобится также и в том случае, когда проект является международным.

Развитие стандартов

По мере того как скорость передачи в сетях возрастала от 10 Мбит/с до 1000 Мбит/с и выше, к качеству кабеля выдвигались все новые и новые требования. Старые типы кабеля зачастую не подходят для использования в более быстрых современных сетях. По этой причине с течением времени изменяются типы используемых кабелей, и стандарты отражают такие изменения. Ниже перечислены стандарты спецификации TIA/EIA 568-B.2.

- Для кабельных систем на основе витой пары на сегодняшний день разрешается использовать только кабель с сопротивлением 100 Ом категории 3, 5e и 6. Кабель категории 5 не рекомендуется использовать в новых сетях, поэтому все, что с ним связано, было перенесено из основного текста стандарта в приложение. Витая пара категории 5e и выше является рекомендованным на сегодняшний день типом кабеля.
- Стандарт кабеля категории 6 задает передаточные характеристики и параметры производительности, которые гарантируют, что продукты на его основе соответствуют другим индустриальным стандартам и стандартным компонентам, совместимы с предыдущими стандартами и не зависят от производителя.
- На концах кабеля категории 5e и выше при установке разъемов необходимо убедиться, что пары расплетены не более чем на 13 мм[18] от точки обрезки кабеля. Радиус изгиба неэкранированной витой пары (UTP) горизонтальной кабельной системы не должен быть менее четырех диаметров кабеля. Минимальный радиус изгиба соединительного кабеля на основе неэкранированной витой пары не должен быть менее диаметра кабеля, поскольку у него более гибкая внешняя оболочка, чем у кабеля горизонтальной кабельной системы.

Стандартная максимальная длина соединительного кабеля (patch cord) в телекоммуникационном узле на сегодняшний день составляет 5 м вместо использовавшихся ранее шести[19]. Стандартная максимальная длина кабельной перемычки также

[18] *0,5 дюйма.*

[19] *16,4 и 19,7 футов соответственно.*

изменилась: вместо 3-х метров стандарт предусматривает длину 5 метров. Длина горизонтального сегмента кабеля осталась неизменной — 90 м. Если используется блок MUTOA, длина кабельной перемычки может быть увеличена за счет уменьшения длины горизонтального кабеля; при этом общая длина соединения, как и раньше, не должна превышать ста метров[20] (рис. А.15).

При использовании блока MUTOA или точки концентрации требуется, чтобы между таким оборудованием и телекоммуникационным узлом был проложен отрезок кабеля длиной не менее 15-ти метров, чтобы избежать перекрестных наводок.

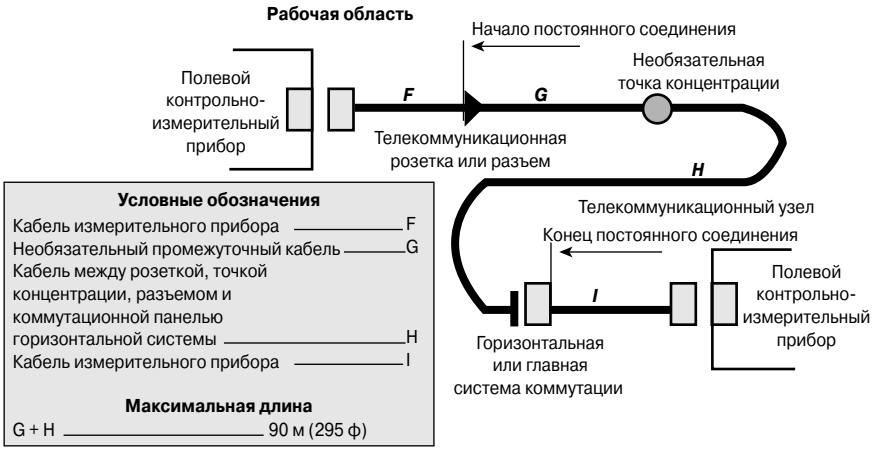


Рис. А.15. Изменения в стандартах горизонтальной кабельной системы

Для всех соединительных кабелей и кабельных перемычек ранее требовалось использовать скрученный кабель повышенной гибкости, чтобы обеспечить их "живучесть" при частых переключениях. В новом стандарте поменялась формулировка соответствующего правила: слово *должен* во фразе "кабель должен быть сделан из" было заменено на слово *может*. Теперь для обоих типов соединений можно использовать кабель в жесткой оболочке.

Соединительные кабели являются важным элементом сетевой структуры. Не возбраняется при необходимости делать такие кабели вручную, так же, как и кабельные перемычки, однако стандарт рекомендует приобретать кабели, изготовленные промышленным способом, которые выпускаются на заводах и соответствующим образом тестируются.

Витая пара категорий 6 и 7 — это новейшие кабели на основе медных проводников. Кабель категории 6 используется наиболее часто, поэтому специалист должен четко представлять себе преимущества его применения.

Существенное отличие между кабелями категории 5e и 6 состоит в том, каким именно образом используется свободное пространство между свитыми парами в кабеле. В некоторые кабелях категории 6 используется специальная вставка внутри

[20] *328,1 фута.*

кабеля, в других — специализированный наполнитель, который фиксирует положение витых пар. Кроме того, в некоторых кабелях этой категории в качестве дополнительной оболочки может использоваться фольга, в таком случае их часто называют экранированными (Screened Twisted-Pair — ScTP).

Чтобы получить еще большую производительность, в кабеле категории 7 используется более современная техника экранирования. В таком кабеле каждая пара проводов обернута экраном из фольги и все четыре пары совместно помещены в металлизированную оплетку, что позволяет практически полностью исключить паразитные перекрестные наводки. В будущем предполагается подключать оплетку к заземлению.

Стандарты структурированной кабельной системы продолжают развиваться. Основное внимание уделяется поддержке новых технологий в сетях передачи данных и ускорению и упрощению процесса слияния различных типов сетей, а именно:

- сетей IP-телефонии с использованием линейного питания IP-телефонов и точек доступа, которое подается по тем же кабелям, использующимся для передачи данных, а также определенных разновидностей беспроводной связи;
- сетей хранения данных, которые требуют Ethernet-соединений с пропускной способностью 10 Гбит/с;
- соединений Metro Ethernet, которые используются для создания абонентского канала, требуют оптимизации использования пропускной способности и имеют ограничение по длине кабеля.

Один из наиболее многообещающих стандартов — стандарт передачи питания по сети Ethernet (Power over Ethernet — PoE) — находится сейчас в стадии разработки и будет издан в ближайшем будущем. Стандарт PoE предполагает возможность подачи питания на устройства по тому же кабелю, который используется в технологии Ethernet для передачи данных. Питание, предоставляемое таким образом, значительно упростит внедрение и уменьшит себестоимость публичных IP-телефонов и беспроводных точек доступа к сети, поскольку не требует отдельного подключения к настенным розеткам или блокам питания.

Правила безопасности

Правила и требования личной безопасности содержат множество полезной информации, на которую обычно не обращают внимания при выполнении низковольтных телекоммуникационных работ. Для тех, кто не привык к физической работе и не имеет навыков установки сетей, будет полезно проделать соответствующие лабораторные работы или пройти необходимое обучение. К наиболее важным разделам личной безопасности можно отнести следующие темы:

- стандарты и правила безопасности в США;
- правила безопасности при работе с электроприборами;
- методы обеспечения безопасности на рабочем месте и в лабораториях;
- приспособления для повышения личной безопасности.

Стандарты и правила безопасности в США

В большинстве стран существуют определенные правила, соблюдение которых поможет избежать опасных для жизни ситуаций на рабочем месте. В Соединенных Штатах Америки вопросы, связанные с безопасностью работников и их здоровьем, описаны в *Законе о технике безопасности и гигиене труда (Occupational Safety and Health Administration — OSHA)*. С момента принятия этого закона в 1971 году количество несчастных случаев на производстве уменьшилось вдвое, а число производственных травм и заболеваний, связанных с определенным характером работы, снизилось на 40 процентов. Приведенные цифры особенно впечатляют, если учесть, что количество рабочих мест практически удвоилось: ранее в США насчитывалось около 65 миллионов рабочих и 3,5 миллиона рабочих мест, в настоящее время количество работников возросло до 105-ти миллионов, а количество рабочих мест составляет 6,9 миллионов.

ВНИМАНИЕ!

Закон о технике безопасности и гигиене труда (OSHA) можно прочитать на Web-сайте `www.osha.gov`.

Организация OSHA ответственна за защиту работников и соблюдение законов о труде США. Технически эта организация напрямую не отвечает за правила построения зданий или выдачу разрешений на определенные виды строительства. Инспекторы OSHA обладают достаточными полномочиями для того, чтобы наложить на фирму значительные штрафы и даже закрыть определенные рабочие места, если они не соответствуют требованиям безопасности. Каждый, кто работает над чем-либо или ответственен за рабочее место или оснащение офиса, должен быть знаком с правилами и требованиями администрации в рамках закона OSHA. Информацию по безопасности, статистику и публикации данной организации можно найти на их Web-сайте.

MSDS

Справочник по безопасности материалов (Material Safety Data Sheet — MSDS) — это набор документов, в которых содержится информация о правилах хранения, использования и перевозки опасных для здоровья материалов. В нем представлена подробная информация о том, как влияют на здоровье человека определенные вещества и материалы и как обезопасить себя при работе с ними. В этом документе указано, какие материалы являются опасными для здоровья, как безопасно их использовать, чего следует ожидать в том случае, когда рекомендации по работе с опасными материалами не выполняются, что предпринять, если произошел несчастный случай, как распознать симптомы воздействия вредных веществ и материалов, а также информация о том, что необходимо предпринимать для избежания несчастных случаев.

Лаборатория Underwriters Laboratories, Inc

Лаборатория по технике безопасности (Underwriters Laboratories — UL) — это независимая некоммерческая организация, которая занимается тестированием и сертификацией различной продукции на предмет ее вредоносности для здоровья человека. Организация существует уже более ста лет. Лаборатория UL специализируется на стандартах и нормативных документах по безопасности и защите здоровья, тем не менее, она расширила свою программу сертификации продуктов и провела тестирование кабеля витой пары согласно стандартам измерения производительности кабельных систем корпорации IBM и организаций TIA и EIA, а также на соответствие кабелей требованиям безопасности организации NEC. Лаборатория по технике безопасности также разрабатывает отдельные программы сертификации для экранированной, фольгированной и обычной витых пар для локальных компьютерных сетей, с тем чтобы производителям и потребителям было проще установить, соответствует ли кабельная продукция и материалы, из которых изготовлен кабель, самым последним спецификациям. Наличие продукта в списке лаборатории UL означает, что продукт был проверен, что он периодически перепроверяется и что он полностью соответствует стандартам безопасности и правилам охраны здоровья.

ВНИМАНИЕ!

Подробную информацию о лаборатории по технике безопасности можно найти на Web-сайте `www.ul.com`.

Лаборатория по технике безопасности тестирует и оценивает образцы кабеля один раз для выдачи начального сертификата и потом периодически перепроверяет кабельную продукцию на соответствие параметрам, которые были измерены в первый раз. Такое независимое тестирование и сопровождение продукта позволяет покупателю быть уверенным в том, что характеристики продукта или материала не изменились.

Программа сертификации локальных сетей лабораторией UL описывает не только безопасность кабельных систем, но и их производительность. Компании-производители, чьи кабели включены в список проверенных лабораторией по технике безопасности продуктов, наносят соответствующие метки на внешнюю оболочку кабеля, например, Level I, LVL I и LEV I.

Национальные электротехнические нормативы

Основной целью организации, которая поддерживает и обновляет *национальные электротехнические нормативы (National Electrical Code — NEC)*, является охрана населения и имущества от несчастных случаев, связанных с пользованием электричеством. Эта организация финансируется национальной Ассоциацией по пожарной безопасности (National Fire Protection Association — NFPA) и находится под протекцией национального Института по стандартизации США (American National Standards Institute — ANSI). Правила безопасности пересматриваются каждые три года.

ВНИМАНИЕ!

За более подробной информацией о национальной Ассоциации по пожарной безопасности (NFPA) обратитесь на Web-страницу `www.nfpa.org/Home/index.asp`.

Многие организации, в том числе и лаборатория UL, издают стандарты, которые регулируют требования к пожарной безопасности кабельной системы здания. Правила NEC являются прежде всего стандартами, которые поддерживают местные лицензионные и контрольные инстанции.

Группы нормативов NEC

Группы нормативов NEC перечислены в специализированных каталогах кабелей и сопутствующих материалов. Они используются для классификации по специфическим категориям продуктов и по методам их использования (табл. А.1).

Таблица А.1. Группы нормативов NEC

Тип кабеля	Описание
OFC (оптоволоконный кабель)	Кабель этого типа содержит металлическое армирование для повышения жесткости
OFN (оптоволоконный кабель)	Кабель не содержит металла
CMP (телекоммуникационный пленум)	Кабель прошел тестирование на огнеупорность, при пожаре не воспламеняется и дает мало дыма. Кабель, который размещается в пленуме, обычно покрыт специализированной оболочкой, например, из тефлона (Teflon). Буква *P* в коде означает, что кабель предназначен именно для размещения в пленуме или в вентиляционных шахтах и трубах
CMR (телекоммуникационный стояк)	Буква *R* в коде свидетельствует о том, что кабель прошел тестирование, подобное используемому для кабеля CMP, но к нему выдвигаются другие требования относительно воспламеняемости. Согласно своему назначению, такой кабель проверяется на воспламеняемость в вертикальном положении. Его необходимо использовать в вертикальной кабельной системе (в стояке) в том случае, если сеть охватывает несколько этажей. Кабели CMR обычно покрыты поливинилхлоридной оболочкой (PVC)

В наиболее распространенных телекоммуникационных структурах развертываются кабели категорий CM (communications — коммуникационный) и MP (multipurpose — многоцелевой). Многие компании с целью повышения уровня безопасности передаваемой информации тестируют используемые кабели на уровень излучения электромагнитной энергии. Таким тестам соответствуют категории CL2 и CL3 (power-limited circuit cable), часто их маркируют как Class 2 и Class 3 (кабель 2-го и 3-го классов защиты соответственно). Несмотря на то что тесты CM и MP, на первый

взгляд, для таких кабелей не используются, следует отметить, что критерии оценки воспламеняемости для кабелей разных категорий одинаковы. Принципиальное отличие между указанными категориями состоит в уровне излучаемой наружу (из кабеля) энергии, поэтому для разных кабелей используется разная маркировка. Предполагается, что кабель MP имеет самый высокий уровень излучаемого сигнала, кабели CM, CL2 и CL3 излучают меньше энергии.

Техника безопасности при работе с электроприборами

При монтаже кабельной системы не достаточно просто знать список организаций, которые регулируют правила техники безопасности. Монтажник обязательно должен знать основные методы и принципы техники безопасности, которые, несомненно, понадобятся ему в повседневной работе. Правила техники безопасности также необходимо соблюдать при выполнении лабораторных работ, которые описаны в книге и приведены на прилагаемом компакт-диске. В процессе установки кабеля может возникнуть множество опасных для жизни ситуаций, квалифицированный монтажник должен быть готов к ним, чтобы уменьшить вероятность несчастного случая.

Высокое напряжение

Специалисты по монтажу кабеля работают с проводами, которые рассчитаны на низковольтные системы. Ток, который передается по таким кабелям, для большинства людей едва заметен. Тем не менее, напряжение, которое подается на сетевые устройства, значительно больше: от 100 до 240 В. Если обрыв в электрической цепи приводит к утечкам, работник, который монтирует кабель, может получить электрический удар и шок — такое поражение может быть смертельным. Кроме того, монтажник, который работает с цепями низкого напряжения, может непреднамеренно коснуться оголенного высоковольтного провода, и результат тоже будет плачевным.

Не стоит быть слишком самоуверенным и игнорировать правила работы с высоковольтными системами просто потому, что приходится работать с низковольтными сетями. Если случайно коснуться высоковольтного провода, мускулы сведет судорога, и отбросить провод с высоким напряжением будет очень сложно.

Освещение и высокое напряжение

Высокое напряжение присутствует не только в линиях питания: освещение тоже относится к высоковольтным системам. Осветительные устройства могут повредить сетевое оборудование при неосторожном обращении, поэтому следует аккуратно обращаться с ними во избежание поломок.

Ниже перечислены меры предосторожности, которые следует соблюдать, чтобы избежать поражения электрическим током и не вывести сетевое оборудование из строя при работе с осветительным оборудованием или случайно не закоротить высоковольтные линии.

- Все наружные провода должны быть соответствующим образом заземлены или снабжены сертифицированными защитными приспособлениями в точке их входа в здание (entrance point). Защитные приспособления должны быть установлены в соответствии с правилами местной телефонной компании и общепринятыми правилами. Телефонные пары нельзя использовать самовольно (т.е. без соответствующего разрешения). Если разрешение получено, то все равно нельзя убирать защитные приспособления, подавители или провода заземления.
- Нельзя прокладывать провода между разными структурами без соответствующей защиты. Так, например, отсутствие необходимости установки громоотводов — это одно из самых существенных преимуществ использования оптического кабеля в качестве наружных коммуникаций.
- Нельзя прокладывать провода в сырых помещениях.
- Нельзя проводить или подключать медные провода в грозу. Неправильно заземленный или защищенный кабель может передать бросок напряжения, например, от молнии, на много километров.

Безопасность при работе с высоким напряжением

Напряжение невидимо. Его можно обнаружить косвенно: по отказам механизмов, сбоям включенного оборудования или истошным крикам сотрудника, который получил электрический разряд.

Если специалисту приходится работать с чем-либо, что включено в настенную розетку питания, лучше всего предварительно проверить, находятся ли под напряжением корпуса приборов, прежде чем касаться их. Такую проверку можно выполнить *мультиметром* (универсальный измерительный прибор) или измерить напряжение с помощью вольтметра. Повторные замеры следует проводить после перерыва в работе или на следующий день, поскольку кто-то другой мог что-либо изменить в оборудовании. После окончания работ также необходимо провести измерения.

Некоторые электрические явления невозможно предсказать, например, электрические молнии и статическое электричество. Запрещено устанавливать или соединять медные кабели в грозу, поскольку они прекрасно проводят ток на большие расстояния. Это требование очень существенно при прокладке наружной проводки между зданиями или в подземных кабельных колодцах. Вся наружная проводка должна быть качественно заземлена в соответствии со стандартами и оборудована специальными сертифицированными защитными устройствами. Защитные устройства должны быть установлены в соответствии с местными нормативными документами и стандартами, которые в большинстве случаев просто повторяют общепринятые в данной стране стандарты.

Заземление

Заземление обеспечивает прямой контакт с землей. Разработчики аппаратуры специально изолируют электрические цепи в оборудовании от *шасси*: фактически от корпуса, в котором смонтированы электрические и электронные платы. Любой заряд, который перетекает из плат оборудования в шасси, не должен в нем оставаться. Заземление позволяет убрать паразитное напряжение, чтобы оно не нанесло вреда оборудованию. Если отсутствует уверенный контакт с заземлением, паразитное напряжение может перетечь в землю по любому другому пути, например, через тело работающего с оборудованием человека.

Электрод заземления представляет собой стержень, вкопанный глубоко в землю рядом с точкой входа проводки в здание, т.е. в том месте, где в здание поступает электричество. Как именно система заземления подведена к земле — это уже совсем другой вопрос. Многие годы трубы системы водоснабжения (а именно — трубы с холодной водой) считались достаточно хорошим средством заземления, поскольку они проложены под землей и обеспечивают контакт с грунтом на достаточной глубине. Крупные компоненты структуры здания, перекладины и двутавровые балки также считаются приемлемым контактом заземления. Несмотря на то что перечисленные архитектурные компоненты обеспечивают неплохое заземление, новые правила требуют наличия отдельной системы заземления, например, специальных медных линий для соединения оборудования с электродами заземления.

Специалисту необходимо точно знать, как именно подключено заземление к лабораторным и рабочим местам. Обязательно проверьте, действительно ли заземление присутствует. Вполне вероятно, что оно сделано неправильно или вообще не работает. Не менее часто встречается ситуация, когда специалисты, которые занимаются монтажом сети, делают специальные перемычки, которые обеспечивают технически приемлемое заземление, но не являются стандартным методом решения проблемы. Изменения в сети или в структуре здания могут разрушить такую нестандартную систему заземления и создать как опасность поражения током людей, так и возможность выхода из строя оборудования.

Зажимы

Зажимы представляют собой специализированные приспособления для соединения оборудования и сетевых устройств с системой заземления здания (рис. А.16). Корпус сетевого устройства, такого, как коммутатор или маршрутизатор, должен быть подключен посредством специализированного контакта-зажима к общей системе заземления.

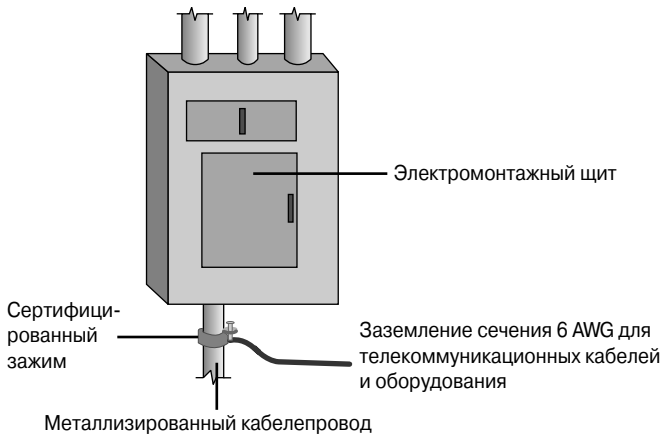


Рис. А.16. Закрепление с помощью зажима

Заземление и соединительные перемычки, которые установлены должным образом, позволяют достичь следующих результатов:

- свести к минимуму влияние скачков напряжения;
- поддерживать целостность системы заземления;
- обеспечить безопасный и эффективный маршрут для электрического тока к заземлению.

В телекоммуникациях зажимы и перемычки обычно используются в следующих точках:

- распределительном щите электропроводки здания;
- серверных комнатах;
- телекоммуникационных узлах.

Стандарты заземления

Документы NEC (National Electrical Code — Национальные электротехнические нормативы) содержат обширную информацию о правилах установки и подключения заземления. Стандарт ассоциаций TIA и EIA, TIA/EIA-607-A (телекоммуникационные требования к заземлению и перемычкам в офисных зданиях), связывает систему заземления и контактные перемычки со структурированной кабельной системой. В нем четко описаны точки и правила взаимодействия системы заземления здания и заземления телекоммуникационного оборудования. Стандарт не зависит от производителя, типа оборудования и описывает правила установки заземления для различных систем, которые могут быть установлены в точках размещения устройств пользователя. В нем также описаны требования к системе заземления здания, выполнение которых позволить обеспечить адекватное подключение любых приборов и устройств.

Правила безопасности на рабочих местах и в лабораториях

Несмотря на то что профессия монтажника кабеля достаточно безопасна, несчастные случаи не исключены. Основной риск связан с возможностью контакта с так называемыми сторонними источниками опасного напряжения, к которым относятся осветительные приборы, источники статического электричества или любые другие объекты, которые за счет пробоев в изоляции проводки или индуцированных токов являются опасными и по какой-либо причине могут быть связаны с кабельной инфраструктурой.

В процессе прокладки кабеля по стенам или внутри декоративного покрытия, над навесным потолком и на чердаках первое, что необходимо предпринять, — это обесточить всевозможные электрические цепи, которые могут присутствовать в рабочей области. Если сложно определить, какие именно провода используются в рабочем помещении, следует обесточить абсолютно все. Никогда не прикасайтесь к проводам питания! Даже если выключено абсолютно все, никогда нельзя быть уверенным в том, что какой-либо кабель не находится под напряжением.

В большинстве стран существуют официальные организации, которые разрабатывают и сопровождают стандарты по безопасности. Часть стандартов обычно относится к общим принципам общественной безопасности, часть описывает правила охраны труда и безопасность работников. Последние включают в себя требования к безопасности лабораторных, рабочих мест, к параметрам окружающей среды и правила уничтожения опасных для здоровья и окружающей среды отходов.

Требования к безопасности рабочего места

Перечисленные ниже правила помогут обеспечить безопасность на рабочем месте.

- Перед началом работы необходимо определить, где размещены ближайшие огнетушители. Небольшое возгорание может привести к большому пожару, если сотрудники не смогут быстро найти огнетушитель.
- Необходимо ознакомиться с местными нормами и правилами заранее. Согласно требованиям к определенным типам зданий, нельзя сверлить или рубить отверстия в противопожарных перегородках и даже в подвесном потолке.
- При монтаже кабеля между этажами необходимо использовать соответствующий сертифицированный тип кабеля. Кабель для укладки в стояки покрыт слабовозгорающейся фторированной этиленпропиленовой оболочкой, и пламя не сможет по нему достичь следующего этажа.
- Наружные кабели обычно покрыты поливинилхлоридной (polyvinyl chlorid — PVC) или полиэтиленовой оболочкой. Такая оболочка хорошо горит, выделяя при этом ядовитый газ. Правила NEC требуют, чтобы наружная проводка в поливинилхлоридной оболочке проникала в здание не более чем на 15 метров. Если необходимо проложить такой кабель на бо́льшее расстояние, стандарт предписывает, что кабель должен быть уложен в металлический короб.

- Необходимо заранее выяснить у главного инженера или коменданта корпуса, есть ли в помещениях свинцовые или асбестовые структуры. Если такие структуры есть, следует строго следовать официальным документам по работе с этими материалами, поскольку они являются вредными. Работать без соответствующей защиты в помещениях, где есть перечисленные материалы, нельзя, по крайней мере, легально.
- И, наконец, если кабель необходимо проложить в вентиляционных шахтах или других местах с активной циркуляцией воздуха, необходимо использовать огнеупорный кабель. К огнеупорным кабелям относятся те, которые покрыты тефлоновой или халаровой оболочкой (Teflon, Halar). Кабели данного типа не выделяют ядовитых газов в процессе горения, в отличие от обычных, которые покрыты поливинилхлоридной оболочкой.

Правила безопасности при работе со стремянкой

Существует много разновидностей стремянок различных форм и размеров, которые используются для разных специфических задач. Стремянка (или приставная лестница, ladder) может быть изготовлена из дерева, алюминия, пластика и оргстекла и предназначена как для домашнего, так и для промышленного использования. Чаще всего встречаются два типа стремянок: раздвижная и приставная лестницы. Вне зависимости от конструкции, типа и производителя лестницы, следует убедиться в том, что на ней есть пометки, свидетельствующие о том, что стремянка сертифицирована и соответствует спецификациям института ANSI, лаборатории UL или нормативным документам местных органов и, следовательно, соответствует стандартам безопасности труда.

- Стремянка должна быть предназначена именно для той работы, которую вы выполняете. Необходимо удостовериться, что она имеет достаточную высоту и настолько прочна, чтобы выдерживать нужные нагрузки. Для монтажа кабельной системы зачастую используют либо пластиковые, либо покрытые пластиком специальные стремянки. Несмотря на то что алюминиевые лестницы значительно легче, они менее устойчивы и с ними опасно выполнять электротехнические или любые другие работы, которые связаны каким-либо образом с электричеством, поэтому, согласно правилам техники безопасности, использовать можно только лестницы из диэлектрических материалов.
- Перед началом работы следует проверить стремянку. Любая мелочь может привести к неприятным последствиям. Следует проверить лестницу на наличие незакрепленных или сломанных ступеней, перекладин, поручней и скоб. У раздвижной стремянки обязательно должен быть фиксатор и упоры безопасности, которые обеспечат дополнительную устойчивость и уменьшат скольжение лестницы, а также обезопасят вас от ситуации, когда половинки стремянки могут “разъехаться” в процессе работы. Никогда не используйте сломанную лестницу!

- Когда раздвижная лестница полностью раздвинута, ее шарниры в рабочем положении обязательно должны быть зафиксированы. Приставная лестница должна быть установлена согласно так называемому правилу “4:1”, т.е. основание (нижний конец лестницы) должно быть отодвинуто от стены или любой другой вертикальной поверхности из расчета 0,25 м на каждый метр высоты лестницы. Стремянку необходимо поставить как можно ближе к точке опоры, чтобы предотвратить скольжение, на твердую горизонтальную поверхность.
- Не следует подниматься выше второй от верха лестницы ступени, для того чтобы сохранять устойчивость в процессе работы.
- Следует пометить рабочую область, например, специальной лентой, флагами, дорожными конусами и т.п. Можно также установить специальные знаки или расклеить объявления. Если в непосредственной близости от места выполнения работ находится дверь, ее следует закрыть на ключ или заблокировать, чтобы она не могла задеть лестницу, если кто-то ее откроет.

Правила безопасности при работе с оптоволокном

Оптоволоконный кабель содержит стекло, поэтому работать с ним нужно с особой осторожностью. Обрезки кабеля могут иметь острые концы, поэтому выбрасывать их нужно также осторожно. От любого изделия из стекла, когда оно разбивается, могут отколоться тонкие и очень маленькие осколки, которые могут застрять в коже.

Ниже перечислены основные требования, которые следует выполнять в процессе работы с оптическими волоконными кабелями; это поможет избежать несчастных случаев.

- Работать разрешено только в специальных очках, у которых есть боковые защитные накладки.
- На рабочий стол необходимо положить специальный коврик или кусок клейкого материала, к которому будут прилипать осколки стекла, чтобы после завершения работы их легко можно было убрать.
- Нельзя касаться глаз в процессе работы с волоконно-оптическими кабелями; после окончания работ следует тщательно вымыть руки. Аналогично нельзя производить какие-либо действия с контактными линзами, поскольку осколки стекла легко могут попасть в глаза.
- Все обрезки кабеля, остатки оболочки и другой мусор необходимо сложить в специализированную упаковку и только потом выбросить.
- Если какие-либо материалы попали на одежду, используйте специальную липкую ленту или щетку для чистки одежды. Осколки стекла с пальцев рук нужно удалять с помощью специальной липкой ленты.
- В рабочей области запрещено принимать пищу или какие-либо напитки.
- Строго воспрещается смотреть в просвет кабеля или световодов, поскольку некоторые лазерные устройства могут повредить глаза.

Правила пользования огнетушителями

Любому работнику необходимо уметь пользоваться огнетушителями разных типов на случай возникновения пожара. Перед началом работы изучите инструкции и проверьте пожарные краны. В Соединенных Штатах Америки правила пожарной безопасности требуют, чтобы огнетушители, которые используются в офисных зданиях, периодически проверяли и заменяли в том случае, если они не работают или не соответствуют противопожарным требованиям.

ВНИМАНИЕ!

Следует запомнить простое правило на случай пожара: “Останови, повали, покатай по полу” (“Stop, Drop and Roll”).

- Остановитесь! Бежать нельзя! Огонь разгорается значительно быстрее, если горящий человек бежит. Если человек начинает паниковать и бежит, следует остановить его: подставить подножку (только так, чтобы он не разбил нос, падая), сбить с ног и т.п.
- В любом случае горящего человека (даже если он не бежит) следует повалить на пол (но не придавливать к полу, удерживая его в таком положении).
- Третье правило: горящего человека следует покатать по полу, чтобы сбить с него пламя.

На огнетушителях должны присутствовать наклейки, на которых указано, для каких целей они предназначены; такие наклейки содержат “паспортные данные” огнетушителя. В США огнетушители делят на четыре типа; они перечислены ниже.

- Огнетушители класса A используются для тушения обычных (и, стоит заметить, великолепно горящих) материалов, таких, как древесина, бумага, картон, пластмассы и другие.
- Огнетушители класса B применяются для тушения легко воспламеняющихся, огнеопасных и горючих жидкостей, таких, как бензин, керосин, и распространенных органических соединений и растворителей, которые используются в лабораториях.
- Огнетушители класса C применяются для тушения электрооборудования, различных приборов, коммутаторов, активных панелей, механизированных инструментов и устройств, нагревательных плит и многих других электромеханических и электронных устройств. Следует помнить, что тушить объекты, для которых предназначен данный тип огнетушителей, исключительно опасно водой, поскольку при этом очень велик риск получить электрический шок.
- Огнетушители класса D используются для тушения так называемых “легко воспламеняющихся металлов”, а именно: магния, титана, калия и натрия. Эти металлы при горении дают высокую температуру, очень легко взаимодействуют с водой, воздухом и другими веществами (т.е. они химически активны).

Приспособления для личной безопасности

Перед тем как приступить к работе, нужно убедиться, что все правила безопасности и охраны труда соблюдены. Наиболее существенным моментом личной безопасности работника является профессиональная экипировка. Правила охраны труда описывают требования к одежде, в которую должен быть облачен сотрудник при выполнении разного рода работ. Так, например, специальный комбинезон, рабочий халат или другая спецодежда (gear) могут свести к минимуму или вообще исключить возможность телесных повреждений.

При работе с разными строительными инструментами и другим механическим оборудованием необходимо надевать специальные очки, которые защитят глаза от летящих осколков, стружек и т.п.; кроме того, необходимо надевать специальные звукоизолирующие наушники или противошумовые вкладыши (беруши), которые уменьшат интенсивность шума. Отсутствие защитных очков либо берушей может привести к частичной или полной потере зрения или слуха на длительный период или даже на всю жизнь.

Рабочая одежда

Брюки с длинными штанинами и куртка с длинными рукавами помогут защитить руки и ноги работающего человека от царапин, порезов и других повреждений (шорты и футболку при выполнении работ надевать запрещено!). Запрещено также надевать просторную одежду при выполнении многих видов работ, поскольку такая одежда может зацепиться за выступы или застрять в высоковольтном оборудовании.

Обувь должна соответствовать выполняемой работе: быть прочной и закрытой. Рабочая обувь должна защищать ступни от возможных повреждений, острых краев и обломков на полу. Обувь на толстой подошве — это наилучший выбор для того, кому может случиться наступить на гвоздь, обрезки металла и других материалов, которые легко проколют подошвы обычных кроссовок или другой повседневной обуви. Армированная обувь защитит пальцы ног даже в том случае, если монтажник уронит себе на ноги что-то тяжелое. Подошвы должны быть рельефными, не скользить.

Защита глаз

Глаза проще защитить, чем вылечить и восстановить зрение после несчастного случая, поэтому защитные очки следует надевать практически во всех случаях, тем более, когда приходится что-либо сверлить, резать, выдалбливать, пилить или когда приходится работать в подвале, на чердаке и т.п. (рис. А.17). В процессе прокладки кабеля, особенно когда кабель приходится обрезать, подготавливать или удалять, могут откалываться и разлетаться мелкие куски и стружки. При работе с оптоволоконным кабелем осколки стекловолокна, клейкие материалы и растворители могут попасть в глаза. Кроме того, мелкие осколки, стружки и химические вещества могут попасть на руки и потом быть случайно занесены в глаза. Следовательно, очки защитят как от прямого взаимодействия с веществом, так и от грязных рук. Рекомендуется носить защитные очки всегда, когда приходится выполнять работы в подвальных

помещениях, под полом или над подвесными потолками. При выполнении многих видов работ и на многих рабочих местах требуется, чтобы защитные очки были надеты всегда.

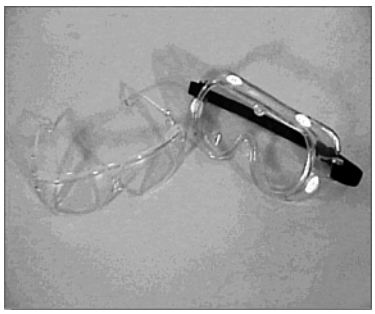


Рис. А.17. Защитные очки

Защитные очки должны использоваться при выполнении всех лабораторных работ. Перед тем как начать выполнять какие-либо задания, ознакомьтесь с инструкциями по технике безопасности и определите, какие приспособления для безопасности необходимы.

Использование касок

Как и любые другие приспособления, которые обеспечивают безопасность, каска защищает человека от несчастных случаев. Каски требуется носить постоянно на определенных рабочих местах, например, на стройке или при выполнении монтажных работ. Многие работодатели выдают своим работникам каски, другие же требуют, чтобы работники покупали их сами. Каска, которая является частью экипировки, может быть окрашена в фирменные цвета компании или на ней может быть нарисован логотип компании, чтобы с первого взгляда можно было определить принадлежность работника к определенной фирме или компании. Даже если вы покупаете каску для личного использования, не украшайте ее какой-либо символикой без разрешения работодателя. Правила организации OSHA (и многих других) запрещают приклеивать наклейки на каски, поскольку под ними можно не заметить трещин в материале.

Следует периодически проверять каску на наличие трещин. Треснувшая каска вряд ли защитит голову. Чтобы обеспечить адекватную и эффективную защиту, следует правильно надевать каску. Лучше потратить некоторое время на подгонку внутренних и внешних ремешков и убедиться, что каска сидит правильно и удобно, чем затем лежать прикованным к постели. Каску следует надевать при работе на стремянке или приставной лестнице, а также тогда, когда приходится работать в недавно построенном здании.

Профессиональные инструменты

Как и в любом ремесле, профессиональное оборудование — это то, что отличает тяжелый труд и посредственные результаты от легкой работы и выдающихся достижений. Специалист по прокладке кабеля обязательно должен иметь практический опыт работы с базовым инструментарием монтажника низковольтных кабельных систем, чтобы достичь высоких профессиональных показателей.

Следует уметь работать со следующими типами инструментов:

- инструментом для обрезки и зачистки;
- инструментом для запрессовывания (обжимки или распайки[21]) кабеля;
- диагностическими приборами;
- вспомогательными инструментами.

Инструмент для обрезки и зачистки

Для зачистки проводов и удаления изолирующего материала используется специализированный инструмент. Чтобы удалить внешнюю изолирующую оболочку с четырехпарного кабеля, аккуратно и ровно обрезать концы пар, можно использовать специализированное устройство для кабеля UTP компании Panduit[22] (рис. А.18). Этот инструмент также может быть использован при монтаже практически всех разновидностей коаксиального кабеля. Основная особенность инструмента заключается в том, что у него регулируется величина выступа обрезочного лезвия, поэтому он подходит для многих типов кабеля с разной толщиной оболочки. Кабель необходимо вставить в отверстие инструмента, затем инструмент необходимо обернуть несколько раз вокруг кабеля. Правильно отрегулированное лезвие позволяет перерезать только внешнюю оболочку кабеля, которую потом можно без лишних усилий снять и получить доступ непосредственно к проводам витой пары.

Для зачистки кабеля и удаления внешней оболочки могут быть также использованы электротехнические ножницы и кабельный нож (рис.А.19). Кабельные ножи применяются преимущественно тогда, когда требуется снять внешнюю оболочку с крупногабаритных кабелей, в частности, с магистрального кабеля телекоммуникационной компании, оператора связи или провайдера, который проложен от их точек доступа в точку присутствия в конкретном здании. Такой нож обычно очень хорошо заточен, поэтому при работе с ним нужно соблюдать максимальные меры предосторожности. При работе с кабельным ножом рекомендуется надевать специальные жесткие защитные перчатки, которые защитят руки, если нож вдруг выскользнет.

---

[21] *В настоящее время кабель очень редко паяют, подавляющее большинство кабелей рассчитано на специальные разъемы, которые просто надеваются на концы кабеля. и кабель запрессовывается в них — такой процесс зачастую называют* обжимкой. *— Прим. ред.*

[22] *Компания Panduit является бизнес-партнером корпорации Cisco и выступила спонсором совместного специализированного курса по прокладке кабельных сетей для передачи голоса и данных (*Voice and Data Cabling*), поэтому на иллюстрациях показано кабельное оборудование именно этой компании. — Прим. ред.*

Рис. А.18. Инструмент для зачистки и обрезки кабеля UTP компании Panduit

Ножницы обычно используются чтобы ветх случаях, когда требуется перекусить отдельные проводники, удалить внешнюю оболочку с тонких кабелей или снять изоляцию с отдельных проводов. На противоположной лезвию стороне электротехнических ножниц есть два выреза стандартного размера, предназначенные для удаления изоляции с проводников сечением 22 и 26 (к сожалению, на рисунке эта особенность не видна).

Рис. А.19. Электротехнические ножницы и кабельный нож

Обжимной инструмент

Обжимной инструмент (termination tools), зачастую называемый запрессовочным, предназначен для обрезки и запрессовки определенных типов кабелей. Многопарный инструмент предназначен для обрезки и подготовки кабеля UTP, а также для запрессовки кабеля в контактные разъемы (рис. А.20). За счет своего эргономичного дизайна такой инструмент значительно облегчает процесс подготовки кабеля и упрощает процедуру терминирования соединений. Вот некоторые его особенности:

- инструмент позволяет обработать несколько пар одновременно;
- он позволяет одновременно обрабатывать контакты как самого кабеля, так и коммутационного блока или контактного разъема;
- в инструменте используются сменные режущие лезвия;
- инструмент может быть использован как в режиме обрезки, так и в обычном;
- он позволяет рассмотреть проверяемую схему (CUT — Circuit Under Test) в процессе работы с кабелем и убедиться в том, что контакты и проводники размещены согласно цветовой схеме разводки кабеля;
- инструмент имеет встроенный ударный механизм для запрессовки;
- ручка инструмента имеет эргономичный дизайн и покрыта прорезиненным ребристым материалом, благодаря чему при работе рука не скользит по рукоятке.

Запрессовочный инструмент, называемый иногда однопарным (рис. А.21), комплектуется сменными лезвиями и, следовательно, может использоваться совместно с пассивным оборудованием разных типов, например, с оборудованием типов 66 и 110. В отличие от многопарного инструмента, он позволяет работать только с одной парой проводов. Двустороннее лезвие такого инструмента в одном положении позволяет одновременно и запрессовывать, и обрезать проводники, в другом положении — только обрезать провод.

Практическое задание А.3. Работа с кабельными инструментами и правила личной безопасности

Выполнив эту практическую работу, вы научитесь идентифицировать, проверять и использовать инструменты, которые применяются при прокладке кабеля.

Диагностические средства

Зачастую монтажнику необходимо получить доступ к отдельному проводу или кабелю в телекоммуникационной панели или блоке розеток. Для этой цели используется специализированный модульный адаптер (на сленге называемый просто “коробка”), который показан на рис. А.22. Обычный кабель включается в нужный разъем и с другой стороны — в адаптер. Техническому специалисту не нужно полностью разбирать розетку, блок или коммутационную панель, для того чтобы проверить кабель; ему достаточно подключить тестирующее оборудование, например,

омметр, к адаптеру и провести требуемые измерения. Такие адаптеры производятся двух типов: трех- и четырехпарные.

Рис. А.20. Многопарный инструмент компании Pandiut

Рис. А.21. Запрессовочный инструмент компании Pandiut

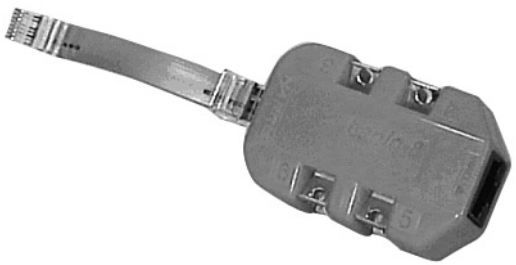


Рис. А.22. Модульный адаптер

Чтобы определить местонахождение труб, арматуры, стальных балок и других строительных элементов в стенах, в пол или потолок используются датчики металла. Ими рекомендуется пользоваться монтажникам и строителям перед тем, как они начнут сверлить отверстия для прокладки кабеля. Высокочувствительные датчики позволяют обнаружить крупного и среднего размера гвозди внутри стен, металлизированные желобки, медные и латунные трубопроводы, электропроводку, арматуру, телефонные пары и многие другие металлические объекты. Такие датчики сканируют стену на глубину до 15 см, если внешнее архитектурное покрытие не металлизировано (т.е. стены обшиты деревом, пластиком, покрыты штукатуркой или просто сделаны из бетона). Местоположение более-менее крупных металлических объектов (труб и арматуры), которые находятся достаточно глубоко внутри стен, этот прибор позволяет установить с точностью до 30 см.

Существует также другая разновидность датчика — датчик для обнаружения металлических балок и перекрытий (рис. А.23). Он предназначен для обнаружения металлических компонентов архитектуры, например, балок, которыми укрепляют стены. Описанные выше устройства позволяют правильно принять решение о том, где именно сверлить отверстия, выпиливать куски стен и т.п., и, конечно же, где разместить телекоммуникационные розетки и кабелепроводы. Второй тип датчика, предназначенного для обнаружения крупных объектов, позволяет определить местонахождение металлических частей и арматуры на глубине вплоть до 100 см. Все модели датчиков позволяют обнаружить электропроводку в стенах и избежать несчастных случаев при прокладке кабельной системы.

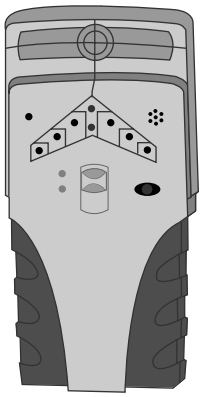


Рис. А.23. Датчик металла

Вспомогательные инструменты

Существует множество необязательных, но полезных в работе инструментов, которые значительно облегчают и упрощают процесс монтажа кабеля. Одним из них является “измерительное колесо”, которое служит для оценки длины куска кабеля (рис. А.24). У этого приспособления имеется счетчик, который подсчитывает число оборотов колеса. Специалист по укладке кабеля просто катит колесо вдоль маршрута, по которому будет проложен кабель; когда колесо достигнет конечной точки, счетчик будет показывать длину кабеля, необходимого для прокладки сегмента.

Монтажнику в работе также приходится использовать приспособления для поддержания порядка на рабочем месте. Веник, совок, пылесос — это не только инструменты уборщика, но и вспомогательный инструмент современного кабельного специалиста. Вакуумную мусороуборочную машину можно также отнести к инструментам монтажника, оборудование такого типа преимущественно используется в промышленных целях и в промышленных помещениях.

Рис. А.24. Измерительное колесо

Проволока для протягивания кабеля

Чтобы быстро и максимально просто достать или проложить провод внутри стен или под декоративным покрытием, необходимо использовать специальное приспособление (рис. А.25). Проволока для протягивания кабеля прокладывается в стенах или кабелепроводах. После того как такая проволока проложена до требуемой точки назначения или до какого-либо разветвления коробов, к ее концу крепко привязывают кабель, проволоку вытягивают с нужного конца наружу и сматывают. Кабель проложен по требуемому маршруту!

При работе с кабельными сетями рекомендуется использовать не стальную проволоку, как это принято обычно, а пластиковый шнур или леску, поскольку они с меньшей вероятностью могут повредить уже проложенные кабели. Многие опытные специалисты по монтажу кабельных сетей всегда вместе с кабелем укладывают в короба крепкую стальную проволоку (на всякий случай); впоследствии, если нужно будет проложить несколько дополнительных кабелей, это можно будет сделать легко и быстро.

Кабельная подставка

При прокладке кабеля используется множество приспособлений, которые упрощают этот процесс, облегчают работу с бобиной, на которой намотан кабель, и помогают избежать узлов (часто называемых “барашками”) и запутывания кабеля: *кабельные подставки* (за внешний вид их часто называют кабельными деревьями), лебедки, барабаны и т.п. На кабельной подставке можно разместить несколько небольших бобин кабеля одновременно (рис. А.26). Поскольку все кабели обычно прокладываются от какого-либо места до телекоммуникационного узла, кабельные подставки чаще всего используются на технологических площадках или в самом узле. После того как кабель проложен в нужную точку, его обрезают и заводят в коммутационную панель телекоммуникационного узла.

Рис. А.25. Проволока для протягивания кабеля

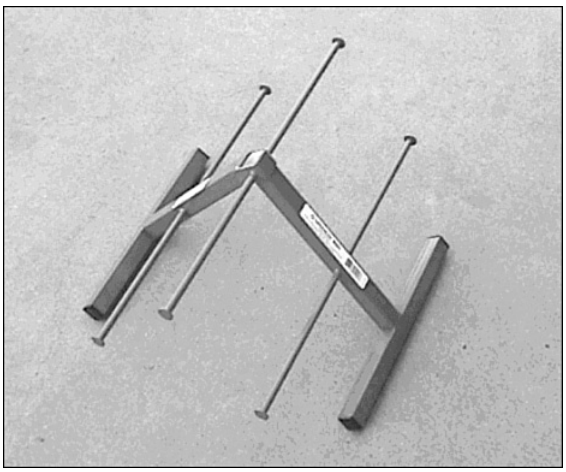


Рис. А.26. Кабельная подставка

Кабельные лебедки и барабаны используют при прокладке магистральных кабелей, поскольку большие бобины зачастую слишком тяжелы для того, чтобы поднять их вручную[23]. У лебедок обычно есть рычаги или другие приспособления, которые помогают приподнять бобину; после того как бобина приподнята, она свободно вращается на подшипниках, и кабель можно без лишних усилий размотать (в некоторых промышленных реализациях бобина фиксируется специальной защелкой).

[23] *Бобина с магистральным бронированным кабелем обычно весит несколько сотен килограммов. — Прим. ред.*

Чтобы облегчить процесс размотки кабеля, для некоторых типов бобин используются специальные вращающиеся барабаны. Для одной бобины необходимо два таких барабана, по одному с каждой стороны, — они устанавливаются у основания бобины. Далее в процессе укладки кабеля один монтажник тянет кабель, а второй вращает барабан.

Инструментальный барабан

Инструментальный барабан часто используется для того, чтобы обеспечить некоторый запас кабеля в его начальной и конечной точках, но ничто не мешает использовать его и в середине сегмента кабельной системы.

Инструментальный барабан похож на катушку большого диаметра, которая используется в механических кабелеукладчиках. Такие барабаны достаточно редко применяются при укладке кабеля вручную. Обычно их изготавливают из алюминия, диаметр барабана составляет не менее 30 см (около 1 фута), барабан встраивается в основу наподобие рамки. Он отличается от катушки тем, что у него нет креплений, с помощью которых он может быть к чему-либо прикреплен, кроме того, его можно извлечь из корпуса и использовать для намотки слабины где-нибудь в середине кабельного сегмента.

Кабельные блоки

Блоки, или ролики, обычно используются, когда необходимо проложить сегмент на открытом воздухе и при этом кабель не должен соскальзывать с той поверхности, на которой он лежит, или вообще не должен касаться какой-либо поверхности по требованиям пожарной или любой другой безопасности. Кабельные блоки используются также в том случае, если нужно проложить кабель над какой-либо хрупкой поверхностью или если кабель может повредить (например, поцарапать) поверхность. Следует устанавливать блоки, которые без особых проблем выдержат вес кабеля. Кабельные блоки уменьшают трение при прокладке кабеля и облегчают этот процесс (рис. А.27). Для прокладки кабеля посредством блоков могут использоваться специализированные лебедки, но он может быть проложен и вручную. Если кабель нужно повернуть на 45 градусов и более, рекомендуется установить инструментальный барабан.

Кабельные блоки можно использовать как для укладки нескольких сегментов кабеля, так и для установки тяжелого магистрального кабеля: для нескольких или единичных кабелей используются облегченные кабельные блоки; более тяжелые, промышленного образца блоки, рекомендуется использовать только для укладки магистральных кабелей. Магистральные блоки комплектуются бо́льшими по размеру и более жесткими креплениями, катушка блока обычно имеет бо́льший диаметр.

Проволочная сетка

Проволочная сетка (или зажим Келлема — Kellem grip) закрепляется на конце кабеля таким образом, что трос для протягивания кабеля может быть прикреплен к кабелю (рис. А.28). Сетку надевают на конец кабеля с тем расчетом, чтобы захватить

около 15 см телекоммуникационного кабеля (например, витой пары), и обматывают высококачественной изоляционной лентой. Чем большее усилие прикладывают к кабелю (т.е. чем сильнее приходится его натягивать), тем сильнее сетка обхватывает кабель. Зажим такого типа предназначен для работы только с одним кабелем, не рекомендуется пытаться надеть его на связку кабелей. Проволочные сетки выпускают нескольких размеров, чтобы можно было подобрать нужную для каждого случая.

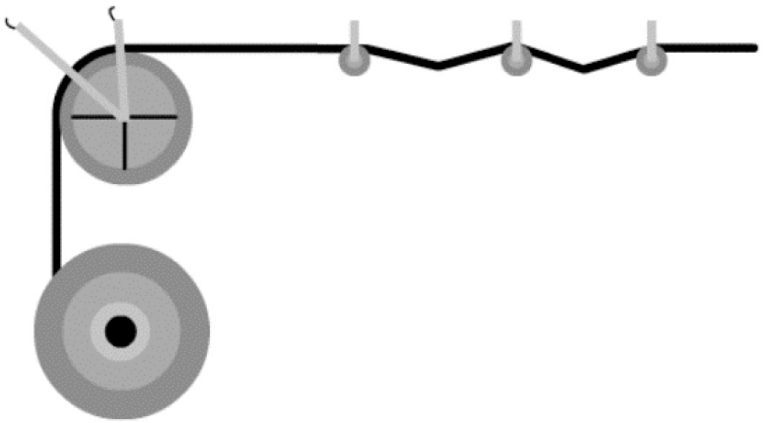


Рис. А.27. Укладка кабеля с помощью кабельных блоков и барабана

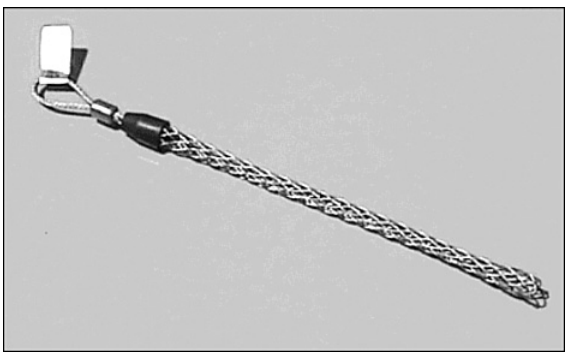


Рис. А.28. Проволочная сетка, или зажим Келлема

Часто встречаются разъемы Келлема, которые состоят из двух частей, они используются в том случае, если кабель необходимо захватить не в конце, а где-либо посередине. Такие разъемы используются для того, чтобы вытянуть слабину в середине кабельного сегмента. Разъемы, которые состоят из двух половинок, зачастую также используются для укладки магистрального кабеля в горизонтальные направляющие, т.е. для прокладки кабеля между этажами. Чтобы закрепить такое приспособление на кабеле, разъем разделяется на две половины, которые потом размещают вокруг кабеля, далее разъем затягивают с помощью специального прута.

Процесс установки

Процесс монтажа кабельной системы состоит из многих этапов, первым из которых является создание "чернового варианта" структурированной кабельной сети, когда кабели протягиваются между контрольными точками или кабельными узлами. Вертикальные кабели следует прокладывать только в специально предназначенных для этого местах и только в специальных отверстиях в противопожарных перегородках, независимо от того, проложен кабель через перекрытия или через отверстие в стене. Самый последний этап включает в себя терминирование медного кабеля, подключение розеток, запрессовку и др.

Ниже будут рассмотрены следующие темы, имеющие отношение к кабельным системам:

- черновая работа;
- укладка вертикальных кабелей;
- противопожарные мероприятия;
- терминирование кабеля;
- зачистка.

В процедуре развертывания кабельной системы можно выделить четыре основные фазы, которые являются составной частью любого проекта: черновая фаза, зачистка, доводка системы и поддержка установленной сети. Ниже указаны характеристики каждой из фаз.

- **Черновая фаза.** На этом этапе все кабели размещаются над подвесным потолком, в пленумах, под фальшполом, в стенах, коробах и т.д.
- **Фаза зачистки.** Основные действия, которые выполняют специалисты на этом этапе, — терминирование и упорядочивание кабелей.
- **Фаза доводки.** На этом этапе выполняются проверка и тестирование кабелей, поиск и устранение неисправностей и сертификация кабельной системы.
- **Поддержка клиентов.** Финальной фазой любого кабельного проекта является фаза поддержки системы и тестирования ее соответствия запросам пользователей. На этом этапе представители компании, которая разворачивала сеть, вместе с представителями компании-заказчика проверяют работоспособность сети, заказчику демонстрируются результаты тестов сети, техническая документация изготовителя и другая, относящаяся к структурированной кабельной системе. После окончания указанной процедуры заказчик может подписать акт о выполнении работ, если результат его удовлетворяет. Впоследствии компания-разработчик кабельной системы обеспечивает поточную поддержку своей системы, техническое сопровождение и устранение неисправностей в кабельной сети пользователя.

Черновая фаза

Данная фаза включает в себя прокладку кабеля в рабочей области (иногда называемой технологической), а именно: укладку кабелей в отдельные комнаты или прокладку кабеля к конкретным рабочим местам. Под технологической областью обычно понимают область снаружи телекоммуникационного узла или помещения. Оба конца каждого прокладываемого кабеля нужно обязательно промаркировать. В рабочей области нужно оставлять запас кабеля, поскольку в процессе запрессовки могут возникнуть проблемы, если укладчик совершит несколько ошибок, и кабеля может не хватить. Если кабель необходимо проложить позади декоративного покрытия стен, потолков или пола, его следует протягивать от кабельного узла к рабочему месту.

В большинстве случаев укладывать кабель в новом здании значительно проще, чем перепроектировать уже существующую кабельную систему или развертывать сеть в старом здании, поскольку в новых строениях меньше преград для кабеля. В новых строениях обычно не требуется выполнять какое-либо специализированное планирование, поскольку в них заранее предусмотрена возможность прокладки кабелей и есть кабельные колодцы. Следует координировать свои действия с другими рабочими, например, строителями, которые выполняют какие-либо работы в здании. Остальные работники должны знать о том, что в здании проложен кабель и его местоположение, чтобы ненароком не повредить только что развернутую кабельную систему.

Рабочей областью укладчики кабеля зачастую называют участок, где проводятся монтажные работы. Обычно такая область расположена рядом с телекоммуникационным узлом, как раз там, где терминируют и запрессовывают в разъемы кабели. Правильное размещение и установка оборудования значительно экономят время при монтаже кабеля, поскольку различные типы кабелей укладываются и устанавливаются различным образом. Кабель рабочих областей (т.е. зоны распределения) обычно предполагает использование нескольких небольших бобин кабеля одновременно, в то же время при установке магистральной кабельной системы обычно используется одна большая бобина.

Практическое задание А.4. Определение типа кабеля
В этом задании нужно идентифицировать различные типы кабелей, которые необходимо знать для выполнения лабораторных работ.

Установка горизонтального кабеля

Горизонтальным называют кабель, проложенный между горизонтальным кабельным узлом (HC) и настенной розеткой. Физически кабель может быть проложен как в горизонтальном, так и вертикальном положении. При укладке элементов горизонтальной кабельной системы рекомендуется следовать таким правилам:

- кабель всегда должен быть проложен параллельно стене;
- кабель нельзя укладывать по диагонали в пустотах;

- при разметке маршрута для укладки кабеля следует всегда выбирать кратчайший маршрут с минимальным количеством поворотов;
- кабель нельзя укладывать непосредственно на плиты подвесного потолка.

После того как установлена магистральная кабельная система, специалисты по монтажу переходят к установке горизонтальной кабельной системы, так называемой распределительной сети. Горизонтальная кабельная система обеспечивает сетевую связь на физическом уровне для пользователей и сетевых устройств с устройствами опорной сети и магистралью. Наиболее часто такая распределительная сеть разворачивается между пользователями и телекоммуникационными узлами, которые, в свою очередь, могут быть напрямую подключены к магистральному кабелю.

Укладка горизонтальных кабелей в кабелепроводы

Укладка кабеля в декоративные кабелепроводы очень похожа на процесс монтажа и установки кабеля в пустотах, над подвесным потолком и т.п. При монтаже данного типа кабеля обычно нет необходимости использовать блочные системы, чтобы временно зафиксировать кабель, поскольку он закрепляется в кабелепроводах (часто называемых *коробами*). Несмотря на то что начальная фаза укладки кабеля в короб очень похожа на тот процесс, что мы рассмотрели выше, при выполнении некоторых последующих этапов следует применять специфическую технику и оборудование.

Кабелепровод должен быть достаточно широк, чтобы вместить в себя требуемое количество кабельных соединений. Считается, что кабелепровод (или короб) должен быть заполнен кабелями не более чем на 40% от максимальной его емкости. Чтобы облегчить работу укладчикам кабеля, все компании-производители сопутствующего сетевого оборудования выпускают специальные таблицы, по которым можно подсчитать максимальную длину кабеля, который может быть уложен в определенный тип короба. Следующее, что следует принять во внимание, — общая длина короба и количество изгибов на 90 градусов. Общепринято такое ограничение: общая длина одного отрезка короба не должна превышать 30 м[24] без специальных фиксаторов кабеля и на одном участке кабелепровода разрешено делать не более двух изгибов на 90 градусов. Чем толще пучок кабелей, тем большим должен быть радиус изгиба. Так, например, стандартно радиус для короба шириной 10 см[25] составляет 60 см[26]. Однако такой радиус изгиба, что интуитивно понятно, неприменим к пучкам кабелей от сети распределения, когда в одном коробе проложено 400 и более соединений; в таком случае радиус изгиба короба (и кабелей) должен быть не меньше 90 см[27].

При укладке кабеля в кабелепроводы неоценимую помощь может оказать специальный компрессор, на жаргоне называемый “пылесосом” (рис. А.29). Специализированный зонд из пенорезины, иногда называемый “мышью”, к концу которого

[24] *98 футов. — Прим. ред.*
[25] *4 дюйма. — Прим. ред.*
[26] *24 дюйма. — Прим. ред.*
[27] *35 дюймов. — Прим. ред.*

привязана легкая прочная леска, размещают в торце короба. После того как зонд смазывают каким-либо жидким бытовым моющим средством, к другому концу кабелепровода подсоединяют мощный компрессор, похожий на те, что используются в промышленных установках. Такой компрессор позволяет протащить зонд с привязанной к нему леской через весь короб. Специальные насадки для промышленных компрессоров позволяют не вытягивать, а "продувать" зонд через короб. Для сложных профилей кабелепроводов или в других специфических случаях зачастую приходится использовать два компрессора одновременно: один закачивает воздух в короб, второй откачивает (как пылесос). Когда зонд достигает конца кабелепровода, к леске привязывается крепкий трос (стальной или пластиковый) и протягивается в обратном направлении. Такой трос используется для протягивания кабелей через короб.

Рис. А.29. Система "продувки" кабелепроводов

Кабельные каналы

Кабельными каналами (*raceway*) называют приспособления, в которые укладывается кабель в процессе установки структурированной кабельной системы. Этим термином обозначают как обычные электротехнические коробы для проводов электропитания, так и специальные кабельные направляющие, монтажные стойки, системы, которые встроены в пол или стены, а также пластмассовые и металлические кабелепроводы и настенные коробы.

Настенные коробы обычно используются в том случае, если кабель невозможно проложить нигде в другом месте, кроме как на виду (рис. А.30). Декоративные пластиковые настенные коробы производятся разного размера, поэтому достаточно легко подобрать нужный для определенного количества кабельных соединений. Декоративные пластиковые коробы значительно проще устанавливать, чем металлические, кроме того, они красивее.

Рис. А.30. Кабельные каналы

Запрессовка кабелей в разъемы

Концы кабеля в рабочей области необходимо запрессовать в разъемы либо подключить к настенным розеткам или блокам. Если кабель проложен не непосредственно в полостях за стенами и не над подвесным потолком, а в специализированных кабелепроводах, то для укладки кабеля может быть использована проволока, протянутая от розетки до ближайшего выхода из кабелепровода или рабочей области.

Бетонные и кирпичные стены обычно не имеют пустот или пленумов, в которых можно разместить кабель, поэтому для установки кабеля приходится использовать декоративные настенные коробы. Перед тем как начинать укладку кабеля, следует жестко закрепить такие коробы на стенах согласно рекомендациям и схемам производителя. После этого можно прокладывать кабель в коробах, выводить его в настенные розетки и телекоммуникационные узлы и выполнять распайку или запрессовку концов кабеля.

Закрепление кабеля

Финальным этапом черновой фазы является жесткое закрепление установленного кабеля. Для этого может быть использовано множество приспособлений: самозатягивающиеся петли, гибкие крючки, J-образные крючки и т.п. Кабели компьютерной сети ни в коем случае нельзя прикреплять к кабелям электропитания. Несмотря на то что на первый взгляд такой метод закрепления кажется практичным и удобным, он нарушает правила электрической безопасности и может привести к снижению скорости передачи данных за счет наводок и помех. Кабель также нельзя закреплять на водопроводных трубах и системах отопления или полива газонов.

В высокопроизводительных сетях кабели могут быть изогнуты только под определенным углом, стандартный радиус изгиба кабеля должен быть в четыре раза больше диаметра самого кабеля, поэтому для закрепления кабеля нужно использовать

приспособления, которые учитывают это требование (рис. А.31). Петли, крючки и другие приспособления должны соответствовать стандартным спецификациям, кроме того, их необходимо размещать на определенном расстоянии друг от друга (обычно такое расстояние указано в сопроводительной документации). В том случае, если в документации не указано максимальное расстояние между приспособлениями, следует располагать петли и крючки на расстоянии не более 1,5 м[28] друг от друга.

Рис. А.31. Самозатягивающиеся петли, крючки и другие приспособления для закрепления кабеля

Если кабельный желоб или корзина размещены под потолочным покрытием или в пустотах, то приспособления для закрепления кабеля использовать необязательно.

Меры предосторожности при установке горизонтальной кабельной системы

При протягивании кабелей может быть повреждена внешняя оболочка кабеля, если не будут предприняты специфические меры предосторожности. Избыточные усилия или натяжение кабеля, нестандартный радиус изгиба, который не соответствует стандартам, могут привести к уменьшению скорости передачи данных или вообще к невозможности использования кабельной системы. Укладчик должен проверить маршрут, по которому будет проложен кабель, рассмотреть и проверить проблемные места и преграды, чтобы избежать повреждений в будущем.

Ниже перечислены несколько основных мер предосторожности, которые следует предпринять при укладке горизонтальной кабельной системы.

- Кабель может застрять или повредиться в том месте, где он входит в кабелепровод. Рекомендуется использовать специальные наконечники или заглушки, чтобы избежать повреждения оболочки, оплетки и, возможно, самих проводников кабеля.
- Если в кабельной системе есть крутые повороты под углом около 90 градусов, кабель может быть сплюснут, даже несмотря на то что используются специальные катушки или бобины. Если при укладке кабеля приходится прилагать

[28] *4,9 фута. — Прим. ред.*

большое усилие, чтобы протянуть его, рекомендуется уменьшить кусок кабеля, с которым приходится работать, и выполнять укладку системы поэтапно. Не следует превышать значения нагрузки на кабель, которые указаны в его документации.

- При укладке кабеля с помощью лебедки или катушек следует стараться уложить кабель одним плавным непрерывным движением. Когда укладка кабеля начата, желательно довести ее до конца без перерывов. Частые остановки могут привести к тому, что кабель застрянет, а также повысить нагрузку на кабельную систему, из-за чего кабель может сильно растянуться.

Установка настенных розеток на гипсокартон

Прежде чем приступить к укладке кабельной системы в стенах, над подвесным потолком и в телекоммуникационных колодцах здания, следует выключить электропитание в рабочей области. Если сложно определить, проходят ли какие-либо провода электропитания через помещения, в которых ведутся работы, или проходит ли провод от конкретного щита электропитания через помещения, рекомендуется выключать питание во всем здании.

ВНИМАНИЕ!

Никогда не прикасайтесь к кабелям питания! Даже если питание было выключено во всей рабочей области, никогда нельзя быть уверенным в том, что какой-то кабель не находится под напряжением.

Перед началом работ следует выяснить, где размещены огнетушители.

Одежда работающих должна соответствовать некоторым минимальным требованиям: рукава и штанины рабочей одежды (лучше — комбинезона) должны быть длинными, чтобы защищать руки и ноги от мелких порезов. Запрещено носить излишне свободную одежду, поскольку она может за что-то зацепиться или застрять в деталях каких-либо механизмов.

Перед тем как начать работы над подвесным потолком, следует изучить рабочую область. Приподнимите несколько плит подвесного потолка и осмотритесь. Прежде всего следует установить местоположение электрических кабелепроводов, отверстий и труб системы вентиляции, механических приспособлений и всего, что может вызвать проблемы при укладке или в процессе эксплуатации кабельной системы.

Глаза работающего должны быть защищены специальными очками, особенно, если монтажнику приходится что-либо пилить или сверлить. Очки также рекомендуется использовать при работе в узких пространствах и проходах, при монтаже кабеля над подвесным потолком на тот случай, если что-либо упадет сверху, чтобы защитить глаза, если монтажник наткнется на что-то в полутьме, а также предотвратить попадание в глаза пыли и мусора.

Следует проконсультироваться с главным инженером или комендантом здания насчет того, есть ли в помещениях асбест, свинец или другие подобные материалы.

Если есть структуры, которые содержат подобные вещества, следуйте принятым нормам безопасности при работе с ними.

В рабочей области нужно поддерживать порядок и чистоту. Не следует разбрасывать инструменты, поскольку кто-то может на них наступить. Крупногабаритные инструменты следует складывать в определенном месте так, чтобы никто не споткнулся о них.

ВНИМАНИЕ!

При укладке кабеля в стенах, над подвесным потолком или в подсобных помещениях следует лишний раз убедиться, что система электропитания обесточена. Если в рабочей области есть провода, которые трудно идентифицировать, необходимо отключить абсолютно все электричество в здании.

При монтаже розеток стандарта RJ-45 следует придерживаться такой последовательности действий:

1. розетка должна быть размещена на высоте 30-45 см от пола. Просверлите небольшое отверстие. Проверьте, нет ли преград для кабеля в таком отверстии: например, в отверстие можно вставить кусок кабеля и попробовать вращать его. Если зонд (или кусок кабеля) наткнется на какую-либо преграду, следует выбрать другое место для розетки на достаточно удаленном расстоянии. После этого повторите процедуру;
2. определите нужный размер отверстия для коробки, в которой будет установлена розетка, например, прислонив розетку к стене и обведя ее контур карандашом;
3. перед тем как вырезать отверстие для розетки, используя уровень с отвесом[29], убедитесь, что отверстие будет прямоугольным и размещено ровно. С помощью инструментального ножа вырежьте отверстие: нож следует продавить через гипсокартонную стену, расковырять им небольшое отверстие так, чтобы потом лезвие могло свободно двигаться, либо так, чтобы в отверстие можно было вставить узкую ножовку;
4. вставьте ножовку в отверстие и вырежьте кусок стены по обведенному карандашом контуру. Выпиливать отверстие нужно аккуратно, причем следует сделать все необходимые распилы так, чтобы кусок стены потом не нужно было выламывать и чтобы его можно было без усилий вынуть. Убедитесь в том, что коробка розетки и ее крепления проходят в отверстие.

Если для установки розетки используется специализированный корпус или коробка, не следует закреплять ее до того, как к розетке будет проложен кабель.

[29] *Столярный инструмент. — Прим. ред.*

Установка розеток на бетон и штукатурку

Розетки значительно труднее устанавливать на бетонные стены, чем на гипсокартон. Рекомендуется придерживаться следующей последовательности действий при установке розеток и других приспособлений на твердых поверхностях:

1. выберите место для розетки;
2. с помощью молотка и зубила удалите штукатурку или декоративное покрытие стены. Глубина выемки должна быть такой, чтобы была видна бетонная стена или обрешетка[30] штукатурки;
3. с помощью инструментального ножа следует аккуратно обрезать штукатурку по краям и отделить от стены или обрешетки;
4. приложите коробку розетки к стене таким образом, чтобы она накрывала как минимум три планки обрешетки одновременно и, желательно, равномерно. Обведите контур корпуса розетки карандашом. С помощью электропилы с диском вырежьте отверстие нужной величины;
5. последовательно надрезая планки обрешетки, которые видны под штукатуркой, вырежьте углубление, в которое будет установлена розетка.

ВНИМАНИЕ!

Последний этап следует выполнять с большой осторожностью. Если вы попытаетесь сразу же перепилить электропилой планки с одной стороны, то когда вы будете отрезать их с другой стороны, обрешетка будет сильно вибрировать. Такая вибрация может привести к тому, что штукатурка вокруг отверстия растрескается, отделится от основы и будет обсыпаться.

Планки обрешетки следует сначала надпилить с правой и с левой стороны выемки, аккуратно делая надрезы, но не перепиливая планки полностью. Точно так же следует поступить с верхним и нижним краями углубления. Распилы нужно постепенно углублять таким образом, чтобы вырезаемый кусок лишь слегка держался на месте. Далее следует полностью перепилить планки обрешетки, начиная с правого верхнего угла и заканчивая левым нижним (или наоборот). Поскольку планки подложки обычно размещены по диагонали, кусок обрешетки должен легко выниматься из отверстия. Точно так же следует поступить с оставшимся куском подложки углубления. На последнем этапе подготовки отверстия для настенной или встроенной телекоммуникационной розетки следует удалить выступающие куски планок обрешетки и по краям отверстия.

[30] *Деревянные планки, которые укладывают поверх бетонной стены и покрывают штукатуркой. — Прим. ред.*

Установка розеток на деревянной поверхности

Чтобы установить розетки на деревянной стене, выполните следующие действия:

1. выберите место, где будет установлена розетка. Если телекоммуникационные розетки предполагается устанавливать на плинтус, то нужно очень аккуратно вырезать выемки для розеток и вкручивать шурупы так, чтобы не пробить плинтус насквозь (т.е. следует рассчитывать на то, что толщина плинтуса в среднем не превышает 5 см);
2. используя коробку розетки в качестве шаблона, очертите контуры будущего отверстия. Просверлите дрелью отверстия в углах намеченного контура, выпилите отверстие по контуру узкой ножовкой или лобзиком.

Монтаж телекоммуникационных розеток заподлицо

Когда отверстие для установки готово, можно начинать монтаж розетки. Если в конструкции розетки есть коробка, то нужно сначала пропустить кабель через одно из отверстий на задней панели. Далее следует аккуратно разместить коробку в отверстии или выемке и закрепить с помощью специальных зажимов и приспособлений. Обычно в таких зажимах есть специальные винты, затягивая которые, можно плотнее прижимать коробку к стене.

Далее следует запрессовать кабель в разъем розетки, и после этого можно устанавливать внешнюю декоративную панель. Обычно конструкция розетки позволяет присоединить декоративную панель без каких-либо дополнительных инструментов: ее необходимо просто приложить к коробке розетки в нужном положении и аккуратно прижать пальцами до характерного щелчка, который укажет на то, что панель жестко зафиксирована.

Укладка кабеля в уже существующие коробы

Зачастую возникает необходимость добавить несколько кабелей к уже развернутой кабельной системе и проложить новые соединения к настенным розеткам, разъемам или коммутационным панелям. Если кабельная система между розетками и телекоммуникационным узлом размещена в коробах или промышленных кабелепроводах, то для прокладки кабеля можно воспользоваться проволокой: ее следует пропустить через отверстие розетки и проталкивать до тех пор, пока она не выйдет из кабелепровода на другом конце или в любом ближайшем разрыве короба. Кабель с помощью специальных приспособлений или обычной изоляционной ленты можно прикрепить непосредственно к проволоке и с ее помощью “вытащить” нужный сегмент через розетку.

Если же кабелепроводов нет, кабель можно проложить непосредственно за гипсокартонной стеной или декоративным покрытием. Прежде всего следует проделать отверстие в стене в том месте, где будет размещен разъем; вырезать его следует аккуратно, чтобы оно не было бо́льшим, чем требуется. Обычно диаметр отверстия равен 1-2 см. Второе отверстие нужно вырезать под потолком (предполагается, что кабельная система размещена над подвесным потолком), в него следует вставить проволоку и

опустить ее до уровня нижнего отверстия, далее необходимо достать проволоку из нижнего отверстия. Некоторые специалисты по монтажу предпочитают использовать леску с привязанным к ней грузом вместо проволоки. Через нижнее отверстие такую леску можно подцепить с помощью проволочного крючка.

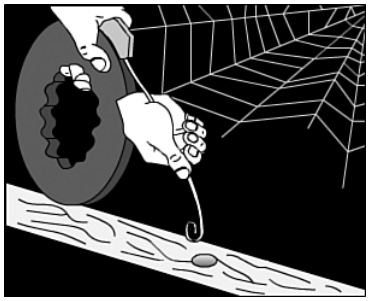


Рис. А.32. Укладка кабеля с помощью проволоки

После того как удастся вытащить проволоку или леску через нижнее отверстие в стене, к ней можно привязать специальную гибкую ленту. Эту процедуру следует повторить для всех участков кабельного сегмента; такой порядок действий необходим, поскольку протащить проволоку через углы здания практически невозможно, и приходится разбивать кабельный маршрут на участки и выполнять укладку поэтапно. К такой ленте теперь можно привязывать кабель и укладывать его по требуемому маршруту.

Если стена сплошная, например, сделана из кирпича и бетона, декоративного покрытия или гипсокартона нет, то проложить кабель в простенке не получится. В таком случае используются настенные декоративные коробы. Перед тем как монтировать кабель такие коробы, следует жестко закрепить их на стенах согласно рекомендациям производителя (обычно это делается с помощью дрели, дюбелей и шурупов). Теперь можно укладывать кабель; монтировать кабельную систему в таких коробах значительно проще.

Укладка горизонтального кабеля в подвале

В процессе установки горизонтальной кабельной системы часто можно столкнуться с такой ситуацией, когда кабель необходимо проложить в подвале здания или каких-либо пустотах в фундаменте. Рекомендации по тому, каким образом можно выполнить эту задачу, приведены ниже. Такая последовательность действий не является обязательной — это один из вариантов укладки кабеля.

1. Просверлите отверстие диаметром 3,2 мм в углу помещения в полу на самом нижнем этаже здания.
2. В отверстие можно вставить либо штырь с зажимом на конце, либо кусок проволоки, который потом легко будет обнаружить с другой стороны.
3. Спуститесь в подвал и найдите установленный кусок проволоки.

4. Пометьте нужное место в подвальном помещении, например, с помощью изоляционной ленты. Метка должна быть размещена на 57 мм[31] ниже просверленного отверстия.
5. В том месте, где была нанесена метка, просверлите еще одно отверстие диаметром 19 мм. Его нужно сверлить строго горизонтально и перпендикулярно стене (параллельно перекрытию), в отличие от первого, которое было сделано под углом.
6. Протолкните кабель через второе отверстие большего диаметра к телекоммуникационной розетке рабочей области.
7. Рекомендуется оставить достаточный запас кабеля, 60-90 см, как со стороны розетки, так и с обратной.

Установка вертикальной кабельной системы

Методы укладки кабелей вертикальной кабельной системы достаточно сильно отличаются от методов горизонтальной. К вертикальной кабельной системе могут относиться магистральные соединения и каналы уровня распределения сети. Несмотря на то что магистральные кабели могут быть развернуты горизонтально в здании, с точки зрения принадлежности к логической структуре сети они считаются элементом вертикальной инфраструктуры. Кабели и каналы уровня распределения сети чаще относят именно к горизонтальной распределительной кабельной системе, но иногда их также считают вертикальной кабельной структурой.

Кабели вертикальной кабельной системы обычно размещают в специализированных кабелепроводах, кабельных рукавах или кабельных колодцах в полу. Прямоугольное углубление в полу, в котором может быть размещен кабель, обычно называют кабельным желобом. Кабельными спусками называют отверстия в полу и перекрытиях здания, которые обычно имеют диаметр около 10 см; в таких отверстиях размещают кабельные рукава. Не все спуски или кабельные колодцы могут совпадать в вертикальном направлении, они могут быть сдвинуты относительно друг друга; специалист по монтажу кабеля в таком случае должен рассмотреть этот вопрос и попытаться совместить отверстия или разработать альтернативную схему укладки кабеля.

Развертывать вертикальную кабельную систему можно как от самого верхнего этажа до нижнего, так и наоборот. Первый вариант установки кабеля — сверху вниз — обычно проще, поскольку монтажникам будет помогать гравитация, и необходимость во многих вспомогательных инструментах (лебедках, барабанах и т.п.) отпадет. Второй вариант укладки кабеля — снизу вверх — предпочтителен в тех случаях, когда по каким-либо причинам доставить большие бобины с кабелем на верхние этажи невозможно либо технически сложно. В такой ситуации тоже далеко не всегда приходится пользоваться специализированными приспособлениями, однако следует помнить, что необходимо закреплять кабель и использовать тормоз бобины, чтобы кабель не упал вниз.

[31] *Данная величина соответствует стандартной высоте плинтуса в США. — Прим. ред.*

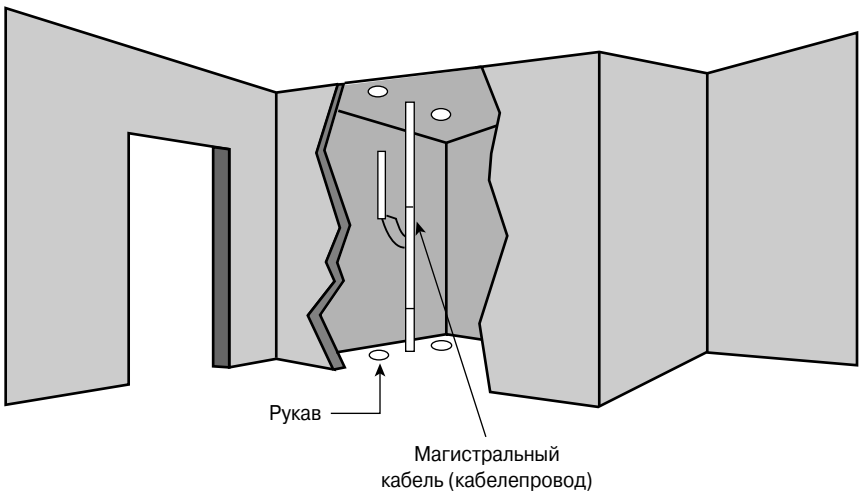


Рис. А.33. Типичная вертикальная кабельная система и кабельный спуск

Кабельные лебедки

Укладка кабеля в вертикальные колодцы и стояки — это трудоемкая и опасная задача. Монтажнику следует следить за тем, чтобы бобина кабеля не начала разматываться слишком быстро и не вышла из-под контроля. Чтобы предотвратить такие ситуации, бобины снабжают специальным фиксирующим устройством или тормозом.

Чтобы поднять кабель (т.е. проложить его в вертикальные кабелепроводы), часто используют специальное приспособление, которое называется кабельной лебедкой (рис. А.34). Оборудование, используемое для прокладки кабеля, может представлять опасность как монтажников, которые с ним работают, так и для тех, кто находится неподалеку. Строго рекомендуется, чтобы в рабочей области находились только специалисты по монтажу кабеля и не было посторонних. Например, при протягивании крупногабаритного кабеля или большого куска кабеля большим нагрузкам подвергается как сама лебедка для укладки кабеля, так и трос, который используется для монтажа. Если такой трос лопнет, он может причинить увечья кому-либо из работников. Опытные монтажники стараются держаться подальше как от сильно натянутых тросов, так и от механических частей и механизмов.

На заводе-производителе можно заказать кабельные бобины с фиксаторами, которые окажут неоценимую помощь в работе. Если же найти требуемый кабель проблематично, для фиксации может использоваться проволочная сетка Келлема. Следует помнить, что выполнять протяжку кабеля нужно плавно, останавливать процесс не рекомендуется. Остановить укладку кабеля можно только в случае крайней необходимости. После того как кабель уложен в кабелепроводы, трос и лебедки нужно каким-либо образом закрепить и оставить в таком состоянии до тех пор, пока не будут установлены распорки, крепеж или проволочная сетка (рис. А.35).

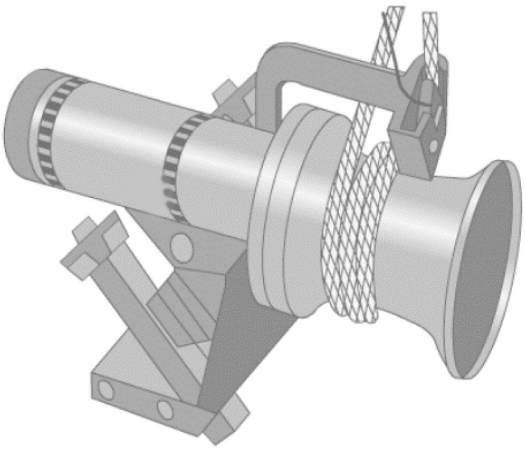


Рис. А.34. Шпилевая лебедка

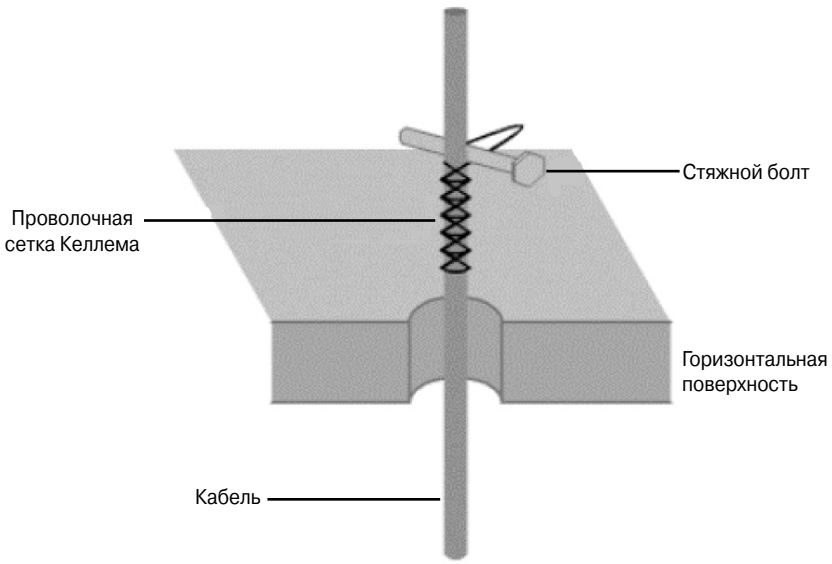


Рис. А.35. Фиксация вертикального кабеля с помощью проволочной сетки и болта

Метод фиксации вертикальных кабелей

Один из методов закрепления кабеля предполагает использование проволочной сетки размером 25?30 см, которая похожа на сетку Келлема, но состоит из двух половинок. Размер сетки должен совпадать с диаметром пучка кабелей, которые необходимо зафиксировать. Бобину кабеля или лебедку нужно поставить на тормоз, кабель следует закрепить с помощью проволочной сетки на каждом этаже и затянуть ее

потуже болтом. Далее следует аккуратно отключить фиксирующие устройства на бобинах и ослабить кабель. Установка вертикальной кабельной системы окончена.

Советы по установке кабеля

При укладке кабельной системы можно руководствоваться советами, перечисленными ниже.

- По возможности рабочую зону по монтажу кабеля следует располагать как можно ближе к первому повороту кабельного маршрута на девяносто градусов. Значительно проще укладывать кабель через резкий поворот, когда он еще не далеко отмотан от коробки или бобины, чем делать это в самом конце, когда по маршруту уже проложено несколько десятков метров кабеля. Чем больший сегмент кабеля уже установлен, тем больше он будет весить, иными словами, чем больше кабеля уложено, тем больший вес нужно поднимать монтажнику и бо́льшие усилия прикладывать.
- Рекомендуется использовать специальные синтетические смазочные материалы на длинных маршрутах или маршрутах со сложным профилем, чтобы не повредить кабели.
- Бобину с кабелем в коробке следует располагать так, чтобы отверстие находилось сверху.
- Если проволока, которая используется для протяжки кабеля, застряла, следует обернуть ее несколько раз вокруг оси и одновременно с этим попробовать ее вытянуть.
- Вместе с кабелем рекомендуется укладывать стальной или пластиковый трос. Он может понадобиться в будущем, если возникнет необходимость установить дополнительные кабели.
- Если необходимо оставить запас кабеля, рекомендуется уложить его в виде восьмерки, чтобы избежать изгибов, переломов и не запутать. В качестве подручных средств в таком случае можно использовать как специальные катушки, так и все, что может оказаться под рукой, например, два ведра.
- Закрепить кабель в вертикальном положении, если он проложен через несколько этажей, может быть очень даже непросто. Для решения этой проблемы можно использовать стальной трос, оба конца которого следует закрепить. К такому тросу по мере необходимости можно привязывать кабели и значительно облегчить себе этим задачу.

Противопожарные стены

В зависимости от того, какие именно кабельные материалы были выбраны в процессе установки структурированной кабельной системы и как именно был проложен кабель, может существенно измениться маршрут распространения огня в здании и уровень защиты сооружения от пожаров. От указанных двух факторов также зависит то, какой и в каком количестве дым и какие токсичные вещества будут выделяться, а также скорость распространения пламени и дыма. За счет использования

специальных кабелей в огнеупорной оболочке можно значительно уменьшить степень проникновения дыма и пламени за огневые преграды, а использование специальных противопожарных перегородок в тех случаях, когда проникновения не избежать, позволяет уменьшить количество дыма и замедлить скорость распространения пламени. При возникновении пожара чаще всего убивает именно дым, а не огонь.

Противопожарные перегородки

Противопожарные перегородки изготавливаются из специальных материалов и препятствуют проникновению дыма и пламени из одной части здания в другую. Огнеупорные стены позволяют ограничить область распространения пламени в строении, изолировать пожар и области, не затронутые огнем. Если какая-либо часть здания еще не затронута пожаром, задача противопожарных перегородок — не допустить распространения пламени или, по крайней мере, задержать его. Не менее важным свойством таких барьеров является то, что они должны изолировать области выделения токсических веществ и дыма при пожаре или, по крайней мере, замедлить этот процесс, чтобы у людей, находящихся в здании, было время на эвакуацию.

Отверстия в противопожарных перегородках

Часто возникает ситуация, когда кабель нужно проложить через противопожарную перегородку, т.е. проделать отверстие, которое на языке строителей называют “проходом”. В таком случае отверстие должно быть просверлено определенным образом и соответствовать некоторым стандартам (рис. А.36).

Рис. А.36. Типичные отверстия в противопожарной перегородке

Противопожарные перегородки обычно изготавливаются из нескольких общепринятых материалов. Чаще всего в качестве основного материала используется гажа. Если этим материалом покрыть пол, стены и потолок, то каждый его стандартный слой способен противостоять пламени пожара приблизительно в течении получаса, соответственно, двухслойное покрытие способно выстоять в два раза дольше. Вторым

не менее распространенным материалом для огнеупорных структур является бетон, как уложенный, так и в виде блоков.

В случае, когда необходимо проложить кабель через противопожарную перегородку, в ней придется высверливать отверстие. Их можно сделать как в одной или нескольких перегородках, так и в одной из стен полой противопожарной стены (такое отверстие называют *проколом*).

После того как в стене просверлено отверстие необходимого размера и формы, в него вставляют *рукав* — кусок кабельного короба или кабелепровода. Рукав должен быть достаточно широким, чтобы вместить жгут кабелей, и в нем должно оставаться место на будущее. Кусок короба по стандарту должен выступать с обеих сторон из стены на 30 см. После того как в рукав будет заведен кабель, его нужно залить специальной сертифицированной огнеупорной пеной, которая будет препятствовать распространению пламени через отверстие в перегородке в случае пожара.

Если необходимо проложить дополнительные кабели через существующее отверстие, следует сначала удалить огнеупорный материал, потом установить дополнительные кабели и залить отверстие пеной заново.

Запрессовка разъемов на концах медных кабелей

Оплетка проводов кабеля, за очень редким исключением, делается разного цвета, чтобы было легко различить пары. Цвета оболочки кабеля являются стандартными и должны быть одинаковы для всех телекоммуникационных кабелей по всему миру. Цветная маркировка — это универсальный метод идентификации отдельных пар в кабеле, поскольку в стандарте каждый цвет связан с определенным номером пары проводников.

Четырехпарный кабель

Для большинства сетей передачи голоса и данных используется неэкранированная витая пара (Unshielded Twisted Pair — UTP), в которой есть четыре свитые пары проводников в синтетической оболочке. Пары маркируются разными цветами согласно следующей схеме:

- **пара 1** — бело-голубой/голубой;
- **пара 2** — бело-оранжевый/оранжевый;
- **пара 3** — бело-зеленый/зеленый;
- **пара 4** — бело-коричневый/коричневый.

Первая пара всегда должна быть подключена к контактам 4 и 5 стандартного восьмиконтактного разъема или телекоммуникационной розетки. Пара 4 всегда должна быть подключена к контактам 7 и 8 стандартного разъема. Две оставшиеся пары могут быть подключены по-разному в зависимости от того, какой стандарт распайки используется: T568A или T568B (рис. А.37).

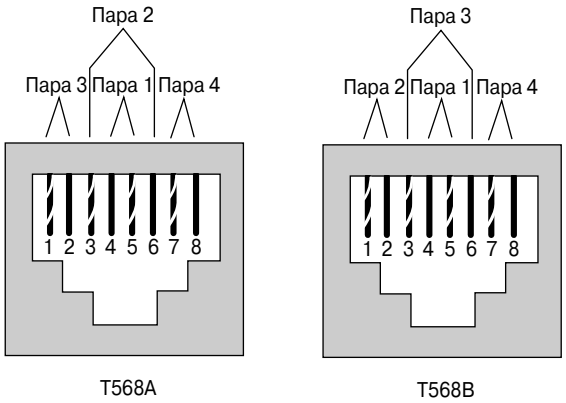


Рис. А.37. Стандарты распайки T568A и T568B

Стандарты T568A и T568B должны всегда использоваться в качестве схемы распайки для разъемов. Не следует создавать свою собственную схему распайки, поскольку у каждого провода в кабеле есть определенное предназначение. Если схема распайки неправильная, то устройства в сети либо не смогут взаимодействовать, либо производительность соединения значительно уменьшится.

Когда сеть проектируется и создается "с нуля", например, в новом здании, какую именно распайку использовать для запрессовки разъемов — T568A или T568B, должно быть четко указано в договоре. Если же тип распайки не указан, рекомендуется использовать тот, который наиболее популярен в данном регионе. Если же сеть разворачивается в старом здании или в здании, в котором уже есть некоторая кабельная система с определенным типом распайки, рекомендуется и в новой инфраструктуре использовать существующую распайку. Следует помнить, что каждый монтажник кабеля в одной и той же бригаде должен использовать один из двух стандартов, иначе вместо сети получится мешанина!

К сожалению, в нумерации пар и контактов разъема легко запутаться. Номер контакта — это определенное положение проводника в разъеме. Пары с одним и тем же номером окрашены в один и тот же цвет в любом кабеле, например, пара 2 всегда состоит из бело-оранжевого и оранжевого проводов. Тем не менее, в стандартном разъеме RJ-45 такая пара (пара 2) может быть подключена как к контактам 3 и 6, так и к контактам 1 и 2, в зависимости от того, какой стандарт используется: T568A или T568B.

Разъемы и розетки RJ-45

RJ-45 — это восьмиконтактный разъем, который может быть установлен в соответствующую розетку (рис. А.38). Кабель должен быть запрессован в разъем согласно стандарту T568A или T568B.

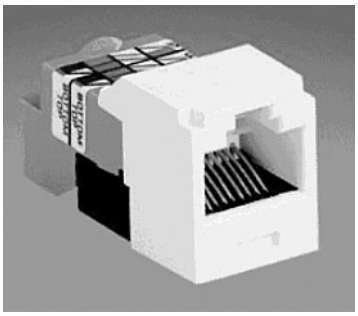


Рис. А.38. Стандартная восьмиконтактная розетка для разъема RJ-45

В разъемах и розетках стандарта RJ-45 есть восемь контактов, которые предназначены для подключения от одной до четырех пар. Точно так же, как и в разъемах RJ-11, пара с номером 1 всегда подключена к центральным контактам, в данном случае — к контактам с номерами 4 и 5. Пара с номером 4 (бело-коричневый и коричневый провода) всегда подключена к контактам 7 и 8. Пары с номерами 2 и 3 могут быть подключены к разным контактам в зависимости от схемы распайки. Если в сети используется стандарт T568B, пара с номером 2 (бело-оранжевый и оранжевый провода) заводится на контакты 1 и 2, а пара с номером 3 (бело-зеленый и зеленый провода) подключается к контактам 3 и 6. В стандарте T568A поменяны местами пары с номером 2 и 3, следовательно, пара с номером 2 должна быть подключена к контактам 3 и 6, а пара с номером 3 — к контактам 1 и 2.

Разъем RJ-45 обычно устанавливается на одном конце горизонтального кабеля, другой конец линии либо заводится в коммутационную панель, либо в так называемый блок 110.

Практическое задание А.5. Запрессовка кабеля категории 5e в разъемы
Основная задача этой практической работы состоит в том, чтобы читатель освоил технику безопасности при работе с кабельным инструментом, а также научился использовать стандарт T568B запрессовки разъемов для кабелей категории 5e и для установки кабелей в коммутационную панель.

Блок 110

Блок 110 представляет собой пассивное или активное коммутационное устройство с высокой плотностью портов, предназначенное для подключения телефонных линий и каналов передачи данных (рис. А.39). Блок выполнен таким образом, что при запрессовке в него кабеля создается надежный контакт между проводником и разъемом с низким сопротивлением. Существует множество разных конфигураций таких блоков, все они рассчитаны на объединение блоков, и поэтому могут удовлетворить потребности сети практически любого размера. Блоки 110 содержат специальные приспособления для укладки кабеля, которые позволяют аккуратно уложить и не перепутать кабели. Для установки кабеля в данный тип коммутационной панели используется специальный обжимный инструмент, который позволяет запрессовать

одновременно до пяти пар проводников. Такой инструмент нужно использовать осторожно или не использовать вообще в том случае, если блок содержит микросхемы или печатные платы, потому что они могут быть повреждены при запрессовке проводников в блок 110.

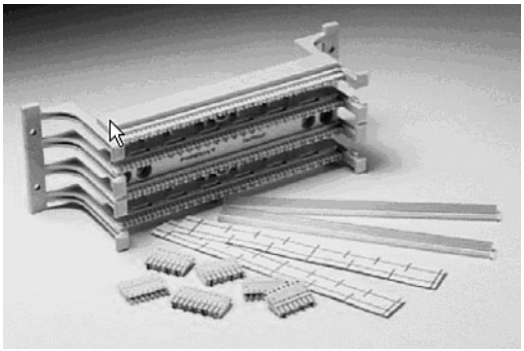


Рис. А.39. Блок 110

Практическое задание А.6. Запрессовка кабеля категории 5е в блок 110
В этом практическом задании необходимо запрессовать витую пару категории 5е в блок 110, научиться правильно пользоваться запрессовочным инструментом и многопарным запрессовочным инструментом модели 110.

Фаза зачистки

После того как кабельная система была развернута, необходимо удалить ненужный запас кабеля и подровнять его концы. Такие запасные кольца кабеля, которые обеспечивают слабину в процессе установки и могут пригодиться, если вдруг необходимо будет сделать какие-либо изменения, называют обычно абонентским ответвлением. Запас кабеля, который сворачивается в виде кольца и помещается в кабелепровод, не одобряется в стандартах TIA/EIA. Часто при укладке кабеля оставляют порядка 1 м запаса к концу первой фазы монтажа структурированной кабельной системы, хотя это и не является общепринятой практикой. Также не является общепринятым и не одобряется в стандартах такой подход, когда в телекоммуникационных узлах, в которые заведены сотни кабелей, монтажники оставляют запас кабеля длиной 2-3 м. Тем не менее, этот подход используется.

Несмотря на то что описанный выше подход может показаться расточительным, опытные монтажники знают, что запас кабеля никогда не помешает, а также оставит “пространство для маневра” (т.е. будет возможность внести какие-либо небольшие изменения) и упростит доступ к кабелям при их тестировании (или, как говорят монтажники, “прозвонке”). Наиболее часто встречающаяся ошибка начинающих монтажников — отрезанный кусок кабеля оказывается слишком коротким. Помните: избыточный кабель всегда можно отрезать, а вот нарастить слишком короткий кабель весьма и весьма сложно. Если кабель короткий, единственная альтернатива

состоит в том, чтобы проложить его заново, а это обойдется недешево с точки зрения затрат времени и труда.

Если при установке настенной розетки остается запас кабеля длиной около метра, рекомендуется укоротить его на 25 см и наклеить новую метку на расстоянии приблизительно 15 см от конца кабеля. Внешнюю оболочку кабеля необходимо удалить на расстоянии 5-7 см от его конца, чтобы получить доступ к отдельным парам проводников. Пары следует расположить требуемым образом и завести в розетку. Розетка правильно установлена, когда длина несвитых проводников кабеля без оболочки не превышает 1,5 см. Выступающие за контакты розетки провода должны быть обрезаны (рис. А.40).

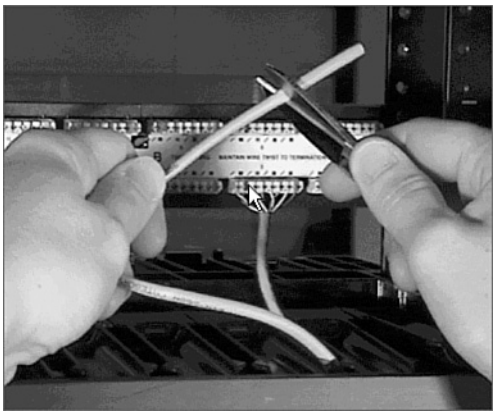


Рис. А.40. Обрезка кабеля до нужной длины

После того как розетка уже установлена, обычно остается от 15 до 20 см лишнего кабеля. Такой запас либо аккуратно сматывают, либо проталкивают обратно в стену. Избыток кабеля может пригодиться в будущем, если необходимо будет установить новую розетку вместо существующей; он также позволит снять розетку и получить доступ к отверстию в стене, если понадобится установить дополнительные розетки или проложить еще один кабель. Для кабелей, которые ведут к рабочим станциям, характерна такая ситуация, когда контакт между проводами и разъемом ухудшается или теряется вовсе за счет того, что кабель постоянно перетягивается с места на место, растягивается, изгибается и т.п.

Терминирование, или запрессовка кабеля

Процесс запрессовки кабеля в коммутационные панели телекоммуникационного узла обычно называют монтажом. Кабели запрессовывают в телекоммуникационные настенные панели или коммутационные панели сзади.

Проводники кабеля размещают в нужных контактных зажимах телекоммуникационных панелей, после поверх кабеля размещают монтажный инструмент (punch-down tool) и запрессовывают кабель. В зависимости от того, какое именно коммуникационное оборудование используется, в монтажный инструмент можно установить

соответствующие сменные лезвия, которые подходят именно к данному типу коммутационного устройства (рис А.41).

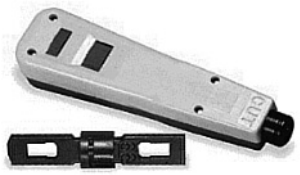


Рис. А.41. Устройство со сменным лезвием

Когда на монтажное приспособление оказывают давление, пружина внутри него позволяет умножить усилие и направить его в нужную точку за счет быстрого распрямления; сам механизм с некоторой точки зрения похож на спусковой курок пистолета. Монтажный инструмент проталкивает проводники кабеля между двумя ножами, которые срезают с них изолирующую оболочку и одновременно отсекают выступающие лишние куски провода. Такой метод запрессовки кабеля стандартно называется *монтажом с прорезанием изоляции* (insulation displacement), поскольку оболочка кабеля удаляется самими контактами коммутационного оборудования в процессе монтажа.

Монтаж с прорезанием изоляции обеспечивает надежный, вакуум-плотный контакт. Под вакуум-плотным контактом понимается такой контакт, когда само соединение проводника и ножа контакта не подвергается воздействию атмосферы, в данном случае подобное происходит за счет того, что изоляция продолжает плотно прилегать как к проводу, так и к прорезавшему ее ножу. Такой тип контакта долго служит и не окисляется. Обычные коммутационные панели используются в основном для сетей передачи данных, блок 110, в отличие от них, используется и для структур передачи данных, и для голосовых соединений.

Приспособления для укладки кабелей

Практически все коммутационные системы поставляются со строенными средствами для укладки кабелей. В блоках 110 есть специальные желоба и распорки для укладки кабеля между блоками панели. Распорки могут быть установлены как вертикально, так и горизонтально. Существует множество приспособлений для укладки кабеля, которые предназначены для использования в монтажных телекоммуникационных шкафах (рис. А.42).

При покупке оборудования для монтажа кабеля необходимо учитывать следующие особенности:

- система должна защищать кабель от изломов, перегибов и т.п., а также должна позволять использовать максимальный радиус изгиба кабеля в соответствии со стандартами;

- система должна быть масштабируемой: если необходимо добавить дополнительные кабели, они должны быть легко установлены в коммутационные приспособления;
- система обязана быть гибкой: кабель может быть подключен в любом направлении;
- коммутационная система должна быть совместима со стандартными горизонтальными кабелепроводами, кабель не должен быть поврежден или согнут под нестандартным углом;
- система должна быть прочной, она должна служить не меньше, чем прослужит кабельная система или оборудование, которое монтируется в нее.

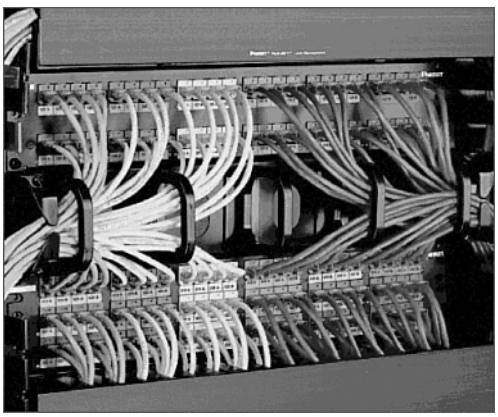


Рис. А.42. Приспособления для укладки кабеля компании Panduit

Правильная маркировка

Маркировка является очень важной частью структурированной кабельной системы. Если кабели не промаркированы на обоих концах, в будущем может возникнуть путаница. В стандарте TIA/EIA-606 указано, что каждый аппаратный терминал или разъем должен быть помечен уникальным идентификатором. Такой идентификатор можно нанести как непосредственно на само устройство, так и написать на метке, которую на него наклеивают. Когда такие идентификаторы наносятся на оборудование в рабочей области, метки или надписи должны быть нанесены или наклеены на передней панели каждой настенной розетки, на корпусе устройства, на разъеме или около него (в зависимости от конструкции). В большинстве технических заданий (ТЗ) на построение структурированной кабельной системы указано, что метки должны быть сгенерированы определенным образом на компьютере и распечатаны, тогда они будут уникальными, легко читаемыми и будут выглядеть достаточно солидно.

Метки и условные обозначения следует выбирать и генерировать таким образом, чтобы они были понятны не только вам, но и тому, кто будет работать с кабельной

системой много лет спустя. Среди системных администраторов широко распространена такая практика, которая предполагает, что в метку каким-либо образом включается номер комнаты. Далее каждому кабелю, который входит в эту комнату, присваивается одна или две (если кабелей много) буквы. В некоторых системах маркировки, например, в очень крупных сетях, используются разноцветные метки.

Чтобы быть уверенным в том, что метка не сотрется или не оборвется (если она наклеена), свободный конец кабеля можно промаркировать несколько раз, например, через каждые 60 см. Соответствующую метку также следует разместить на настенной розетке, катушке или точке входа в кабелепровод. Если проложено несколько кабелей к настенному телекоммуникационному блоку, их обычно связывают в пучок с помощью изоляционной ленты.

Вернемся опять к вопросу укладки кабеля.

При укладке дополнительных кабелей их следует приматывать изоляционной лентой к монтажному тросу на обоих концах и даже несколько раз посередине; следует также убедиться, что кабель не болтается отдельно от троса и не запутается в узел при прокладке. Не следует экономить изоляционную ленту! Вытащить застрявший кабель значительно сложнее, проложить новый — дороже; сэкономив небольшие деньги на изоленте, монтажник может потерять затем значительно больше денег и времени на укладку кабеля.

После того как кабель проложен по маршруту, его следует завести в телекоммуникационный узел. На кабеле также не следует экономить и укладывать его "внатяжку": проложите достаточное количество кабеля и оставьте приличный запас, чтобы кабель не был натянут, — обычно от 60 до 90 см.

Когда вы уже проложили кабель с запасом по маршруту и завели его в телекоммуникационный узел, вернитесь к бобине и наклейте или нанесите метки на все кабели, которые были проложены только что. Например, если был проложен пучок кабелей, пометьте каждый из них меткой, которая содержит соответствующий номер комнаты и букву. Не следует отрезать кабель до нанесения на него метки. Если следовать описанной выше процедуре, сетевая среда, которая используется для горизонтальной кабельной системы, к моменту окончательной установки будет четко промаркирована на обоих концах всех кабелей.

Фаза доводки

На последнем этапе установки структурированной кабельной системы монтажники тестируют и в определенных случаях сертифицируют свою работу. Тестирование позволяет убедиться в том, что кабели и проводники ведут туда, куда предполагалось, и запрессованы согласно требуемой распайке. Сертификация подразумевает проверку качества соединений, кабелей и контактов.

Основные темы, которые связаны с фазой доводки, включают:

- тестирование кабелей;
- принцип работы динамического рефлектометра (time-domain reflectometer — TDR);

- сертификацию и документирование кабельной системы;
- зачистку.

Тестирование кабелей

Для поиска закороток, разрывов, распаровки и других проблем с распайкой кабелей используются кабельные тестеры. После того как монтажник проложил кабель и запрессовал его в разъем, разъем необходимо включить в кабельный тестер и проверить правильность расположения проводов и наличие контакта. Если один из проводников был случайно заведен на неправильный контакт разъема, кабельный тестер поможет выявить ошибку. Даже простейший кабельный тестер позволяет обнаружить такие проблемы, как короткое замыкание двух проводников и разрыв одного из проводов. Тестер должен обязательно входить в стандартный набор инструментов монтажника. После того как вы проверили кабель с помощью кабельного тестера и убедились, что разрывов нет, его можно проверять с помощью кабельной измерительной аппаратуры и сертифицировать.

Тестирование — самый важный этап завершающей фазы монтажа кабельной системы. Оно позволяет убедиться в том, что все провода находятся в рабочем состоянии и что заказчик впоследствии не столкнется с какими-либо проблемами в кабельной сети. Проблему лучше всего устранить до того, как проект сети будет сдан, и до тех пор, пока она не стала большой неприятностью.

Тесты, которые используются для проверки функциональности кабеля, описаны в стандарте TIA/EIA-568-B.1. Самые распространенные тесты включают в себя проверку перечисленных ниже дефектов (рис. А.43).

- **Разрыв**. Провода или один провод в кабеле могут быть переломлены и не образовывать замкнутую цепь. Этот дефект может появиться как из-за неправильной запрессовки разъемов в кабеле, так и из-за повреждения кабеля, реже — из-за того, что кусок кабеля может быть испорчен или быть некачественным изначально.
- **Закоротка**. Оголенные проводники кабеля касаются друг друга, замыкая накоротко электрическую цепь.
- **Распаровка**. Провода из разных пар перепутаны и перемешаны.
- **Ошибки распайки или запрессовки**. Провода в многопарном кабеле подключены не к тем контактам, к которым положено, или на разных концах кабеля используются разные стандарты распайки.

В большинстве случаев простые функциональные тесты на наличие короткозамкнутых проводов, разрывов, распаровки и неправильной запрессовки проводятся на одном конце кабеля.

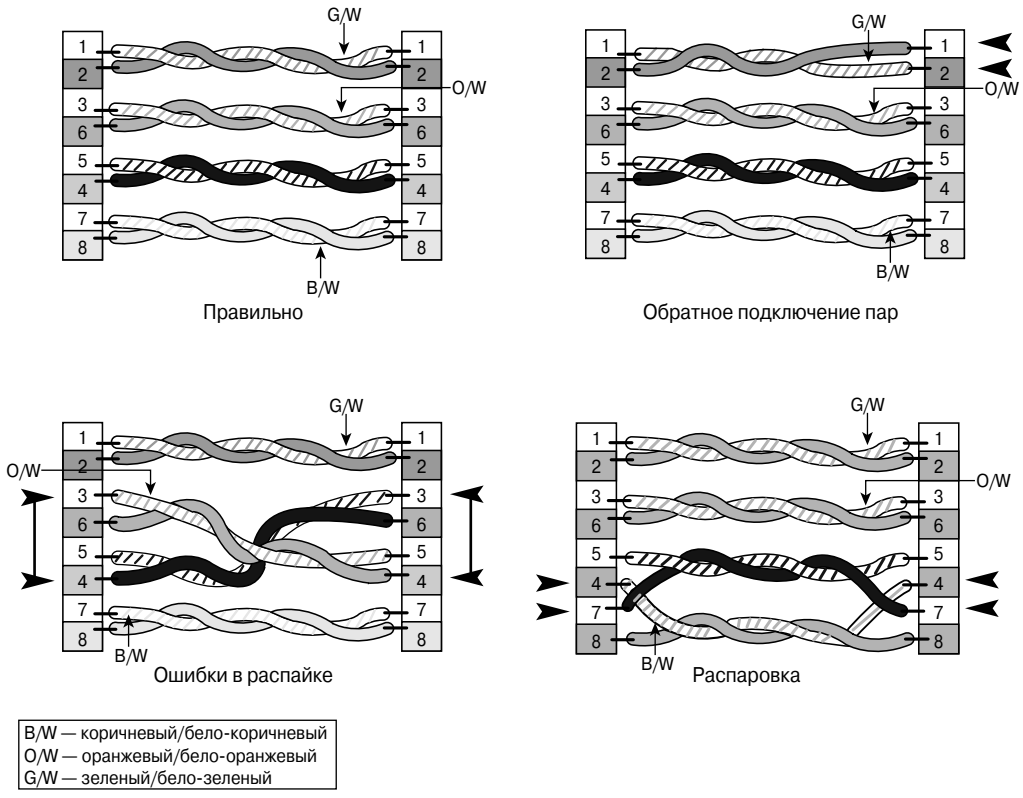


Рис. А.43. Дефекты кабеля, связанные с неправильной запрессовкой

Поиск короткозамкнутых проводов

Короткое замыкание возникает в том случае, когда один оголенный проводник касается другого, и они образуют замкнутую цепь для электрического тока (рис. А. 44). Короткое замыкание приводит к резкому падению напряжения; скорее всего, с оборудованием ничего не случится, но передать сигнал будет невозможно.

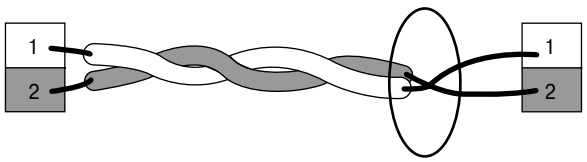


Рис. А.44. Короткое замыкание проводников кабеля

Чтобы определить, есть ли в кабеле короткозамкнутые проводники, нужно измерить сопротивление между двумя проводниками. Если короткого замыкания проводов нет, то между разными проводами омметр должен показывать бесконечное сопротивление. При этом прибор должен быть установлен на измерение небольших сопротивлений: при определенных условиях сверхчувствительная аппаратура может измерить сопротивление воздуха между проводами, но это не означает, что проводники замкнуты. Кроме того, если в омметре включен режим измерения высоких сопротивлений, монтажник может измерить сопротивление своего тела вместо сопротивления между проводами[32]. Зачастую у измерительных приборов есть как минимум один зажим с зубчиками (специалисты всего мира называют его "крокодилом"), который позволяет закрепить один щуп прибора на одном проводе, а вторым быстро проверить все оставшиеся проводники. Даже если такого зажима в комплекте с измерительной аппаратурой нет, его стоит приобрести, поскольку он позволяет проводить измерения, касаясь только одного щупа.

Поиск инвертированных проводов

Провода инвертированы, когда на одном конце кабеля сигнальный провод заведен на сигнальный контакт (Ring), а на втором конце кабеля он подключен к контакту заземления (Tip). Проще: в паре перепутаны "+" и "-" (рис. А. 45).

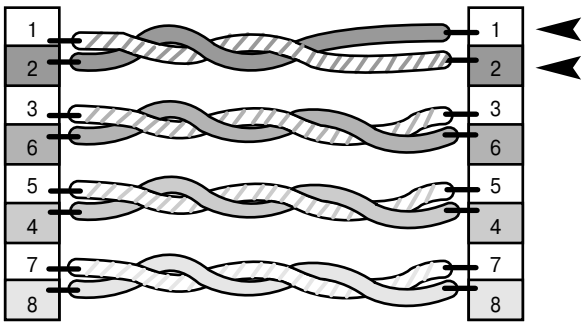


Рис. А.45. Инвертирование пары

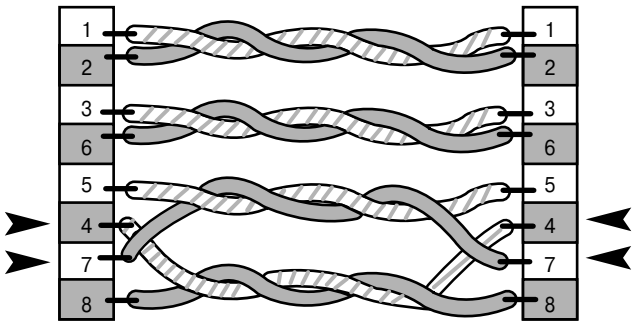
Исправить этот дефект можно, только удалив разъем RJ-45 с конца кабеля и установив новый.

Поиск распаровки

Если перепутать провода из разных пар, то получится распаровка (рис. А.46). Один из вариантов поиска распаровки — проверка кабеля с помощью омметра (с кабельным тестером сделать это проще). Прежде всего следует убедиться в отсутствии

[32] *Обычно щупы измерительного прибора вставляют в пластиковые кембрики (пластиковые трубки), чтобы не вносить искажения в измерения. — Прим. ред.*

в кабеле короткозамкнутых проводов. Если таковых нет, следует замкнуть каждую пару накоротко и проверить с помощью омметра, соответствует ли результат ожидаемому. Если будет обнаружен разрыв, значит, либо пары разведены неправильно, либо одна из пар переломана. Определить целостность пары можно с помощью генератора звуковой частоты, этот процесс часто называют "прозвонка кабеля". Кабельные тестеры высокого класса позволяют обнаружить распаровку проводников в кабеле за счет измерения уровня *перекрестных наводок* между парами.



Распаровка

Рис. А.46. Распаровка

Простые и простейшие кабельные тестеры также могут быть использованы для обнаружения распаровок в кабеле. В самых простых кабельных тестерах есть светодиодные индикаторы, которые сигнализируют о неправильной "полярности" подключения пар, замыканиях или обрывах.

Исправить этот дефект можно, только удалив разъем RJ-45 с одного или обоих концов кабеля и установив новый.

Динамический рефлектометр

Динамический рефлектометр (Time-Domain Reflectometer — TDR) — это устройство, которое передает импульс по проводам кабеля и принимает и интерпретирует отраженный сигнал ("эхо"), по которому устанавливает, есть ли в кабеле проблемы. Рефлектометр позволяет определить наличие в кабеле дефектов и распознать их: короткое замыкание это или разрыв. Устройство позволяет также определить расстояние до места, где есть дефект. Импульсный сигнал отражается от конца кабеля; если в проводниках присутствует дефект, сигнал отразится от этого места. Скорость, с которой сигнал распространяется в медном кабеле, называют нормальной, или номинальной, скоростью распространения. Она хорошо известна и занесена в таблицы для разных типов кабелей. При правильной настройке устройства такой кабельный тестер, измерив интервал времени между переданным импульсом и полученным ответом, рассчитывает длину кабеля на основании скорости распространения сигнала. Стандартно TDR-устройства позволяют показывать длину куска кабеля как в метрах,

так и в футах, их необходимо правильно сконфигурировать и нужно уметь ими пользоваться. Динамический рефлектометр — это одно из самых полезных средств для поиска и устранения проблем в кабельной системе.

Сертификация и документирование кабельной системы

Тестирование и сертификация структурированной кабельной системы — это не одно и то же. Тестирование — это проверка функциональности кабелей, она позволяет убедиться в том, что проводники могут передавать сигнал от одного конца кабеля на другой. Сертификация — это проверка производительности структуры, она позволяет определить качество кабельной проводки и ответить на следующие вопросы: "Насколько хорошо сигнал передается по кабелю? Подвержен ли передаваемый сигнал интерференции? Достаточно ли мощности сигнала на удаленном конце кабеля для его обнаружения и распознавания?"

Сертификационные тестеры

После того как работоспособность кабельной системы проверена, проводится ее сертификация и измерение производительности. Если структурированная кабельная система претендует на соответствие стандартам, ее нужно сертифицировать. Специализированные сертификационные тестеры позволяют выполнить все необходимые измерения параметров производительности сети, которые описаны в стандартах ANSI/TIA/EIA-568-B (рис A.47). Обычно в таких измерительных устройствах есть функция автоматического тестирования, поэтому все требуемые тесты можно запустить нажатием одной-единственной кнопки. Такие тесты включают в себя измерение уровня перекрестных наводок на передающем конце (near-end crosstalk — NEXT), проверку правильности запрессовки, измерение импеданса, определение длины кабеля, измерение сопротивления постоянного тока, измерение задержки распространения и потерь сигнала, флуктуаций задержки, затухания и отношения коэффициента затухания к наводкам. Результаты нескольких последовательных тестов устройство сохраняет в своей оперативной памяти. Результаты тестов могут быть загружены в персональный компьютер для дальнейшего анализа, из них могут быть сгенерированы документальные отчеты по тестам и представлены заказчику в качестве доказательства. Кроме функций сертификации, такие расширенные тестеры выполняют диагностические функции, которые позволяют не только обнаружить проблему, но и показать, как далеко от конца кабеля находится дефект и как он влияет на сеть.

Тестирование производительности кабельной системы проводится обычно на определенной заданной частоте. Такая частота определяется исходя из того, на какой скорости и в каком режиме будет работать кабельная инфраструктура. Например, кабель категории 5e проверяется и сертифицируется на частоте 100 МГц, кабель категории 6 тестируется на частоте 250 Мгц. Методы измерения производительности и соответствующие им тесты описаны в различных приложениях к стандарту TIA/EIA-568-B. Современное оборудование и программное обеспечение для тестирования сетей позволяют выводить информацию как в текстовом, так и в графическом виде.

Рис. А.47. Измерительный сертификационный тестер Fluke Networks 4000

Практическое задание А.7. Запрессовка разъемов на кабель категории 6
В этой работе необходимо попрактиковаться в запрессовке кабеля категории 6 и повторить основные требования и правила безопасности и охраны труда. При запрессовке кабеля следует соблюдать все требования к высокоскоростным соединениям.

Сертификация структурированной кабельной системы позволяет определить ее базовую производительность (baseline). При подписании договора на прокладку сети в него обычно включается стандарт сертификации, которому должна соответствовать будущая сеть. Установленная согласно договору сеть должна отвечать требованиям стандарта или может превышать их, например, за счет использования более качественного кабеля. Подробная документация, в которой показано, что сеть соответствует требуемым стандартам, должна быть представлена в качестве доказательства заказчику.

Процедура сертификации представляет собой довольно важный аспект финальной части проекта по установке кабельной системы сети. Она позволит компании, которая занималась установкой кабеля, определенно сказать, что в такой-то день и час кабели соответствовали заданному стандарту. Если впоследствии производительность кабельной системы изменится, то необходимо искать причину такого изменения; если же найти ее невозможно, нужно установить состояние кабельной системы ранее. Обычно чем выше категория кабеля, тем меньшие отклонения в качестве его производства допустимы, тем выше качество кабеля и его материалов и тем выше производительность сети.

Сертификационные тесты

Кабельная система считается прошедшей сертификацию в том случае, если она отвечает минимально допустимым для кабеля данного класса параметрам. Кабели должны соответствовать самым низким результатам или превышать их. Чаще всего результаты тестов в реальных условиях превосходят минимальные стандартные

величины. Разницу между результатами тестов в полевых условиях и минимальными параметрами называют *зазором*. Если при тестировании кабельной системы получен большой зазор, то это означает, что поддержка кабельной системы в будущем будет проста и сеть будет устойчива к низкокачественным соединительным кабелям или плохим кабелям оборудования.

Наиболее часто для сертификации используются спецификации, которые перечислены ниже.

- **Частотный диапазон**. Каждый кабель проверяется и сертифицируется в пределах некоторого частотного диапазона, который используется для обычной передачи информации по кабелю. Чем выше категория кабеля и его класс, тем шире частотный диапазон.
- **Затухание**. Этот параметр описывает величину (или, скорее, коэффициент) поглощаемой кабелем мощности сигнала. Чем меньше затухание, тем лучше проводники используются в кабеле и тем более высокого качества кабель используется.
- **Уровень перекрестных наводок на передающем конце (near-end crosstalk — NEXT).** Такие наводки возникают, когда сигналы от одной пары интерферируют с сигналами от другой на ближнем конце кабеля. Перекрестные наводки влияют на возможность передачи данных через кабель. Уровень наводок NEXT, приемлемый для каждого из классов кабелей, указан в их спецификациях.
- **Суммарная мощность наводок NEXT.** Когда в кабеле для передачи данных используются все проводники (например, как в технологии Gigabit Ethernet), то сигнал в одном проводнике интерферирует с сигналами всех пар, а не только с сигналом проводника своей пары. Этот параметр позволяет учитывать в расчетах эффективных помех взаимовлияние всех пар многопарного кабеля.
- **Отношение величины затухания к наводкам (Attenuation-to Crosstalk Ratio — ACR).** Этот параметр описывает, насколько принимаемый сигнал сильнее наводок NEXT или шума в кабеле. Иногда такой коэффициент называют соотношением сигнал-шум (SNR), но это название не совсем правильно. Следует помнить, что коэффициент отношения сигнала к шуму учитывает не только внутренние наводки, но интерференцию сигнала и шум от внешних источников.
- **Суммарная мощность ACR.** Точно так же, как и при подсчете суммарных наводок, если в многопарном кабеле для передачи сигнала используются все проводники, расчет параметра ACR становится сложнее. Чем большее количество проводников вовлечено в процесс передачи сигнала на физическом уровне, тем сложнее учесть их взаимное влияние; этот параметр позволяет учесть в расчетных уравнениях помехи и затухание в многопарном кабеле.
- **Равноуровневые наводки на дальнем конце кабеля (Equal-level far-end crosstalk — ELFEXT)** — это определенным образом измеренные наводки на приемном конце кабеля (иногда их связывают с однонаправленными сигналами). Если

величина этого параметра высока, то по кабелю невозможно передавать сигнал из-за высокого уровня шумов.

- **Суммарная мощность ELFEXT.** Точно так же, как и при расчете других интегральных параметров, этот коэффициент учитывает взаимодействие между многими парами в одном и том же кабеле, что значительно усложняет его расчет.
- **Коэффициент возвратных потерь (return loss).** Часть мощности сигнала, который передается по проводникам кабеля, отражается от неоднородностей среды, например, при несогласованности импеданса участков кабеля, переходников, разъемов и т.п. Энергия отражается в обратном направлении и может быть источником интерференции на ближнем конце кабеля.
- **Задержка распространения сигнала (Propagation Delay).** Электрические свойства кабеля влияют на скорость распространения сигнала в нем. Время распространения известно и давно измерено для разных материалов и широко используется во многих приборах, например, в динамических рефлектометрах (TDR). Задержка распространения сигнала обычно указывается в паспорте как максимально допустимый интервал времени (или задержки), измеряется в наносекундах.
- **Флуктуация задержки (Delay skew).** Поскольку каждая пара в кабеле может иметь различное количество витков, и оно для разных пар не одинаково, сигналы, которые на вход в кабель были поданы одновременно, на выходе уже не будут строго синхронизированы. Такое запаздывание или опережение одними сигналами других в смежных парах называют флуктуацией задержки. Проблема рассинхронизации сигналов в разных парах одного кабеля может быть усугублена неаккуратной запрессовкой кабеля в разъемы, например, если проводники асимметрично подключены к контактам разъема. И, наконец, разная величина задержки распространения сигнала в разных парах или проводниках кабеля может также привести к флуктуациям задержки сигнала в кабеле.

Тестирование соединений и каналов

В телекоммуникациях используются два вида тестов: тест соединения и тест канала. Тестирование канала происходит в сквозном режиме: от рабочей станции или телефона до устройства в телекоммуникационном узле. Канальный тест позволяет проверить абсолютно весь кабельный маршрут: соединительный кабель от оборудования телекоммуникационного узла до коммутационной панели, горизонтальный кабель, соединительный кабель от розетки до устройства или рабочей станции пользователя. Тестирование соединения подразумевает проверку только кабельного маршрута от настенной розетки до коммутационной панели. Существуют две разновидности тестов соединений: основной тест и тестирование постоянной части соединения. Когда выполняются основные тесты, предполагается, что нельзя подключать измерительную аппаратуру посредством дополнительных переходников и разъемов, поэтому характеристики среды измеряют непосредственно в гнездах

телеметрического оборудования. Тестирование постоянной части соединения также подразумевает, что оборудование для эксплуатационных испытаний не должно быть подключено посредством удлинителей, однако разъемы и стыковочные соединения сети учитываются и влияют на конечный результат (рис. А.48).

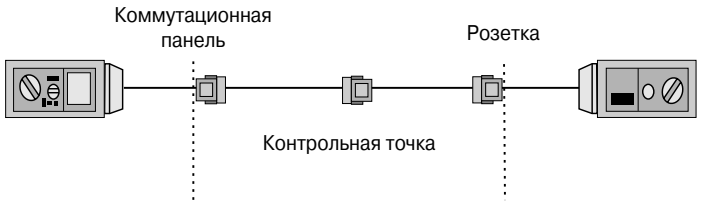


Рис. А.48. Тестирование постоянного канала

Для тестирования постоянных соединений в кабельной системе могут быть созданы специальные контрольные точки (иногда называемые объединительными), в которых участок кабеля может быть разорван для подключения измерительного оборудования.

На сегодняшний день стандарты предписывают использование только тестирования постоянных соединений. Канальный тест был официально исключен из стандартов, начиная со спецификации TIA/EIA-568-B.1.

Советы по сертификации сети

Правильная интерпретация результатов сертификации не менее важна, чем поиск и устранение неисправностей. Лучше всего учиться интерпретировать результаты тестов с использованием лабораторного оборудования совместно с известными наборами проводов, каналами, кабелями и электрическими цепями. Подобный подход позволяет монтажнику набрать необходимую базу знаний, научиться правильно использовать тестовое оборудование и привыкнуть к тому, как должны выглядеть результаты тестов в нормальных условиях, когда структура работает правильно.

Чтобы приобрести необходимый опыт поиска и устранения неисправностей, можно искусственно создать дефекты в кабеле и посмотреть, как кабельные тестеры реагируют на них. Далее следует попрактиковаться в обнаружении дефектов в случайно выбранных кабелях из такого набора. Стоит потратить какое-то время на совершенствование своих навыков, чтобы в практической работе уметь быстро находить и исправлять различные проблемы.

Профессиональная сертификационная документация

Большинство оборудования для сертификации кабеля позволяет экспортировать результаты исследований в формат какой-либо базы данных. Далее такие данные могут быть использованы для создания высококачественной документации с помощью обычного персонального компьютера (рис. А.49).

PASS	MAIN	SR	MAIN	SR
Worst Pair	36-45	36-45	36-45	12-45
ACR (dB)	18,2	71,7	15,2	16,5
Freq, (MHz)	214,5	3,5	250,0	248,0
Limit (dB)	8,2	61,8	4,8	4,8
Worst Pair	45	36	45	36
PSACR (dB)	16,0	13,2	13,0	13,2
Freq, (MHz)	250,0	240,0	248,5	250,0
Limit (dB)	5,7	2,0	2,2	2,0

PASS	MAIN	SR	MAIN	SR
Worst Pair	45	12	45	45
RL (dB)	17,4	26,0	17,4	20,2
Freq, (MHz)	244,0	7,3	244,0	174,0
Limit (dB)	10,1	21,0	10,1	11,5

Compliant Network Standards:

10BASE-T	100BASE-TX	100BASE-T4
1000BASE-T	ATM-25	ATM-51
ATM-155	100VG-AnyLan	TR-4
TR-16 Active	TR-16 Passive	

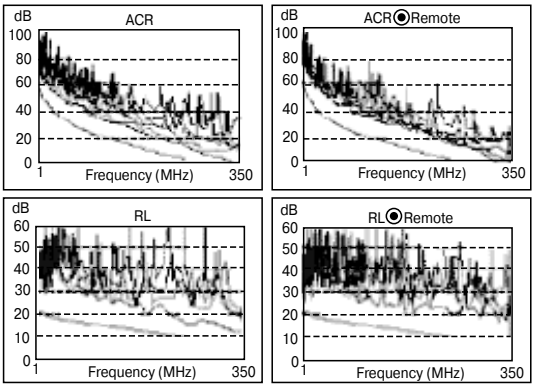


Рис. А.49. Сертификационная документация кабельной системы

Специализированное программное обеспечение, которое обычно поставляется с многофункциональными кабельными тестерами, позволяет подрядчику предоставлять результаты проверок в упорядоченном и презентабельном виде. Такие программные продукты облегчают жизнь специалиста по кабельной системе, поскольку результаты исследований не нужно вручную вносить в инженерные и офисные программы. Программное обеспечение сохраняет как положительный, так и отрицательный результаты тестирования. После того как дефекты в кабельной системе исправлены, результаты повторного тестирования перезаписываются на место старых и могут быть представлены заказчику. Обычно заказчик требует, чтобы ему предоставили как печатную, так и электронную копии результатов тестирования структурированной кабельной системы.

Чтобы документация приносила пользу, она должна быть легко доступна. Электронная копия документации прежде всего удобна тем, что к ней легко обеспечить доступ специалистам, которым это действительно нужно. Печатная документация хороша тем, что она является некоторым аналогом юридического документа, ее можно заверить нотариально и предоставить заказчику, а также использовать в качестве некоего эталона, который может понадобиться в будущем.

При сертификации структурированной кабельной системы результаты исследований обязательно должны быть сохранены, на их основании создается техническая документация изготовителя. Сертификационные документы могут помочь в решении некоторых разногласий с заказчиком в том случае, если возникнут проблемы либо вопросы, касающиеся качества или точности распайки и укладки кабеля. Такой набор документов может служить доказательством, что в некоторый момент времени в определенный день провода были размещены в определенном порядке и успешно справлялись с задачей передачи сигналов с определенным качеством. Если с течением времени в систему вносились какие-либо изменения, они могли повлиять на способность кабеля переносить сигналы, и этот факт может быть показан путем сравнения

результатов текущих тестов и результатов тестов, которые использовались для составления документации изготовителя.

Из-за неожиданно возникших обстоятельств, изменений в приказах, законах и требованиях заказчика, а также из-за желания заменить оборудование на другое в самый последний момент может возникнуть такая ситуация, когда начальная документация, которая была использована для построения кабельной системы, не совпадает с той, которая получится в результате. Получившаяся сеть также не будет совпадать с использовавшимся изначально проектом. Если кто-либо требует внести изменения в систему разводки кабелей, прежде всего следует оценить, как повлияют эти изменения на всю систему. В некоторых случаях вносимые изменения могут привести к непредсказуемому результату. Техническая документация изготовителя поможет избежать проблем такого рода. Рекомендуется прежде, чем вносить изменения в структурированную кабельную систему, задокументировать те изменения, которые будут вноситься в структуру.

Перекоммутация

Перекоммутацией, или переключением, называют как процесс демонтажа существующей кабельной инфраструктуры с целью установки новой, так и процесс установки нового оборудования в только что развернутую кабельную структуру.

Советы и рекомендации

Правильное переключение требует тщательного планирования, организации и огромного внимания к деталям. При переброске линий рекомендуется придерживаться следующих правил:

- следует вести ясную и четкую документацию для каждого проекта и записывать каждое действие. Поточные записи помогут убедиться в том, что все необходимые кабели установлены и размещены в нужных местах;
- каждый проложенный кабель необходимо тщательно проверить;
- обязательно нужно создавать и поддерживать в актуальном состоянии чертежи, схемы кабельной проводки, телекоммуникационной инфраструктуры, электрических цепей и схемы подключения. Базовая схема кабельной проводки обычно создается на основании требований и запросов заказчика сети;
- процедуру переключения следует запланировать на такое время, когда неудобства, причиняемые пользователям и заказчику, будут сведены к минимуму, поскольку переключение требует выключения и отключения от линий активного сетевого оборудования. Обычно все переключения проводятся вечером или ночью либо в выходные дни.

Демонтаж старого кабеля

Некоторое время назад, когда использовался старый электротехнический стандарт 2002 года, все старые кабели необходимо было демонтировать согласно текущим требованиям. На сегодняшний день удалять кабель или нет — это решение,

принимаемое совместно заказчиком сети и подрядчиком, который монтирует структурированную кабельную систему, и зависящее от стоимости работ по демонтажу и уничтожению устаревшей кабельной системы. Тем не менее, как заказчику, так и подрядчику, следует прежде всего проконсультироваться с местными инстанциями относительно того, какой вариант стандарта или требований используется в данной географической области. Перед тем как приступать к модификации кабельной системы, следует обсудить этот вопрос с заказчиком и включить необходимый пункт в договор на выполнение работ.

До начала демонтажа существующей кабельной системы нужно убедиться, что цепи и кабели отключены. Прежде всего следует выяснить это у заказчика, а потом проверить кабели с помощью мультиметра и телефонного тестера. При удалении старых кабелей соблюдайте осторожность: слишком активные действия и большие усилия могут повредить, например, подвесной потолок, кабелепроводы, распорки или даже привести к несчастным случаям.

Коммерческая деятельность в сфере построения СКС

Кабельный бизнес, как и любое другое дело, будь то мелкая розничная торговля или крупное предприятие, требует от работников определенной доли внимания и правильного отношения к делу. Прежде чем начнется установка кабельной системы, должен быть проведен тендер (как и на рынке, здесь можно поторговаться). Но перед объявлением тендера должен быть сделан коммерческий запрос и собраны коммерческие предложения, следовательно, нужно заранее проанализировать ситуацию, провести небольшую "рекогносцировку" и определить объем работ. Для выполнения работ могут потребоваться различные лицензии[33] и даже членство в каких-либо союзах или организациях. Все проекты следует выполнять согласно календарному плану, в крайнем случае, с минимальным отставанием, и без перерасхода материалов. Чтобы составить хороший план проведения работ и учесть все мелочи, зачастую специалисты используют специализированное программное обеспечение для планирования ресурсов и проектов.

При разработке проектов по установке кабеля следует учесть следующие пункты:

- обеспечение ресурсами (site survey);
- ситуацию с рабочей силой;
- правила и сроки пересмотра и подписания договора;
- методы планирования проекта;
- требования к конечной документации.

Как и в большинстве профессий, внешний вид и манера поведения сотрудников компании по установке кабеля сильно влияет на то, как компания (и сотрудники в частности) будет воспринята заказчиками, руководителями и коллегами по бизнесу.

[33] *Например, лицензия на право построения внешних и внутренних систем связи и коммуникации Госархстроя. — Прим. ред.*

От того, какие решения и как принимают сотрудники компании по монтажу кабеля, зависит их дальнейший карьерный рост. Выполняя свою работу, сотрудник компании представляет собой как бы лицо компании. Его внешний вид, поведение и моральные принципы обычно отражают отношение компании к работе. Если вы начинаете свою карьеру в качестве простого исполнителя, следует всегда поддерживать соответствующий уровень профессионализма, быть аккуратным в одежде и следить за своей манерой поведения.

При выполнении работ нужно выполнять простые рекомендации, они перечислены ниже.

- Уважайте свое рабочее место: содержите его в чистоте и порядке и постарайтесь исключить возможность несчастных случаев и повреждения оборудования и здания. Все инструменты следует убирать после того, как необходимость в них отпала или, по крайней мере, делать это в конце каждого рабочего дня.
- На работу следует приходить в чистой и хорошо выглаженной одежде.
- Неободимо приходить в оговоренное время, не опаздывая. Старайтесь всегда быть пунктуальными.
- Старайтесь не шуметь. Если замена и усовершенствование кабельной системы проходит без остановки других производственных процессов, не следует слушать музыку (особенно громко), свистеть, петь или кричать.
- К заказчику, его сотрудникам или жителям дома, коллегам и руководителям следует относиться с уважением.

Обеспечение ресурсами

Планирование ресурсов, или предварительный анализ потребностей, является одним из наиболее важных этапов перед началом оценки стоимости проекта. На данном этапе можно определить проблемы, с которыми придется столкнуться и которые могут существенно повлиять на проект. Схемы, рисунки и спецификации, предоставляемые заказчиком, не всегда достаточно ясны или подробны, чтобы сходу можно было определить суть проблем и осложнений, которые могут возникнуть в будущем.

Специалисты рекомендуют создавать “набросок” проекта в процессе разработки технического задания и оценки затрат на проект. Такой набросок позволит заранее выявить проблемные участки работ и предварительно оценить затраты времени на их проработку.

Перед тем как описывать требуемые ресурсы, следует ответить на следующие вопросы:

- есть ли в здании кабельные колодцы, подвесные потолки и другие пустоты?
- есть ли возможность разместить где-либо материалы на хранение и достаточно ли пространства для организации работ?
- есть ли какие-либо ограничения на время проведения работ?

- присутствуют ли специфические требования к безопасности (этот пункт особо важен при проведении работ на промышленных предприятиях)?
- где именно размещены противопожарные перегородки?
- есть ли в здании асбестовые конструкции?
- заменит ли заказчик плиты подвесного потолка в случае их повреждения?
- есть ли какие-либо специальные требования к процессу организации работ у заказчика?

Базовые документы проекта

Копии чертежей или архитектурных планов здания (blueprint), которые по сути своей являются уменьшенными чертежами, создаваемые архитекторами, позволяют получить информацию о требуемой длине кабеля и расстояниях между участками здания (рис. А.50). На планах здания обычно указывают также служебные точки и щиты, а также местоположение телекоммуникационных узлов и колодцев.

По схеме здания не всегда можно определить маршрут укладки кабеля, а также наличие кабелепроводов. Информация о кабельных маршрутах должна быть собрана в процессе расчета требуемых ресурсов. В большинстве структурированных кабельных сетей предполагается использование как минимум двух четырехпарных кабелей по каждому кабельному маршруту. Заказчик может захотеть проложить большее число резервных соединений; соответствующая информация должна быть включена в спецификацию проекта и в договор с подрядчиком.

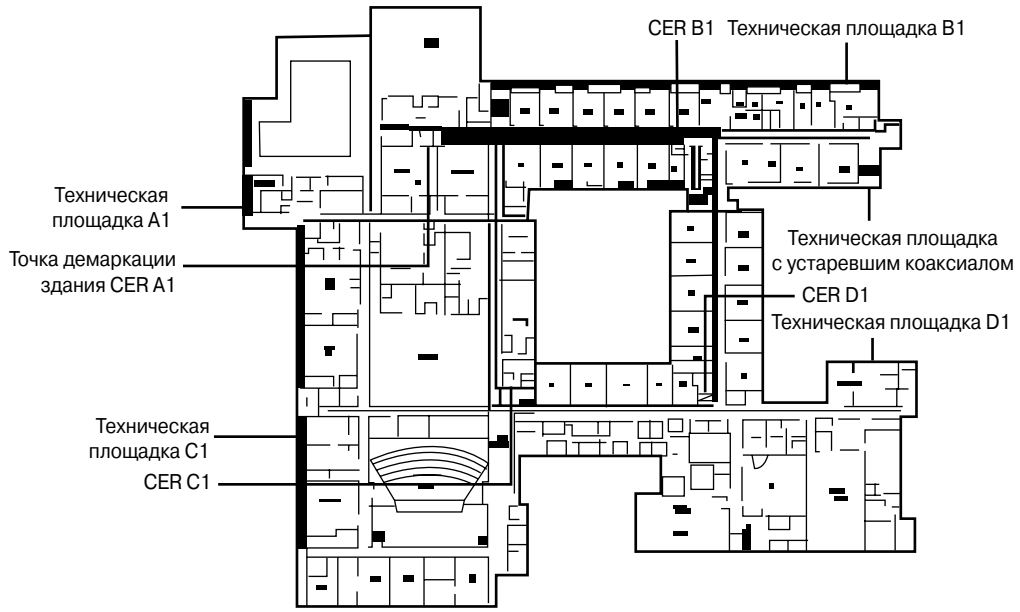


Рис. А.50. Типичная схема здания

Приблизительный подсчет нужного количества телекоммуникационных розеток и расчет длины кабелей по схеме здания — это всего лишь первый этап планирования проекта, далее можно поступить так: либо уточнить цифры на месте, либо предусмотреть некоторый запас материала. Приблизительный подсчет необходимо выполнять аккуратно, поскольку он позволяет оценить как требуемое количество материалов, так и трудозатраты, и использовать эту информацию для участия в тендере. Существует достаточно большое количество механических приспособлений и автоматизированных устройств, которые позволяют облегчить процесс подсчета и свести к минимуму погрешности и вероятность ошибки.

Специальные пиктограммы и символы

На план или чертеж здания наносят специальные стандартизированные пиктограммы и символы, которые схематически указывают кабельные маршруты, кабелепроводы разных типов, а также показывают размещение телекоммуникационных розеток, блоков и разъемов (рис. А.51). Такие пометки представляют собой универсальный метод графического изображения кабельной системы на чертеже здания.

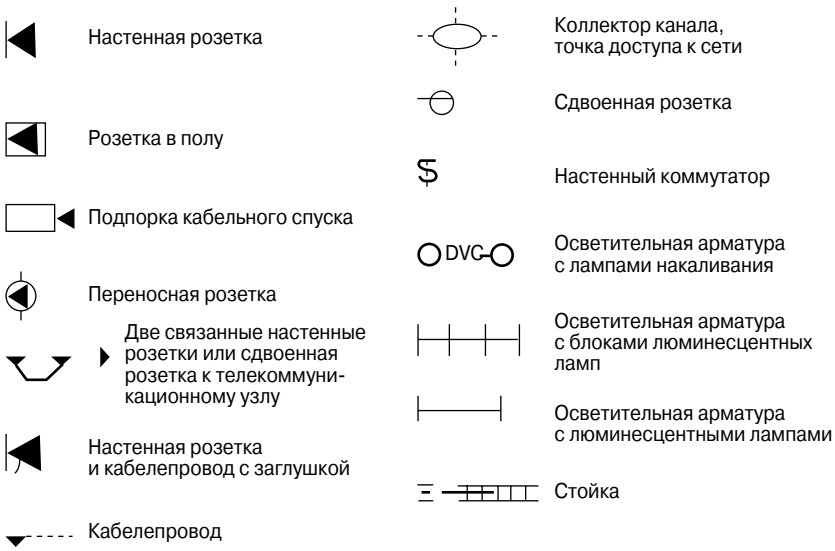


Рис. А.51. Универсальные кабельные пиктограммы

Схемы зданий

План-схемы и чертежи зданий всегда соответствуют некоторому стандартизированному формату. Схемы обычно группируются по определенным категориям. Схемы и чертежи маркируются символами или группами символов, по которым можно определить их принадлежность к определенной категории. Например, чертежи, которые относятся к системе электроснабжения здания или помещений, группируются вместе и маркируются буквой “E”; буквой “A” обозначают архитектурные планы;

схемы водоснабжения здания обозначают буквой "P"[34], и т.д. Схемы и чертежи телефонной проводки и каналов передачи данных группируют и маркируют буквой "T". Существует несколько типов чертежей категории T.

- **Схемы T0** представляют собой планы территориальных коммуникаций, они содержат внешние кабельные маршруты и магистрали между зданиями.
- **Схемы T1** содержат полные чертежи здания и каждого его этажа. В таких схемах указаны технические этажи и границы технических площадок, магистральные и горизонтальные кабелепроводы и кабельные маршруты.
- **Схемы T2** содержат описания технических этажей и площадок, на них обычно нанесены местоположения кабельных спусков и указаны метки кабелей.
- **Схемы T3** содержат чертежи и планы телекоммуникационных узлов, размещения монтажных стоек и настенного оборудования.
- **Схемы T4 —** это наиболее распространенные чертежи, на которых указано размещение противопожарных перегородок, местоположение розеток и их маркировка и нанесены точки размещения средств безопасности.
- **Схемы T5** обычно содержат схему коммутации кабеля и оборудования, таблицы оборудования и другую информацию, которая понадобится при перекоммутации соединений.

В документации могут также присутствовать другие схемы или чертежи, например, планы расстановки мебели. Такие планы обычно включаются в категорию "A" либо в раздел "другие схемы".

Среди документов, которые понадобятся для оценки затрат на проект и составление тендера, следует отметить следующие:

- общий план размещения объектов (site plan), который необходим для оценки проекта;
- планы каждого этажа здания;
- чертежи категории "T" (структура телефонной сети);
- чертежи категории "E" (структура сети электроснабжения);
- планы расстановки мебели, которые понадобятся для определения местоположения розеток;
- чертежи категории "A", которые понадобятся для определения будущих кабельных маршрутов.

Чертежи структуры сети должны содержать подробное описание проекта. Они могут также включать в себя описание функций установленной кабельной системы и ее особенностей. Например, на чертеже может быть фраза "система должна поддерживать 1000BASE-T", которая означает, что данный канал построен на основе технологии Gigabit Ethernet с использованием витой пары.

[34] *От английского* plumbing *— водопровод. — Прим. ред.*

Чертежи структурированной кабельной системы обычно содержат специфическую профессиональную терминологию, условные обозначения и сокращения, которые относятся именно к устанавливаемой инфраструктуре. Человек, которому приходится сталкиваться с такой документацией, должен хорошо разбираться во всех тонкостях специальной лексики. Следует отметить, что периодически издаются специализированные словари и справочники по сокращениям в кабельной промышленности, которые значительно облегчают жизнь как начинающему специалисту, так и опытным монтажникам. Необходимые сокращения и аббревиатуры можно всегда посмотреть на интерактивном Web-сайте Международной консультационной службы строительной промышленности (BICSI — Building Industry Consulting Service International, Inc)[35].

На основании чертежей структурированной кабельной системы можно определить базовые требования к системе и тип используемых материалов. Благодаря информации на таких чертежах, можно определить, сколько кабелей должно быть проложено к каждой телекоммуникационной розетке или разъему, а также требуемое количество самих розеток. В сопроводительных документах сети должны быть указаны спецификации и типы тестов кабелей, спецификации маркировки кабеля и формат меток.

Схематические наброски

Схематические наброски, в отличие от чертежей, выполняются без соблюдения масштаба. Они обычно используются для того, чтобы показать взаимное расположение объектов и указать соединения. Типичная схема содержит план соединений главного, промежуточного или любого другого телекоммуникационного узла, на ней обычно обозначены типы и размеры кабелей, а также длина кабелей между узлами. Следует отметить, что схемы телекоммуникационных узлов традиционно не содержат информацию о розетках, запрессовке кабелей, также не принято наносить на наброски отдельные кабели к розеткам, разъемам и телекоммуникационным блокам. На схемах принято изображать кабельные маршруты к стойкам с оборудованием, например, к серверным, коммутационным блокам и другим крупным телекоммуникационным компонентам проекта.

Трудозатраты и рабочая сила

Каждая компания-интегратор, которая занимается установкой кабельных систем, должна учитывать проблемы, связанные с рабочей силой. Некоторые проблемы могут быть связаны или вызвать недоразумения с профессиональными объединениями, например, с профсоюзами. Руководство компании должно знать правила и нормативы профессиональных организаций, их требования и методы лицензирования.

---

[35] *Формально ассоциация была зарегистрирована в 1977 году, хотя первые образовательные встречи были проведены еще в 1973 году в Университете Южной Флориды. — Прим. ред.*

Союзы

В некоторых проектах выдвигается требование, которое гласит, что работы должны выполнять рабочие, являющиеся членами профсоюза. Профсоюзы — это организации, которые представляют интересы работников. Чаще всего такое требование выдвигается для проектов сетей в новых зданиях, однако оно не является строгим правилом — даже при усовершенствовании существующей телекоммуникационной структуры, возможно, придется иметь дело с профсоюзами. Вопрос о том, будут ли устанавливать сеть рабочие, являющиеся членами профсоюза, или другие, должен быть оговорен при подписании контракта на выполнение работ. Если в договоре четко указано, что в проекте должны участвовать рабочие, которые состоят в профсоюзе, то такое требование обязательно должно быть выполнено во избежание юридических осложнений.

Дополнительные ограничения на выполняемые работы и рабочую силу связаны с реестром профессий и разрешениями на выполнение определенных работ. Согласно правилам профсоюзов, контролеры и руководители не имеют права заниматься установкой кабелей ни в коем случае. Аналогично монтажники не должны устанавливать коробы и кабелепроводы. В исключительных случаях монтажникам разрешено устанавливать кабелепроводы, но только определенного размера, определенной длины и в определенных условиях; все остальные коробы могут устанавливать только сертифицированные электрики, которые имеют разрешение на этот вид работ. Правила проведения работ утверждаются профсоюзами и зачастую определяются и согласовываются между разными профессиональными союзами, подобным образом происходит разделение сфер влияния и сфер ответственности.

Лицензии подрядчика

Во многих странах для проведения кабельных монтажных работ не требуется наличия специализированных лицензий у подрядчика. В США правила лицензирования подрядчиков отличаются в разных штатах, например, в некоторых штатах законы требуют, чтобы любой поставщик услуг или компания, которая что-либо производит, не только могли предоставить лицензию по требованию, но еще и печатали номер лицензии в объявлениях, на визитных карточках и официальных бланках организации. Компании, которые выполняют какие-либо работы или оказывают какие-либо услуги без лицензии, могут быть оштрафованы на довольно солидную сумму, потерять некоторые права, как, например, право накладывать арест на имущество заказчика в том случае, если он не рассчитается за выполненные работы.

Лицензии подрядчика или поставщика услуг могут включать в себя документы, которые подтверждают технические знания и возможности сотрудников подрядчика, коммерческие возможности компании и знание законов о труде данного государства или штата. К сфере ответственности подрядчика относится знание соответствующих законов и требований к лицензиям в данном штате или государстве.

Процедура согласования и подписания договора

После завершения переговоров с заказчиком зачастую возникает необходимость во внесении изменений в начальный вариант договора согласно требованиям и пожеланиям всех участвующих в проекте сторон. И заказчик, и подрядчик должны еще раз подробно рассмотреть и проанализировать договор. Согласование договора — это устное обсуждение его пунктов и положений, позволяющее убедиться в том, что стороны четко понимают друг друга; найденный консенсус должен быть задокументирован и оформлен юридически. Изменения и дополнения к договору, которые могут появиться в процессе выполнения работ, называются поправками к контракту. Поправки согласовываются и подписываются обеими сторонами, только в таком случае они имеют юридическую силу. Полномочные представители, имеющие соответствующие права (например, директора компаний или их заместители, обладающие правом юридической подписи), как со стороны заказчика, так и со стороны исполнителя, должны подписать договор; только после этого он из обычной бумаги превратится в юридический документ. Договор накладывает определенные обязательства на обе участвующие в нем стороны. До подписания договора не следует закупать какие-либо материалы или начинать проведение каких-либо работ.

Некоторые дополнительные документы можно заготовить заранее в виде некоторых шаблонов и согласовать их между участвующими в проекте сторонами, например, формат и бланк заявки на изменение (change order). Впоследствии такие бланки достаточно просто заполнить. Бланки можно даже подписать до начала проекта, например, в процессе уточнения требований к кабельной системе и рекогносцировки на местности, если уровень доверия между заказчиком и исполнителем достаточно высок.

Все изменения в проект после того, как начато выполнение работ, могут быть внесены только единственно правильным образом: с помощью письменных заявок на изменение. Никакие изменения в первоначальный проект на основании устных приказов вноситься не могут, для всех официальных действий необходимо использовать фирменные бланки или бланки заказа (order form), которые обычно хранятся у менеджера проекта. Заявки на изменение, которые предполагают выполнение дополнительных работ, должны содержать дополнительный счет об оплате труда и дополнительных материалов, если это приемлемо. Если счет-фактура не может быть включен непосредственно в заявку, в нее следует включить пункт, в котором должно быть указано, что заказчик согласен с изменениями и обязуется оплатить дополнительные расходы.

Планирование проекта

Фаза планирования проекта начинается после того, как выигран тендер, до формального подписания договора. Тендерную и оценочную информацию следует собрать вместе, проанализировать, отметить все требования, определить необходимые ресурсы и окончательно рассмотреть заявки на предложения (RFP — Request For Proposals); рассмотрение должно затронуть все аспекты и тонкости проекта.

Действия, которые рекомендуется предпринять при планировании проекта, можно разбить на следующие этапы:

Этап 1. Первое, что нужно сделать при планировании нового проекта, — выбрать ответственного за проект или менеджера.

Этап 2. Необходимо рассчитать трудозатраты и подобрать специалистов для выполнения проекта в зависимости от его масштаба. Следует рассчитать календарный план, определить, какие именно специалисты понадобятся, оценить требуемое для выполнения количество рабочих часов.

Этап 3. Необходимо решить, понадобится ли привлекать субподрядчиков, каких именно, и составить расписание.

Этап 4. Следует составить план и расписание поставок материалов.

Этап 5. На последнем этапе необходимо рассмотреть вопрос утилизации мусора, излишков материалов и отходов.

Поставщики

Специалист, который занимается оценкой проекта, обычно выбирает поставщиков на основании стоимости материалов, сроков поставки и качества обслуживания. Выбор поставщиков, как правило, осуществляется на основании общей стоимости материалов, которая определяется перечисленными ниже факторами.

- Входит ли в стоимость материалов стоимость доставки?
- Приходилось ли работать с данным поставщиком и посталяет ли он заказы в срок?
- Какова политика поставщика в отношении возвращенного товара?
- Сможет ли поставщик предоставить необходимые документы и чертежи своевременно?
- Может ли поставщик оказать техническую поддержку, предоставить рекомендации и посоветовать, какие товары выбрать?

Заказ материалов

После подписания договора необходимо оформить документы на поставку материалов. Заказ на поставку должен содержать описание материалов, серийные номера из каталогов производителей, количество материалов, стоимость, дату поставки и указывать, куда необходимо доставить заказ.

Обычно предприятия стараются выбрать поставщика, предлагающего оборудование и кабель по меньшим ценам, но достаточно известного и надежного. При оценке стоимости заказа следует также учесть стоимость доставки материалов. Поставщик должен гарантировать отсутствие изменений цен на весь период выполнения закупок. Стандартно практически любой поставщик гарантирует фиксированную цену в течение минимум тридцати дней. Менеджер проекта или представитель

заказчика должен проследить за тем, чтобы материалы не были заменены другими с целью уменьшения стоимости проекта.

Окончательная документация

Техническая документация изготовителя и чертежи, которые предоставляются заказчику при сдаче проекта, являются одной из наиболее важных частей завершающей фазы установки структурированной кабельной системы. На чертежах должны быть показаны кабельные маршруты, точки терминирования и типы кабелей, которые в действительности установлены. Зачастую под влиянием обстоятельств далеко не все кабели установлены так, как планировалось изначально, и не всегда именно того типа, который предполагалось установить. Обычно расхождения с изначально разрабатывавшимся проектом включают в себя измененные местоположения кабелей и розеток, измененные маршруты прокладки кабелей и добавленные или, наоборот, исключенные кабели и розетки. Чертежи технической документации дают заказчику информацию о той сети, которая была построена в действительности (рис. А.52).

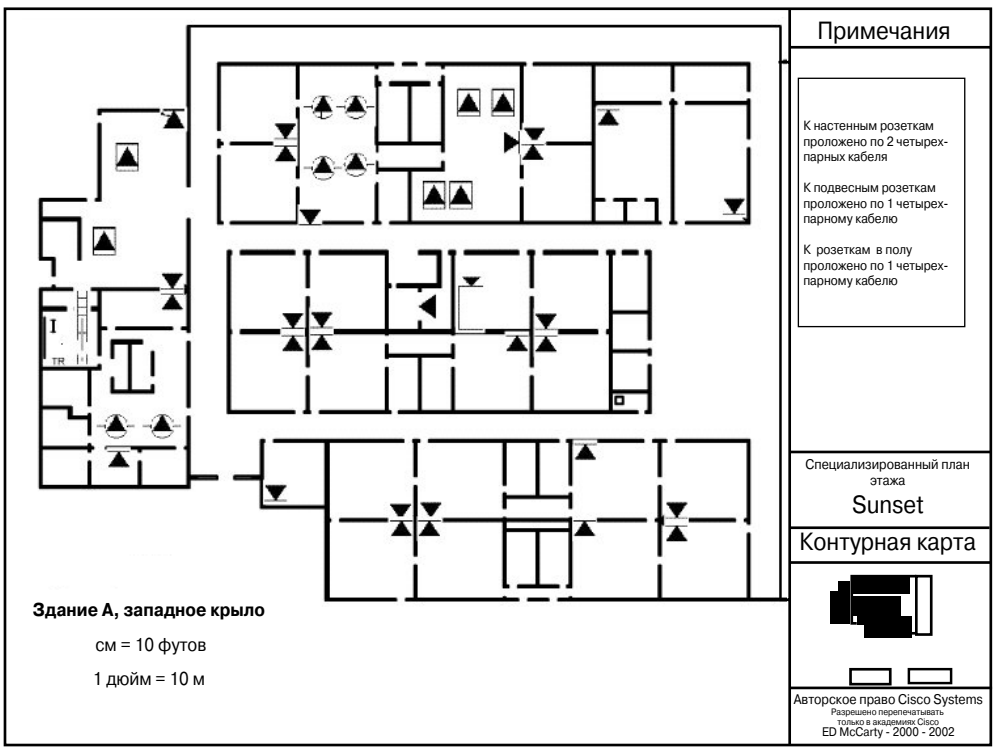


Рис. А.52. Техническая документация производителя

Чертежи создаются только после того, как проложены все кабели, установлены все разъемы и розетки и все кабели запрессованы. Рисовать чертежи можно уже в тот момент, когда начата финальная проверка сети, но при этом следует убедиться в том, что на этом этапе в сеть не были внесены какие-либо изменения или не были выполнены дополнительные работы, которые не отражены в документации. Чертежи этажей, план-схемы размещения мебели или чертежи категории "Т" служат основой для технической документации производителя.

Подрядчику не нужно перерисовывать планы и чертежи здания для того, чтобы создать документацию производителя; достаточно нарисовать кабельные маршруты, контрольные точки, розетки и нанести на схему все условные обозначения и метки установленных кабелей.

Перечень недоделок представляет собой контрольную таблицу, которую заказчик может предоставить подрядчику после завершения проекта (рис.А.53).

Список недоделок

В списке недоделок перечислены все пункты проекта, которые подрядчик должен исправить или завершить до уровня приемлемого заказчиком с тем чтобы могли быть подписаны акты о выполнении работ.

До того как будут подписаны акты и проведена оплата услуг, подрядчик и заказчик или архитектор здания должны выполнить последнюю беглую проверку установленной системы с тем, чтобы убедиться в том, что все недоделки и замечания были устранены.

Все участвующие в проекте стороны подписали соглашение, которое гласит, что когда будут устранены и исправлены недоделки, указанные в данном документе, проект считается завершенным. После завершения проекта заказчик обязуется перечислить все необходимые платежи на счет подрядчика.

Недоделки	Дата	Принято

Рис. А.53. Типичный перечень недоделок

Перечень недоделок — это список незавершенных пунктов проекта (например, отсутствующих розеток и кабелей), а также пунктов проекта, качество которых неудовлетворительно (кабелей, не закрепленных должным образом, неработающих розеток и т.п.), или не до конца убранных участков территории (осколки и мусор в коридоре), т.е. все, что необходимо доделать по требованию заказчика перед тем, как будет выплачена остаточная сумма за проект. Перечень недоделок может выполнять функции завершающего документа проекта. После того как все пункты такого списка выполнены, заказчик удовлетворен, проект закончен, клиент перечисляет последнюю из оговоренных сумм.

Практическое задание: проектирование и внедрение структурированной кабельной системы для компании FARB Software Development

Лабораторные работы дают возможность получить практический опыт построения структурированных кабельных систем. Практическое задание, которое приведено ниже, предназначено для того, чтобы попрактиковаться и поучаствовать в планировании и разработке кабельной сети для воображаемой компании, занимающейся разработкой программного обеспечения. Компания переезжает в новое трехэтажное здание, и для нее необходимо спланировать и развернуть кабельную систему.

Обзор задания

После окончания изучения текущего раздела специалист сможет:

- собрать информацию о компании и спланировать процесс развертывания структурированной кабельной системы;
- создать документацию, которая требуется для разработки настоящей сети;
- ознакомиться со стандартами TIA, EIA и правилами электротехнической безопасности.

Это приложение совместно с курсом CCNA версии 3.1 поможет как подготовиться к сдаче экзаменов, так и быть готовым к решению многих заданий, связанных с построением реальных сетей. Задачи дизайна сети, которую требуется создать, разъясняются в рамках данного учебного примера от лица Шерил Фарб (Cheryl Farb), директора компании FARB Software Development, Ltd. Читатель представляет подрядчика, а компания FARB Software Development выступает в качестве клиента вашей компании, занимающейся построением структурированных кабельных сетей.

Ниже приведены несколько обзорных разделов, которые содержат всю необходимую для выполнения практического задания информацию.

Общий план работ

Разрабатывать сеть рекомендуется согласно предложенному ниже подходу. Чтобы определить, как и где необходимо прокладывать кабели, нужно знать основные структуры разворачиваемых сетей. Необходимо предварительно установить, где будут размещены пользователи и какие им необходимы приложения, перед тем как делать схематический план будущей сети. Прежде всего необходимо разработать логическую и физическую топологию первого уровня сети. Первый этап включает в себя определение типов кабелей и физической топологии (т.е. распайки и разводки сети), а также физическое местоположение точек соединения узлов сети.

План сегментации сети на втором уровне следует выполнить с учетом разработанной топологии первого уровня. План второго уровня должен включать в себя устройства, которые добавляются в топологию сети, чтобы улучшить ее эффективность и функциональность. В качестве примеров подобных устройств можно

указать коммутаторы и мосты. Данный уровень также включает в себя технологии микросегментации, виртуальных сетей LAN (VLAN) и протокол распределенного связующего дерева (Spanning Tree Protocol — STP), которые помогут улучшить эффективность и надежность телекоммуникационной инфраструктуры.

Третий уровень иерархического плана перекрывает оба предшествующих уровня. Планирование этого уровня включает в себя выбор соответствующих устройств, которые обеспечивают функциональность внутренней и внешней сетей, а также структуру адресации устройств сети. Третий уровень связан с маршрутизацией, брандмауэрами и описывает логическую структуру сети передачи данных. В рамках этого уровня два указанных устройства также могут быть использованы для сегментации широковещательных и коллизионных доменов.

Для расширения плана третьего уровня может быть выполнен учет средств четвертого уровня. План четвертого уровня иерархически перекрывает структуры первых трех уровней; он более тесно, чем первые три уровня, связан с программным обеспечением и отвечает за контроль доступа и доступность сети, он связан со списками контроля доступа и конфигурацией брандмауэров. Несмотря на то что полный проект сети полностью привязан к эталонной модели OSI, обычно верхние уровни (начиная с пятого) находятся за пределами компетенции проектировщиков сети.

Это практическое задание сконцентрировано на технологиях Ethernet, IP и первых трех уровнях эталонной модели взаимодействия открытых сетей, которые являются основой как данной книги, так и одноименного учебного курса. Все основные структуры логически привязаны к уровням модели OSI.

В процессе разработки проекта следует помнить об одной из наиболее существенных конечных целей построения кабельной системы. Кабельная сеть должна быть рассчитана на изменение и расширение любой существующей службы. Многие компании хотели бы создать себе кабельную сеть, которая может существовать вечно, поскольку ее модернизация — занятие весьма утомительное. В таком случае следует с некоторыми оговорками придерживаться существующей структуры сети или предполагаемого профиля разрабатываемой инфраструктуры и учесть возможные в будущем изменения или реорганизацию компании. Правильно спроектированная структурированная кабельная сеть должна не только полностью соответствовать нуждам компании сегодня, но и предполагать возможность реорганизации согласно новым требованиям.

Документация — это очень важная и часто самая пренебрегаемая часть проекта по разработке и внедрению кабельной сети. Одна из самых важных тем текущего практического задания — как составить правильную документацию и собрать информацию при построении сети. Документация любого проекта должна содержать план-схему разводки проводов, схемы адресации, разные идеи мозгового штурма, матрицы решения проблем и всевозможные заметки, которые делаются в процессе выполнения задания.

Предварительный набросок проекта

Перед тем как сеть будет сконструирована, необходимо собрать данные, которые понадобятся в процессе выполнения проекта. Чтобы сеть работала с максимальной эффективностью и соответствовала потребностям пользователей, данные должны быть собраны в соответствии с некоторой методичной последовательностью, согласно стандартным, предварительно запланированным этапам. Выполнение всех этапов поможет собрать наиболее полные данные, которые в перспективе потребуются для построения сети. Самый первый этап любого проекта структурированной кабельной системы — сбор информации об организации. Полезная информация включает в себя:

- историю организации и ее текущее положение;
- предполагаемые темпы развития;
- рабочую стратегию и процедуры управления;
- чертежи и схемы зданий;
- диаграммы и документацию по существующей сети;
- офисные служебные системы и процедуры;
- блиц-опрос сотрудников компании, которые будут использовать локальную сеть.

В информационном блоке, который сопровождает эту часть, вы найдете письмо президента компании FARB Software Development, Ltd, в котором содержится вся необходимая начальная информация.В этом письме президент компании перечисляет некоторые специфические требования к рассматриваемому проекту.

Второй этап — детальный анализ и оценка текущих и намечающихся требований к разрабатываемой сети, собранных на первом этапе. Это необходимо для идентификации проблем, которые потребуется решить в процессе выполнения проекта (например, некоторые удаленные комнаты в здании не смогут иметь доступ к сети). В результате проработки второго этапа будет получена информация о возможном будущем росте размера сети, принципах доступа к ней и требуемому уровню безопасности.

Третий этап — идентификация ресурсов и ограничений организации, для которой разрабатывается сеть. Ресурсы организации, которые могут существенно влиять на внедрение новой локальной сети, могут относиться к категориям аппаратного и программного обеспечения, а также людским ресурсам. Если требуется расширить сеть или провести ее модернизацию, существующее компьютерное оборудование и программное обеспечение должны быть зарегистрированы, информация о них должна быть внесена в документацию. Идентификация и определение запланированных потребностей сети также должны быть проведены на данном этапе. Ответы на вопросы, приведенные ниже, помогут установить, какое количество персонала необходимо будет дополнительно обучить и сколько необходимо будет задействовать человек, чтобы поддерживать локальную сеть.

- Какими денежными ресурсами располагает организация?
- Какие ресурсы и каким образом в настоящее время взаимосвязаны друг с другом?
- Сколько сотрудников будут использовать сеть?
- Каков уровень компьютерной грамотности пользователей сети?
- Каково отношение персонала к компьютерам и компьютерным приложениям?

Выполнив указанные выше инструкции и задокументировав информацию в виде формального отчета, разработчик сети в дальнейшем сможет рассчитать стоимость и разработать бюджет проекта внедрения компьютерной сети.

Методология проекта и подбор комплектации

После ознакомления с материалами, которые были представлены в качестве сопровождающей документации, необходимо разработать концепцию и выработать общее представление о многоуровневой модели коммуникационной структуры. Используя модель OSI в качестве базиса и представляя себе основные функции сетевых устройств, которые обеспечивают работу соответствующих уровней, специалист может приступать к разработке структуры сети.

Для того чтобы выполнить это практическое задание, необходимо изучить материал, связанный с физической структурой сети и требованиями к ее установке. Как было указано выше, правила и стандарты регулируют и указывают, как именно должна быть разработана и построена сеть. Необходимо изучить как местные правила и стандарты, так и международные, перед тем как приступать к разработке проекта.

Завершив изучение текущего раздела, специалист должен уметь:

- разработать топологию первого и второго уровней;
- уметь собирать информацию для предварительной обработки и последующего использования в проекте;
- уметь создавать документацию в процессе выполнения проекта;
- овладеть стандартами TIA, EIA и знать правила электротехнической безопасности.

Следует отметить, что для разрабатываемого проекта и рассматриваемой компании характерны те же требования, что указаны выше.

Организации по стандартизации

При проектировании и построении сетей необходимо обеспечить соответствие проекта всем стандартам пожарной безопасности, правилам строительных организаций и стандартам безопасности, которые применимы в данном регионе. Возможно, наиболее важные части процесса построения и внедрения сети должны соответствовать промышленным стандартам EIA/TIA и ISO/IEC. Основное внимание как в этой книге, так и в одноименном курсе обучения уделено стандартам сетевой среды, которые разрабатываются и публикуются следующими группами и организациями:

- **ISO (International Organization for Standardization)** — Международной организацией по стандартизации (см. словарь терминов в конце главы);
- **IEEE (Institute of Electrical and Electronics Engineers)** — Институтом электрической и электронной инженерии;
- **UL (Underwriters Laboratories)** — Лабораторией по технике безопасности;
- **EIA (Electronics Industries Association)** — Ассоциацией электронной промышленности;
- **TIA (Telecommunications Industry Associastion)** — Ассоциацией промышленности средств связи.

Последние две организации совместно выпускают обширный список спецификаций, которые носят название TIA/EIA-стандартов. В дополнение к стандартам, разрабатываемым указанными организациями, местными, государственными, окружными и национальными правительственными организациями могут быть изданы спецификации и требования, которые могут влиять на тип кабеля, который необходимо использовать в локальной сети.

Следует четко представлять, что все стандарты регулярно пересматриваются и периодически обновляются, чтобы соответствовать новым технологиям и постоянно возрастающим требованиям к сетям телефонной связи и сетям передачи данных. Одновременно происходят два параллельных процесса: некоторые новые технологии добавляются к существующим стандартам, другие выходят из употребления, и их постепенно исключают из стандартов. Во многих случаях сеть может включать технологии, которые уже не являются частью действующих стандартов или находятся в процессе исключения из них. Обычно такая ситуация не требует немедленного изменения структуры, модернизации или перестройки сети, но старые и медленные технологии в итоге заменяются более быстрыми.

Выбор стандартов

Первичные стандарты, которые оказывают существенное влияние на общую структуру многоуровневой сети, относятся к группе TIA/EIA. Ассоциация промышленности средств связи (Telecommunications Industry Association — TIA) и Ассоциация электронной промышленности (Electronics Industries Association — EIA) — это две наиболее известные профессиональные ассоциации, которые совместно разрабатывают и издают серии стандартов для структурированных кабельных систем телефонных сетей и локальных сетей передачи данных. Промышленные стандарты начали активно развиваться в США после известного акта по прекращению регулирования телефонной индустрии в 1984 году, который "передал кабели в зданиях владельцам самих зданий". Ранее корпорация AT&T использовала собственные запатентованные кабели и системы.

Ассоциации TIA и EIA были аккредитованы Национальным институтом стандартизации США (American National Standards Institute — ANSI), раздел 6.2.7, для разработки любых промышленных стандартов для широкого круга телекоммуникационных продуктов. Многие стандарты были разработаны организациями ANSI/TIA/EIA

и содержат их метки в названии. Различные комитеты и подкомитеты ассоциаций TIA и EIA разработали стандарты для оптоволоконных кабелей, оборудования абонентов, сетевого оборудования, беспроводных коммуникаций (радиосвязи) и спутниковой связи.

Спецификация TIA/EIA 568-A представляет собой стандарт телекоммуникационной кабельной структуры офисного здания. Она описывает минимальные требования к кабельной системе, рекомендуемую топологию и ограничения по длине кабелей, указывает спецификации среды передачи данных и производительность каналов между сетевым аппаратным обеспечением, а также задает параметры используемых разъемов и правила их распайки. Этот стандарт постепенно вытесняется стандартом TIA/EIA 568-B.

Спецификация TIA/EIA 568-B представляет собой общий стандарт кабельной системы. В нем указаны компоненты и передаточные характеристики сетевой среды. В стандарте TIA/EIA 568-B.1 описана "обобщенная" кабельная телекоммуникационная структура офисного здания, которая способна взаимодействовать с различным оборудованием разных производителей. Стандарт TIA/EIA 568-B.1.1 является приложением, в котором описано применение восьмипроводной неэкранированной витой пары (Unshielded Twisted-Pair — UTP) и экранированной витой пары (Screened Twisted-Pair — ScTP), а также указаны радиусы изгиба соединительного кабеля обоих типов. В стандарте TIA/EIA 568-B.1.1 описаны компоненты кабельной системы, моделирование процессов передачи и кабельных систем, а также измерительные процедуры, которые используются для проверки кабелей. Спецификация TIA/EIA 568-B.2.1 является приложением, в котором перечислены требования к кабельным системам на основе витой пары категории 6. В стандарте TIA/EIA 568-B.3. описаны компоненты и передаточные функции оптоволоконных кабельных систем.

Спецификация TIA/EIA 569-A представляет собой стандарт, описывающий кабелепроводы и маршруты прокладки кабеля кабельной структуры офисного здания. В этом стандарте перечислены требования к оборудованию, описаны принципы дизайна и методы построения опорных структур для прокладки кабеля как внутри, так и за пределами зданий. Отдельные субстандарты описывают требуемые для установки в помещениях кабелепроводы и коробы для кабельных маршрутов, а также методы установки телекоммуникационного оборудования.

Спецификация TIA/EIA 606 представляет собой стандарт управления телекоммуникационной кабельной структурой офисного здания и содержит правила маркировки кабелей. Именно в этом стандарте указано, что каждая конечная точка или порт оборудования должны быть промаркированы уникальным идентификатором, а любой кабель должен быть промаркирован на обоих концах. Все метки должны соответствовать спецификации UL969, в которой описаны требования к их физическим характеристикам, удобочитаемости и т.п. В данном стандарте также перечислены требования к документации по сети и описано, как поддерживать записи в административных журналах в актуальном состоянии.

Спецификация TIA/EIA 607 является стандартом, который описывает правила заземления кабельных оболочек, или брони, кабельной системы офисного здания. Она учитывает особенности различных типов оборудования многих производителей, в

частности, указывает общепринятые методы безопасной установки устройств в серверной комнате потребителя. В этом стандарте четко описаны стандартные точки заземления в здании, конфигурации заземления телекоммуникационного оборудования и заданы требования к стандартной оснастке офиса, которые позволят обеспечить стабильную и безопасную работу сетевых устройств.

Дополнительная информация: стандарты TIA/EIA

Дополнительную информацию по различным стандартам и правилам TIA/EIA можно получить на Web-сайте `http://www.tiaonline.org`.

Правила электрической безопасности

Как правило, электрической ток проходит по пути с наименьшим сопротивлением. Поскольку такие металлы, как медь, имеют низкое сопротивление, они часто используются в качестве проводников электрического тока. Для многих материалов (стекла, резины, пластмассы) характерно высокое сопротивление, поэтому они не могут быть хорошими проводниками тока и часто используются в качестве изоляторов. Материалы с очень высоким сопротивлением используются для изоляции провода, обеспечивая защиту от протекающего по проводам тока, исключают искрение и возможность возникновения короткого замыкания.

Существует множество различных моделей электрических розеток. Два из трех штырей электротехнической вилки предназначены для подключения питания. Третий штырь защищает людей и оборудование от ударов током, коротких замыканий; его называют заземлением. В том электрооборудовании, где используется такой контакт, провода заземления соединены с какой-нибудь оголенной металлической деталью оборудования. Если внутри устройства произойдет поломка, заземление защитит людей от повышенного напряжения.

Случайное соприкосновение оголенных проводов, которые находятся под напряжением, и корпуса — это наиболее распространенный пример неисправности проводки в сетевых устройствах. Если возникла какая-либо неисправность (например, разрыв проводника), провода заземления, присоединенные к устройству, должны послужить маршрутом с низким сопротивлением, по которому разряд уйдет в землю. Защитное заземление обеспечивает меньшее сопротивление, чем человеческое тело, и риск получить удар током значительно снижается.

Когда оборудование правильно установлено, путь с низким сопротивлением, который создается посредством заземления, обеспечивает относительно слабое противодействие потоку электронов и свободное прохождение электрического тока, поэтому как опасное напряжение, так и паразитный статический заряд будут перетекать в землю. Цепь заземления обычно имеет непосредственный контакт с землей.

Требования к телекоммуникационным узлам

Разработка структуры первого уровня (эталонной модели) — это самый объемный компонент всего проекта структурированной кабельной системы. Она включает

в себя черновой набросок структуры сети на основе собранной заранее предварительной информации о сети и, собственно, в перспективе полноценную разработку структурированной кабельной системы. Структура первого уровня включает в себя разработку логической топологии, схем распайки и укладки кабеля, выбор местоположения кабельных узлов, подбор типа кабеля и многое другое. Разработанная структура должна полностью соответствовать стандартам и требованиям организаций по стандартизации.

После выполнения этого практического задания читатель должен уметь:

- составить список телекоммуникационных узлов и описать требования к ним;
- уметь объяснить, какие системы укладки кабеля будут использоваться, почему, указать их спецификации;
- перечислить и объяснить причины, почему выбраны монтажные шкафы определенного типа;
- объяснить ключевые моменты, которые связаны с требованиями к окружающей среде, безопасности и питанию в каком-либо телекоммуникационном проекте, а также пояснить, почему выбрано определенное местоположение для телекоммуникационных узлов, определенная структура сети и процесс установки.

Кабельная система рабочей области

К кабельной системе рабочей области относится все, что находится между настенной телекоммуникационной розеткой и рабочим местом пользователя. Такая система изначально разрабатывается исходя из того, что она должна быть максимально проста, чтобы было можно сравнительно легко ее переместить или изменить. Каждая рабочая область рассчитана на обслуживание максимум 10-ти м^2 свободного пространства пола.

Оборудование рабочей области включает в себя следующие компоненты:

- оборудование рабочих мест, такое, как персональные компьютеры, терминалы ввода данных, телефоны, факсимильные аппараты и принтеры;
- различные типы кабелей: соединительные, кабели для подключения модулей, кабели адаптеров персональных компьютеров, оптические соединительные кабели и перемычки;
- внешние адаптеры телекоммуникационных розеток.

В стандарте TIA/EIA-568-B указано, что требуется разместить как минимум две телекоммуникационные розетки в каждой рабочей области. Первая розетка должна быть подключена к четырехпарному кабелю неэкранированной витой пары (Unshielded Twisted Pair — UTP) или экранированной (Screened Twisted Pair — ScTP) с сопротивлением 100 Ом. Строго рекомендуется использовать кабель категории не ниже 5e для первой розетки в рабочей области. Для второй розетки нужно выбрать один из трех стандартных вариантов, описанных в спецификации:

- четырехпарный кабель с сопротивлением 100 Ом UTP или ScTP и соответствующий разъем (рекомендуется устанавливать категорию 5e);
- двужильное стекловолокно 62.5/125 мкм или 50/125 мкм и соответствующий разъем;
- 150-омную экранированную витую пару (Shielded Twisted-Pair — STP) и соответствующий разъем (для новых сетей не рекомендуется к использованию).

Сетевые приложения компании FARB

Чтобы оценить потоки трафика, которые будут проходить через сеть, необходимо очень хорошо представлять себе природу трафика, для которого предназначена сеть. Перемещение больших таблиц баз данных занимает большую часть пропускной способности инфраструктуры, как, впрочем, и интерактивные видеоконференции. Web-приложения, в отличие от двух указанных, достаточно терпимо относятся к пропускной способности каналов и не перегружают сеть, в качестве исключения можно указать только потоковые видео- и аудио-приложения.

Специалисты по информационным технологиям компании FARB подготовили список наиболее часто используемых в работе сетевых приложений. Приложения разделены на группы, для каждой группы характерно свое специфическое программное обеспечение.

Презентация: требования к сети программного обеспечения компании FARB
Дополнительная информация о компании FARB и требованиях программного обеспечения, а также соответствующий список можно найти на компакт-диске, предоставленном вместе с книгой, в разделе, посвященном практическим заданиям.

С чего следует начать

Как и большинство организаций, компания FARB не достигла такого высокого уровня внутреннего планирования, что для разработки проекта подрядчик может надеяться получить всю необходимую информацию: от точных схем размещения рабочих мест пользователей до точного указания местоположения разных отделов в здании. В лучшем случае компания может предоставить отвратительного качества некоторое количество схем и планов этажей, с них и придется начинать процесс разработки структурированной кабельной системы. Тем не менее, таких схем вполне достаточно для того, чтобы выбрать местоположение для основных и промежуточных телекоммуникационных узлов в рамках разрабатываемого проекта.

Презентация: дополнительные материалы и архитектурные планы
Необходимые схемы размещения мебели, планы водопроводно-канализационной сети, систем нагревания, вентиляции и кондиционирования воздуха, план-схемы комнат, структура телефонной сети, электропитания и освещения, пояснительные заметки и архитектурные схемы можно найти на компакт-диске, предоставленном вместе с книгой, в разделе, посвященном практическим заданиям.

Как обычно, на одной схеме может оказаться недостаточно информации о какой-либо части здания. Некоторые схемы могут и не пригодиться в процессе разработки проекта, поскольку не представляют ценности для проектировщика сети. Тем не менее, с ними следует на всякий случай ознакомиться, чтобы точнее разобраться в требованиях к сети рассматриваемой компании FARB.

Обратите внимание, что на схемах нигде не указано предположительное местоположение телекоммуникационных узлов, за исключением так называемой точки присутствия (Point of Presence — PoP), которая является входным узлом здания и расположена на первом этаже. Также на схемах не указано, где именно будут размещены разные отделы и подразделения компании. В действительности такую информацию следует получить у представителей компании, а в лабораторных условиях — у преподавателя или инструктора.

В следующих разделах представлены полезные советы, которые помогут и в практической работе в будущем, и будут полезны при выполнении текущего задания.

Полезные советы по созданию структурированной кабельной системы

В этом практическом задании необходимо попрактиковаться в умении разрабатывать сетевые и кабельные системы. В задании необходимо разработать сеть компании FARB Software Development. Достичь поставленной цели можно посредством выполнения нескольких задач в несколько этапов, которые сопровождаются дополнительным иллюстративным материалом.

Для разработки сети задействовано четыре типа документации разного уровня.

1. Техническое задание от президента компании, в котором описано его видение идеи телекоммуникационной инфраструктуры для нового здания компании FARB.
2. Документ с требованиями к сети, который был проработан сотрудниками отдела информационных технологий компании. Этот документ обязательно должен присутствовать в проекте.
3. Набор планов и схем каждого из четырех этажей здания.
4. Некоторое количество подробных схем и чертежей, которые помогут выбрать методы внедрения сети и основные используемые конструкции. Они также помогут принять решение о том, каким образом следует прокладывать кабель и как провести кабельные маршруты.

Не следует торопиться с выполнением текущего практического задания. Возможно, вы без подсказки обнаружите, что наиболее ценные результаты дает использование нескольких подходов, разработка разных стратегий. Следует обсудить спорные вопросы и разные идеи с коллегами, соучениками и преподавателями и принять решение о том, какая структура приемлема в данном случае.

План работы

Найдите и внимательно изучите техническое задание, которое вложено в письмо от президента компании для специалистов по информационным технологиям. В этом документе содержатся десять позиций, по которым следует дать достаточно развернутый комментарий. В конце письма приведен прогноз относительно будущего роста и развития компании.

Ниже перечислены основные элементы, которые следует развернуто описать (им соответствуют разные этапы разработки).

1. Необходимо выработать рекомендации по сетевому оборудованию.
2. Следует выработать рекомендации по кабельной системе.
3. Нужно определить основные требования к конструкции.
4. Требуется выбрать месторасположение сетевого оборудования.
5. Необходимо составить план разводки кабельной системы в здании, который включает в себя:
   - логическую структуру горизонтальной и вертикальной кабельных систем;
   - физическую структуру горизонтальной и вертикальной кабельных систем;
   - план-схему кабельной системы серверной комнаты;
   - месторасположение всех главных и промежуточных кабельных узлов;
   - план-схему идентификации телекоммуникационных кабельных розеток рабочих областей.
6. Необходимо выработать рекомендации по безопасности и предотвращению вторжений в серверную комнату, промежуточные и головные кабельные узлы.
7. Требуется предоставить рекомендации по электрической безопасности оборудования.
8. Следует разработать схему IP-адресации для всех сетевых устройств.
9. Нужно оценить затраты на разработку и внедрение сети, в том числе:
   - стоимость покупаемого оборудования;
   - стоимость прокладки кабеля и его тестирования;
   - стоимость установки оборудования;
   - стоимость обучения персонала и технической поддержки сети.
10. Следует согласовать календарный план для рассматриваемого проекта сети.

Ниже приводятся некоторые полезные советы и наводящие вопросы, которые помогут квалифицированно выполнить текущее практическое задание.

Наводящие вопросы и советы

Ответы на вопросы и комментарии к ним приведены в приложении Б, “Ответы на контрольные вопросы”

Начинать разработку проекта следует, что вполне очевидно, с изучения плана первого этажа.

Первый этаж

Изучите соответствующие материалы на компакт-диске и ответьте на следующие вопросы.

Что именно компания-заказчик предполагает разместить на первом этаже?

Какая из дверей будет использоваться для доставки грузов работниками?

Через какую дверь в здание будут входить посетители?

Куда предположительно будут направляться посетители после того, как зарегистрируются на входе?

Где предполагается и предполагается ли вообще использовать беспроводные технологии?

Если в один прекрасный день необходимо будет установить проводные камеры видеонаблюдения, которые используют средства IP, какие участки здания должны быть под наблюдением?

Где расположены точки обслуживания здания телефонной компании, которая предоставляет услуги связи?

Какие замки и средства защиты должны быть установлены на телекоммуникационные шкафчики?

Следует ли разместить серверы в точке присутствия провайдера (POP) службы?

Если необходимо разместить серверное оборудование отдельно от точки присутствия провайдера службы, исходя из каких соображений, следует выбирать месторасположение серверной комнаты?

Следует ли устанавливать стояки в точке присутствия?

Где следует разместить кабельные стояки в здании?

Горизонтальная кабельная система всегда должна быть расположена параллельно стенам. Какова будет длина кабельного маршрута в метрах к комнате 1.2 (см. сопроводительные материалы), если укладывать кабель параллельно стенам? Приемлема ли полученная величина?

Второй этаж

На втором этаже здания помещается множество кабинетов. Над этим этажом находится большая аудитория. Для аудитории может понадобиться установка беспроводных точек доступа и мостов, кроме того, ее наличие влияет на маршрут кабельной системы, поскольку аудитория имеет высоту более одного этажа. Где именно следует разместить телекоммуникационные узлы на втором этаже? (На этаже должно быть как минимум два таких узла.)

Третий этаж

На этом этаже есть неиспользуемое пространство в комнатах 3.1 и 3.2. Если разместить телекоммуникационный узел в комнате 3.10, можно ли будет установить сеть в указанных двух помещениях, в частности, в дальнем углу комнаты 3.2?

Четвертый этаж

На четвертом этаже есть также большое помещение и банкетный зал, в котором стоит пианино. Как можно обеспечить доступ к компьютерной сети в этом случае?

Где на четвертом этаже можно разместить телекоммуникационный узел или узлы?

После того как даны ответы на приведенные вопросы, можно приступать к разработке сети. Следует подсчитать количество рабочих мест (например, столов), которые будут обслуживаться каждым из телекоммуникационных узлов. Далее нужно умножить полученное число на два, поскольку для каждого рабочего места следует устанавливать две розетки, а затем разделить полученное число на 16 (число можно округлить). Результат покажет, сколько необходимо покупать 16-портовых коммутаторов для сети. Таким образом, первый пункт списка оборудования уже готов.

Для установки коммутаторов понадобятся монтажные шкафы. Для начала можно заказать по два таких шкафа в каждый телекоммуникационный узел.Необходимо также заказать коммутационные панели; их число должно соответствовать количеству кабельных соединений. Следует помнить, что в телекоммуникационных узлах придется разметить некоторое количество сетевого оборудования, такого, как маршрутизаторы и коммутаторы, и предусмотреть это в проекте. Чтобы расчеты были точными, аккуратными и без ошибок, рекомендуется воспользоваться программами табличных расчетов или электронными таблицами.

Установка кабельной системы сети

Итак, количество розеток для каждой рабочей области и каждого телекоммуникационного узла подсчитано. Для прокладки нужно использовать высококачественный кабель, например, категории 5e или выше. С помощью линейки начертите кабельные маршруты и измерьте расстояния. Сложите все полученные числа (длины кабельных сегментов), округлите до ближайшей тысячи, добавьте еще 1000

и разделите на 1000. В результате вы получите количество бобин кабеля, которое следует закупить[36].

Нужно укладывать кабель как можно более эффективно. Не следует экономить на бобинах или лениться использовать дополнительные катушки, также рекомендуется дублировать кабели. При прокладке нового кабеля в коробе, где уже установлена кабельная система, проложенный ранее кабель можно легко повредить.

Изменение конструкции здания

Исходя из требований проекта, необходимо установить кабельные стояки между этажами. Вполне очевидно, что в некоторых местах придется пробить потолок. Такая конструкция потребует использования жестких металлических коробов, поскольку нагрузка может быть высокой. Кроме того, возможно, придется перестроить несколько помещений на четвертом этаже, поскольку необходимо где-то разместить телекоммуникационные узлы.

Дальнейшие действия

Теперь, когда вы готовы к работе, можно выполнить все остальные пункты практического задания. Не торопитесь. Помните, что лучше семь раз отмерить, десять раз обсудить некоторые вопросы с коллегами, несколько раз ошибиться в бумажном проекте, чем начинать укладывать кабель заново. Как можно больше советуйтесь и дискутируйте, особенно на первых порах, возможно, в споре родится истина.

Резюме

Стандарты написаны таким образом, что строгое следование им позволяет добиться максимальной эффективности системы и наивысшей производительности. Если в процессе конструирования и установки какой-либо системы разработчики строго придерживались стандартов, система будет в определенной степени универсальна. Например, в современных инфраструктурах связи точка, через которую телекоммуникационные линии проникают в здание, практически всегда называется точкой входа. Точка, в которой происходит разделение ответственности и сферы влияния провайдера службы и пользователя на коммуникационные линии и оборудование, обычно называется точкой демаркации. Точка входа и точка демаркации стандартно размещаются в специально переоборудованном для этого помещении — телекоммуникационном, или коммутационном, узле. Телекоммуникационный узел может быть разного масштаба: главный коммутационный узел (Main Cross-connect — MC) предназначен для передачи сигналов одному и более промежуточным узлам (Intermediate Cross-connects — IC). Последние в свою очередь передают сигнал одному или более горизонтальным коммутационным узлам (Horizontal Cross-connects — HC), в задачу которых входит доставка сигналов непосредственно пользователям в так называемую рабочую область.

---

[36] *Здесь подразумевается, что расстояние измеряют в футах, поскольку кабель обычно выпускают в виде 1000-футовых бобин. 1 фут равен 30,48 см. — Прим. ред.*

Все работы необходимо выполнять с учетом определенных требований безопасности, чтобы избежать несчастных случаев, инцидентов и загрязнения окружающей среды. При выполнении работ рекомендуется по периметру рабочей области расставить предупреждающие знаки или дорожные метки, чтобы заранее предупредить прохожих о возможной опасности. При работе со стремянкой следует обратить особое внимание на безопасность работы с ней, убедитесь, что лестница находится в хорошем состоянии, ее ступеньки целы и крупных поломок нет. Приставную лестницу следует закрепить, если это возможно, недалеко от стены. Желательно также, чтобы кто-то из коллег страховал работающего и следил, чтобы кто-либо, входя в комнату, не сбил лестницу, открывая дверь. При работе на раздвижной стремянке следует убедиться в том, что она плотно прилегает к полу, а ее половинки максимально раздвинуты, закреплены, и лестница не сложится, как книга. Не используйте раздвижную лестницу в качестве приставной и никогда не взбирайтесь на самый ее верх. Установка кабельной системы и запрессовка разъемов требует специальных профессиональных инструментов, монтажники кабеля обычно хорошо с ними знакомы и не согласятся работать с некоторыми их заменителями. Так, например, инструмент для обрезки кабеля позволяет одним движением ровно обрезать кабель и снять с него изоляцию или прорезать ее на нужную глубину (которую можно отрегулировать), не повреждая проводники внутри, что значительно упрощает процесс установки разъемов. Запрессовочный инструмент используется для установки разъемов на заранее подготовленных концах кабеля. Такие основные инструменты должны входить в базовый набор любого монтажника, а для диагностики и тестирования кабелей понадобятся намного более сложные устройства.

Кабельный тестер позволяет убедиться в том, что каждая пара проводников подключена к нужным контактам и провода в разъеме не перепутаны. При установке кабельной системы не рекомендуется делать отверстия в противопожарных перегородках; если же этого не удается избежать, следует использовать специальные приспособления и материалы, для того чтобы восстановить функции перегородок. Специальных материалов существует великое множество, обычно это сертифицированные материалы, которые слабо воспламеняются и препятствуют распространению дыма и огня. В первой фазе развертывания кабельной системы монтажники выполняют укладку сегментов нужной длины, запрессовывают разъемы на концах, запрессовывают кабели в коммутационные панели и устанавливают настенные телекоммуникационные розетки. Последний этап любого проекта по созданию структурированной кабельной системы — это тестирование и сертификация. Сертификация заключается в проверке кабелей специализированными сигналами, с помощью которых специалисты определяют частотные характеристики системы, затухание на разных частотах и запас по характеристикам для развернутой кабельной системы. Результаты сертификации структурированной кабельной системы передаются владельцу здания и заказчику в составе документации на телекоммуникационную инфраструктуру.

Компаний по установке кабелей бы не существовало, если бы на их услуги не было спроса и периодически не объявлялись бы тендеры на разработку сети. Правильно составленный проект и тендерная документация требуют тщательного изучения требований и оценки возможностей и затрат. Различные правила и ограничения

профсоюзов, требования профессиональных организаций могут повлиять на общее время выполнения проекта, поэтому следует учесть их заранее. Некоторые внешние факторы (например, скорость поставки материалов) также сильно влияют на сроки выполнения проекта и календарный план.

Мы рассмотрели практическое задание по построению сети для некоторой фиктивной компании на основе документов, предоставленных президентом, и набора чертежей и схем здания. Основной задачей этого задания было научиться разрабатывать план действий, оценивать затраты и работать с имеющейся документацией.

Ключевые термины

Ассоциация промышленности средств связи (Telecommunications Industry Association — TIA) — организация, которая разрабатывает стандарты для телекоммуникационной промышленности.

Ассоциация электронной промышленности (Electronics Industries Association — EIA) — это группа разработчиков стандартов для электрических систем передачи сигналов. Ассоциации EIA и TIA разработали большое количество известных стандартов для передачи информации, таких, как широко известный стандарт TIA/EIA-232.

Главный коммутационный узел (Main Cross-connect — MC) представляет собой точку кабельной структуры, откуда монтажники прокладывают магистральный кабель. В коммутационном узле обычно размещено большинство активного оборудования сети. Такой узел, как правило, размещается в главных телекоммуникационных узлах или серверных.

Горизонтальный кабельный узел (Horizontal Cross-connect — HC) обеспечивает соединения между горизонтальной и магистральной кабельной системами для одного этажа или небольшого здания. В качестве такого узла может выступать полнофункциональный телекоммуникационный узел, монтажный шкаф, навесной настенный шкафчик, мини-шкафчик, размещаемый под фальшполом или над подвесным потолком.

Динамический рефлектометр (Time-Domain Reflectometer — TDR) — это устройство, которое передает импульс по проводам кабеля и принимает и интерпретирует отраженный сигнал (“эхо”), по которому устанавливает, есть ли в кабеле проблемы. Рефлектометр позволяет определить в кабеле дефекты и распознать их: короткое замыкание это или разрыв. Данное устройство позволяет установить не только наличие дефекта, но и определить расстояние до него.

Закон о технике безопасности и гигиене труда (Occupational Safety and Health Administration — OSHA). Организация OSHA отвечает за защиту работников и соблюдение законов о труде США и является подразделением Министерства охраны труда США. Она определяет правила безопасности и охраны труда, развития и сопровождения стандартов, проведения обучения персонала, поддерживает программы помощи неимущим и нуждающимся, обеспечивает взаимодействие между разными ведомствами и, в конечном итоге, отвечает за улучшение условий труда и усовершенствование техники безопасности на рабочем месте.

Инструментальный барабан представляет собой катушку большого диаметра, которая используется в механических кабелеукладчиках.

Кабелепровод — это канал, в котором размещены кабели. К кабелепроводам относятся как коробы систем питания, так и коробы сетей передачи данных различных типов: сплошные, декоративные, металлические, трубчатые и сетчатые, настенные и встроенные коробы и приспособления для укладки кабелей.

Кабельная подставка служит для размещения нескольких небольших бобин кабеля одновременно. Она позволяет монтажнику прокладывать по одному и тому же маршруту несколько сегментов кабеля одновременно.

Комитет CENELEC (European Committee for Electrotechnical Standardization — Европейский комитет по стандартизации электротехнических средств) — некоммерческая организация Бельгии. Ее основной задачей является разработка электротехнических стандартов Европы.

Коммутационная панель (patch panel) — это объединение определенного количества разъемов и портов, которое можно установить в монтажную стойку либо настенный шкаф в кабельном узле. Коммутационные панели выступают в роли пассивного коммутационного оборудования и используются для быстрого изменения топологии подключения устройств. Задняя стенка панели предназначена для подключения и фиксации кабелей, передняя стенка представляет собой промышленный блок контактных разъемов определенного типа.

Магистраль (backbone) — применительно к структурированной кабельной сети — кабельный маршрут между телекоммуникационными узлами или зданиями.

Магистральная, или вертикальная, кабельная система используется для подключения промежуточных и главных кабельных узлов, расположенных на разных этажах здания.

Многопортовые блоки розеток (Multiuser Telecommunications Outlet Assemblies — MUTOA) — это приспособление, которое за счет модульной структуры позволяет перемещать и добавлять устройства без дополнительной прокладки кабеля. В такие блоки обычно подключают компьютерное оборудование и телефоны.

Мультиметр — это прибор для тестирования электрических цепей, с его помощью можно убедиться, что напряжение в телекоммуникационной линии отсутствует. Большинство мультиметров позволяет измерить постоянное и переменное напряжение, ток, сопротивление, проверить целостность линии и работоспособность диода или транзистора.

Национальный институт стандартизации США (American National Standards Institute — ANSI) — это некоммерческая организация, в которую входят представители государственных ведомств, крупных корпораций и других организаций и которая координирует деятельность, связанную со стандартами. Она утверждает стандарты в США, разрабатывает позицию Штатов в международных организациях по стандартизации и дает рекомендации по применению международных стандартов внутри страны. Институт принимает участие в разработке как международных,

так и национальных стандартов, в частности, тех, которые относятся к телекоммуникациям и сетевым технологиям.

Перекрестные наводки (crosstalk) представляют собой помехи от сигнала в соседней паре кабеля. Уровень наводок тем выше, чем ближе к передатчику проводятся измерения.

Пленум (plenum) — ниша системы отопления, вентиляции или кондиционирования воздуха.

Промежуточный коммутационный узел (Intermediate Cross-connect — IC) — это узел, который подключен к главному и в котором размещено оборудование здания или территориальной сети. Он соединяет между собой магистраль и главные узлы с горизонтальными.

Рабочая область (work area) представляет собой часть помещения или офиса, в которой используется компьютерное, сетевое и телефонное оборудование.

Сборник национальных электротехнических нормативов (National Electrical Code — NEC) представляет собой собрание документов, регулирующих правила охраны населения и имущества от несчастных случаев, связанных с пользованием электричеством. Данная организация финансируется национальной Ассоциацией по пожарной безопасности (National Fire Protection Association — NFPA) и находится под протекцией Национального института по стандартизации США (American National Standards Institute — ANSI).

Серверная (серверная комната) — это помещение, в котором размещено оборудование. Зачастую такое помещение является также телекоммуникационным узлом.

Соединительный кабель (patch cord) представляет собой сегмент кабеля с разъемами на концах, который используется для подключения оборудования.

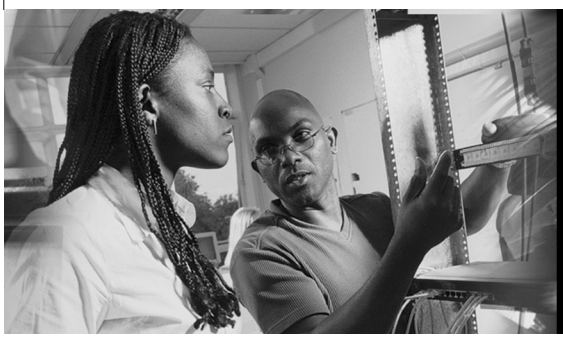
Справочник по безопасности материалов (Material Safety Data Sheet — MSDS) представляет собой набор документов, в которых содержится информация о правилах хранения, использования и перевозки опасных для здоровья материалов. В нем представлена подробная информация о том, какое влияние на здоровье человека окажет воздействие определенных веществ и материалов и как обезопасить себя при работе с ними.

Структурированная кабельная система, СКС (Structured Cabling System — SCS) — универсальная кабельная система, построенная в соответствии со стандартами, описывающими длину кабелей, типы кабелей и терминирующие устройства. Она представляет собой комплексный проект кабельной системы, в котором стандартизированы и сертифицированы все ее части: разъемы, схемы разводки и распайки контактов, центры распределения линий и методы установки кабеля.

Телекоммуникационный узел (Telecommunications Room — TR) представляет собой помещение или область в здании, где размещено телекоммуникационное оборудование и кабельное хозяйство.

Точкой демаркации, или демарком (demarc), называют узел, в котором кабель провайдера службы подключается к кабельной системе организации или здания.

Чертеж, или схема (blueprint) — это архитектурный план здания или технический рисунок, по которому можно выяснить особенности конструкции здания и схему размещения помещений, а также оценить необходимое количество кабеля и измерить расстояния.



ПРИЛОЖЕНИЕ Б

Ответы на контрольные вопросы

Ответы на контрольные вопросы главы 1

1. Г.
2. Б.
3. А.
4. Б.
5. Г.
6. В.
7. 1-а, 2-г, 3-б, 4-в. Бит — наименьшая единица данных в компьютере. Байт — единица измерения, описывающая объем файла данных, объем дискового пространства или другого носителя, объем данных, передаваемых по сети. Кбит/с — стандартная единица измерения скорости передачи данных в сети. МГц — единица измерения частоты; скорость изменения состояния или фазы звуковой волны, переменного тока или другого цикличного сигнала.
8. В.
9. Б.
10. В.
11. А.
12. А.
13. Г.

Ответы на контрольные вопросы главы 2

1. В.
2. В.
3. Б.
4. В.
5. Б.
6. А, Б и Г.

7. А.
8. В.
9. Г.
10. Б.
11. Б.
12. Б.
13. Б.
14. Г.
15. Г.
16. Б.
17. Б.
18. Г.
19. Б.
20. Б.
21. Г.
22. В.
23. Б.
24. В.
25. Г.

Ответы на контрольные вопросы главы 3

1. В.
2. Г.
3. Г.
4. Г.
5. В.
6. Б.
7. В.
8. В.
9. В.
10. Б и В.
11. А.
12. Г.

Ответы на контрольные вопросы главы 4

1. Г.
2. А.
3. А.
4. В, Д и Е.

Ответы на контрольные вопросы главы 5

1. В.
2. В.
3. В.
4. А.
5. Б.
6. Г.
7. Г.
8. Б.
9. Г.
10. А.
11. Б.
12. В.
13. Б.

Ответы на контрольные вопросы главы 6

1. Б.
2. Б.
3. Б.
4. Б.
5. В.
6. Б.
7. В.
8. А.
9. Г.
10. В.
11. А.
12. Б.
13. В.
14. В.

Ответы на контрольные вопросы главы 7

1. Б.
2. В.
3. В.
4. В.
5. В, Г.
6. Г.
7. В.
8. В.
9. А.
10. Г.

Ответы на контрольные вопросы главы 8

1. Г.
2. Б.
3. Г.
4. Коммутация с промежуточным хранением, сквозная и бесфрагментная.
5. Б.
6. Г.
7. В.
8. А, Б, Г.
9. А.
10. Б.
11. А.
12. В.
13. Б.

Ответы на контрольные вопросы главы 9

1. В.
2. Г.
3. Г.
4. В.
5. А.
6. Г.
7. А.
8. В.

9. Г.
10. Г.
11. А.
12. Б.
13. А.
14. А.
15. В.
16. Г.
17. Б.

Ответы на контрольные вопросы главы 10

1. Б.
2. Б.
3. А.
4. Б.
5. В.
6. А.
7. Г.
8. Б.
9. А.
10. Б.
11. Б.
12. Б.
13. В.
14. Б.
15. Г.
16. В.
17. В.
18. В.
19. Б.
20. А.
21. А.

Ответы на контрольные вопросы главы 11

1. А.
2. Б.

3. Г.
4. А.
5. А.
6. Б.
7. Г.
8. Г.
9. В.
10. В.
11. Б.
12. А.
13. Б, В.
14. В.
15. Б.
16. Г.
17. А.
18. Б.
19. А.
20. Г.
21. Б.
22. Г.
23. А.
24. А.

Ответы на контрольные вопросы главы 12

1. А.
2. А.
3. Б.
4. Г.
5. Г.
6. В.
7. Г.
8. Г.
9. Г.
10. Г.
11. Г.

12. Г.
13. В.
14. А.
15. Г.
16. А.
17. Г.
18. А.

Ответы на контрольные вопросы главы 13

1. Б.
2. В.
3. Д.
4. А.
5. А.
6. В.
7. Г, Ж.
8. А.
9. В.
10. Б.
11. А, Б.
12. Г.
13. Г.
14. А.
15. А.
16. Б.

Ответы на контрольные вопросы главы 14

1. Б.
2. В.
3. В.
4. А.
5. А.
6. Б.
7. Б.
8. Г.
9. Б.

10. А.
11. А.
12. А.
13. А.
14. А.
15. Б.

Ответы на контрольные вопросы главы 15

1. В.
2. А.
3. А, В.
4. Г.
5. А.
6. А.
7. Г.
8. А.
9. В.
10. А.
11. Г.

Ответы на контрольные вопросы главы 16

1. А.
2. В.
3. Б.
4. В.
5. Г.
6. Б.
7. В.
8. А.
9. Г.
10. Г.
11. А.
12. А.
13. Г.
14. Б.

Ответы на контрольные вопросы главы 17

1. В.
2. Б.
3. А.
4. А.
5. А.
6. А.
7. Г.
8. А.
9. А.
10. А.
11. Г.
12. В.

Ответы на контрольные вопросы главы 18

1. А.
2. Б.
3. А.
4. В.
5. Г.
6. Б.
7. Б.
8. В.
9. Б.
10. Г.
11. В.
12. В.
13. Б.

Ответы на контрольные вопросы главы 19

1. А.
2. Г.
3. А.
4. А.
5. Б.

Ответы на контрольные вопросы главы 20

1. А.
2. А.
3. А.
4. Б.
5. Б.
6. В.
7. Б.
8. В.
9. А.
10. А.
11. Б.
12. В.
13. А.
14. Г.
15. В.

Ответы на контрольные вопросы главы 21

1. А.
2. Б.
3. А.
4. Г.
5. Б.
6. А.
7. В.
8. Б.
9. Б.
10. В.

Ответы на контрольные вопросы главы 22

1. А.
2. Г.
3. В.
4. А.
5. Б.
6. В.

7. Г.
8. В.
9. Б.
10. А.
11. В.
12. Б.
13. Б.

Ответы на контрольные вопросы приложения А

1. Что именно компания-заказчик предполагает разместить на первом этаже?

   В этом помещении размещен склад и приемное отделение.

2. Какая из дверей будет использоваться для доставки грузов работниками?

   Рабочие доставляют грузы через большие двери тыльной стороны здания.

3. Через какую дверь в здание будут входить посетители?

   Посетители входят через парадный вход в вестибюль, в котором расположена приемная стойка.

4. Куда предположительно будут направляться посетители после того, как зарегистрируются на входе?

   После регистрации посетители, скорее всего, проходят в конференц-зал, примыкающий к приемному отделению.

5. Где предполагается и предполагается ли вообще использовать беспроводные технологии?

   С помощью беспроводных технологий посетители в приемном отделении и конференц-зале могут регистрироваться в сети Internet. Персонал склада может использовать беспроводные технологии для складского учета.

6. Если в один прекрасный день необходимо будет установить проводные камеры видеонаблюдения, которые используют средства IP, какие участки здания должны быть под наблюдением?

   Если возникнет необходимость в использовании камер, нужно будет установить наблюдение за двумя хранилищами, черным ходом и приемным отделением.

7. Где расположены точки обслуживания здания телефонной компании, которая предоставляет услуги связи?

   Телефонная компания обслуживает здание в точке, расположенной рядом с механической мастерской.

8. Какие замки и средства защиты должны быть установлены в точке обслуживания?

Точка обслуживания должна быть оснащена надежным замком, который позволяет открыть дверь изнутри.

9. Следует ли разместить серверы в точке присутствия провайдера (POP) службы?

Помещение точки присутствия может быть пригодно для размещения серверов, если оно достаточно велико и расположено близко к лестницам, что позволит легко попасть туда.

10. Если необходимо разместить серверное оборудование отдельно от точки присутствия провайдера службы, исходя из каких соображений, следует выбирать месторасположение серверной комнаты?

Если в проекте указано, что серверная должна быть размещена отдельно от точки присутствия, ее следует разместить в телекоммуникационном узле на одном из средних этажей.

11. Следует ли устанавливать стояки в точке присутствия?

Устанавливать стояки в точке присутствия нельзя. Над ней находится конференц-зал.

12. Где следует разместить кабельные стояки в здании?

Стояки можно установить в коридорах и на лестницах.

13. Горизонтальная кабельная система всегда должна быть расположена параллельно стенам. Какова будет длина кабельного маршрута в метрах к комнате 1.2 (см. сопроводительные материалы), если укладывать кабель параллельно стенам? Приемлема ли полученная величина?

Горизонтальные кабели должны проходить параллельно стенам. Если проводить их в помещение 1.2, расстояние по трассе составит около 94 м. Этого вполне достаточно, чтобы проложить магистраль, опустить кабель по стенам и включить его в разъем рабочей зоны. Проектировщик должен решить, прокладывать новый кабель или воспользоваться существующей беспроводной сетью, установленной для склада и конференц-зала. Это ослабит систему безопасности, но решит основную проблему.

14. На втором этаже здания помещается множество кабинетов. Над этим этажом находится большая аудитория. Для аудитории может понадобиться установка беспроводных точек доступа и мостов, кроме того, ее наличие влияет на маршрут кабельной системы, поскольку аудитория имеет высоту более одного этажа. Где именно следует разместить телекоммуникационные узлы на втором этаже? (На этаже должно быть как минимум два таких узла.)

Телекоммуникационный узел на втором этаже следует разместить в помещении 2.31, потому что через его потолок можно войти в помещение 3.10 этажом выше и в механическую мастерскую этажом ниже. Еще один узел может быть размещен в помещении 2.7.

15. На этом этаже есть неиспользуемое пространство в комнатах 3.1 и 3.2. Если разместить телекоммуникационный узел в комнате 3.10, можно ли будет установить сеть в указанных двух помещениях, в частности, в дальнем углу комнаты 3.2?

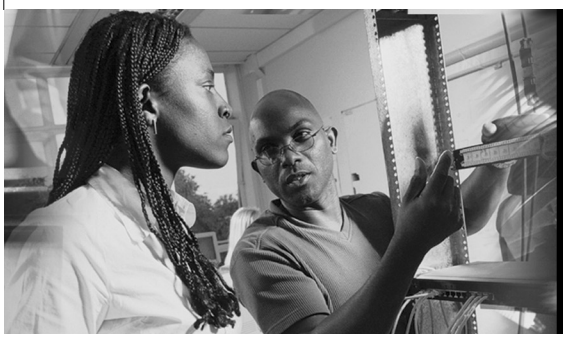
На сегодняшний день неплохим решением является беспроводная связь. При планировке этих помещений одно из них можно отвести под телекоммуникационный узел.

16. На четвертом этаже есть также большое помещение и банкетный зал, в котором стоит пианино. Как можно обеспечить доступ к компьютерной сети в этом случае?

На четвертом этаже расположен большая сцена и банкетный зал. Для обеспечения доступа к сети в нем может понадобиться только один телекоммуникационный узел и несколько беспроводных устройств.

17. Где на четвертом этаже можно разместить телекоммуникационный узел или узлы?

Разместить телекоммуникационный узел довольно сложно. Скорее всего, помещение 4.5 будет использовано под офис, а помещение 4.8 останется незанятым. Кроме того, рядом с лестницей по соседству с помещением 4.10 находится коридор с внешней дверью. Поскольку это четвертый этаж, такое решение может быть ошибочным. К тому же, дверь из помещения 4.10 открывается в лестничную шахту. Возможно, эти ошибки будут учтены и проектировщиком будет предложено установить узел-приемник между помещениями 4.4 и 4.5.



ПРИЛОЖЕНИЕ В

Словарь терминов

1000BASE-LX — спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи данных 1000 Мбит/с, в которой используются длинноволновой лазер и одномодовый оптический кабель. Максимальная длина сегмента составляет 10 000 м (32808,4 фута).

1000BASE-SX — спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи 1000 Мбит/с, в которой используется коротковолновой лазер и многомодовый оптический кабель. Максимальная длина сегмента составляет 550 м (1804,5 фута).

1000BASE-T — спецификация широкополосной технологии Gigabit Ethernet со скоростью передачи 1000 Мбит/с, в которой используются четыре пары UTP-кабеля категории 5 и максимальная длина сегмента составляет 100 м (328 футов).

100BASE-FX — спецификация узкополосной[1] технологии Fast Ethernet со скоростью передачи данных 100 Мбит/с, в которой используются два волокна многомодового оптического кабеля для соединений. Для нормальной синхронизации сигнала в 100BASE-FX соединение не должно превышать 400 м (1312 футов). Описывается стандартом IEEE 802.3.

100BASE-TX — спецификация узкополосной технологии Fast Ethernet со скоростью передачи данных 100 Мбит/с, в которой используется две пары кабеля UTP или STP. Первая пара используется для приема данных, вторая — для передачи. Для нормальной синхронизации сигнала в 100BASE-OX соединение не должно превышать 100 м (328 футов). Описывается стандартом IEEE 802.3.

10BASE2 — спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используется тонкий коаксиальный кабель с сопротивлением 50 Ом. Она является частью стандарта IEEE 802.3; ограничение на длину сегмента составляет 185 м (606 футов).

---

[1] *Способ передачи данных по кабелю, при котором каждый бит данных кодируется отдельным электрическим или световым импульсом; при этом весь кабель используется в качестве одного канала связи. — Прим. ред.*

10BASE5 — спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используется толстый коаксиальный кабель с сопротивлением 50 Ом. Она является частью стандарта IEEE 802.3; ограничение на длину сегмента составляет 500 м (1640 футов).

10BASE-T — спецификация узкополосной технологии Ethernet со скоростью передачи данных 10 Мбит/с, в которой используются две пары кабеля типа витая пара (категории 3, 4, 5): одна пара — для передачи данных, другая — для приема. Она является частью стандарта IEEE 802.3; максимальная длина сегмента равна 100 м (328 футов).

4D-PAM5 представляет собой метод символьного кодирования, используемый в технологии 1000BASE-T. Четырехмерные пятеричные (4D) символы, полученные при 8B1Q4-кодировании, передаются с использованием пяти уровней напряжения (PAM5). Четыре символа передаются параллельно в каждый период времени.

8B1Q4 — кодирование, которое описано в стандарте IEEE 802.3, представляет собой метод обработки данных, используемый в технологии 1000BASE-T при конвертировании GMII-данных в четыре пятеричных символа (Q4), передающиеся за один период (1Q4).

Cisco IOS (Internetwork Operating System, Cisco IOS — межсетевая операционная система корпорации Cisco). Программное обеспечение межсетевой операционной системы корпорации Cisco обеспечивает функциональность, расширяемость и безопасность всех аппаратных продуктов. Программное обеспечение хранится в виде образа во Flash-памяти, загружается в оперативную память устройства и обеспечивает его работу и выполнение всех необходимых функций.

DNS (Domain Name System) — система доменных имен. Система, используемая в сети Internet для трансляции имен узлов в сетевые адреса.

Flash-память (Flash memory) — специализированный тип памяти EEPROM (Electrically Erasable Programmable Read-Only Memory — электронно-перепрограммируемая постоянная память), содержимое которой может быть стерто и перепрограммировано заново блоками, в отличие от обычной побайтовой записи. Во многих современных персональных компьютерах BIOS-функции (Basic Input/Output System — базовая система ввода/вывода) хранятся во Flash-памяти, что позволяет при необходимости обновлять их. Такая микросхема BIOS иногда называется Flash-BIOS (Flash BIOS). Flash-память также широко используется в модемах, поскольку она позволяет производителям модемов поддерживать новые протоколы по мере того, как они становятся стандартами.

IEEE (Институт инженеров по электротехнике и электронике — Institute of Electrical and Electronic Engineers) — это профессиональная организация, деятельность которой включает в себя разработку коммуникационных и сетевых стандартов. Стандарты для LAN-сетей, разработанные Институтом IEEE, в настоящее время являются преобладающими при проектировании и эксплуатации сетей.

IP-адрес — это 32-битовый адрес, назначаемый узлу при использовании протокола TCP/IP. IP-адрес принадлежит одному из пяти классов (A, B, C, D или E) и записывается в виде четырех октетов, разделенных точками (такой формат называется точечно-десятичным). Каждый адрес состоит из номера сети, необязательного номера подсети и номера узла. Адреса сети и подсети совместно используются для маршрутизации, а адрес узла необходим для доставки информации определенному сетевому узлу внутри сети или подсети. Маска подсети используется для извлечения из IP-адреса информации о сети и подсети. Механизм бесклассовой междоменной маршрутизации (Classless InterDomain Routing — CIDR) предоставляет новый способ представления IP-адресов и маски подсети. Этот тип адреса часто называют *Internet-адресом*.

LLC (Logical Link Control — подуровень управления логическим каналом) — это верхний из двух подуровней канального уровня, определенных в стандарте IEEE. Подуровень LLC осуществляет контроль ошибок, управление потоками, созданием фреймов и адресацией на MAC-уровне. Основным протоколом LLC является спецификация IEEE 802.2, которая описывает как вариант сети с установкой соединения, так и без него.

MAC (Media Access Control — подуровень управления доступом к передающей среде) — это нижний из двух подуровней канального уровня, определенных спецификацией IEEE. MAC-подуровень управляет доступом к передающей среде, таким, как передача маркера или конкуренция за доступ. См. также *LLC*.

MAC-адрес — это стандартизованный адрес канального уровня, необходимый каждому устройству, подключенному к локальной сети. Все устройства используют MAC-адреса, чтобы найти определенные устройства в сети, а также для создания и обновления таблиц коммутации и структур данных. Длина MAC-адресов составляет 6 байтов, контролируются они Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers — IEEE). Этот тип адреса также называют *аппаратным адресом* (hardware address), *адресом MAC-уровня* (MAC-layer address) и *физическим адресом* (physical address).

NetBEUI (расширенный пользовательский интерфейс NetBIOS — NetBIOS Extended User Interface) — это усовершенствованная версия протокола NetBIOS, используемого такими операционными системами, как LAN Manager, LAN Server, Windows for Workgroups и Windows NT. NetBEUI формализует транспортные фреймы и добавляет дополнительные функции. Механизм NetBEUI реализует протокол LLC2 модели OSI.

NVRAM (NonVolatile RAM — энергонезависимая память) — оперативное запоминающее устройство, содержимое которого сохраняется при отключении питания.

OUI (Organizationally Unique Identifier — уникальный идентификатор организации) представляет собой три назначаемых Институтом IEEE октета в 48-битовом блоке MAC-адреса устройства.

ping (Packet Internet Groper — запросчик сети Internet) — команда, используемая для отправки эхо-запроса протокола ICMP и получения на него ответа. Часто используется в IP-сетях для проверки достижимости сетевого устройства.

RJ-45 — это разъем, которым обычно заканчивается кабель типа витой пары.

Telnet представляет собой стандартный протокол эмуляции терминала в стеке протоколов TCP/IP. Служба telnet применяется для удаленного соединения эмуляции терминала и позволяет пользователям входить в удаленные системы и пользоваться ресурсами точно так же, как в локальной системе. Описан в RFC 854.

Thinnet — термин, обозначающий более тонкий и менее дорогой коаксиальный кабель для стандарта 10BASE2.

TLV (Type Length Values — тип-длина-значение) — это блоки информации, внедренные в CDP-анонсы.

Traceroute — программа, которая прослеживает путь пакета до пункта назначения. Используется главным образом для отладки процесса маршрутизации между узлами. Существует также протокол отслеживания, определенный в RFC 1393. Эта программа присутствует во многих операционных системах.

Web-браузер. Клиентское приложение для отображения документов с гипертекстовой разметкой и обеспечения других служб, расположенных на удаленных Web-серверах в сети Internet, например, Internet Explorer и Netscape Navigator.

Автономная система — это отдельная сеть или набор сетей, находящихся под единым административным контролем, как, например, домен `Cisco.com`.

Административное расстояние (Administrative Distance — AD) — это величина, характеризующая надежность источника информации о маршрутизации. Эта величина выражается числом в диапазоне от 0 до 255. Чем больше ее значение, тем менее доверительна полученная информация.

Адрес подсети — это часть IP-адреса, задающая подсеть с помощью маски подсети.

Адрес управления доступом к среде передачи, или MAC-адрес (Media Access Control — MAC) — аппаратный адрес, уникальным образом идентифицирующий каждый узел сети. Используется для управления сеансами связи данного устройства.

Адреса класса A разработаны для поддержки очень больших сетей. В адресе этого класса используется только первый октет для описания адреса сети. Остальные три октета служат для указания адресов узлов.

Адреса класса B разработаны для поддержки больших и средних сетей. В адресе этого класса используются два октета из четырех для описания адреса сети. Остальные два служат для указания адресов узлов.

Адреса класса C — это наиболее широко используемый класс адресов. Данное адресное пространство предполагалось использовать для поддержки большого числа малых сетей.

Адреса класса D созданы для поддержки механизма многоадресатной рассылки.

Адреса класса E были зарезервированы проблемной группой проектирования Internet (Internet Engineering Task Force — IETF) для собственных исследовательских нужд. Таким образом, адреса этого класса никогда не были использованы в сети Internet.

Активный концентратор (active hub) — концентратор такого типа должен быть подключен к источнику питания (в настенную розетку), поскольку ему требуется питание для усиления входящего сигнала перед передачей его на другие порты.

Алгоритм выбора кратчайшего маршрута (Shortest Path First — SPF algorithm) — это выполняемые над базой данных вычисления, результатом которых является построение дерева SPF.

Алгоритм кодирования "без возврата к нулю с инверсией" (NRZI —nonreturn to zero inverted) — метод, который обеспечивает постоянный уровень напряжения при отсутствии данных (сигнал не возвращается к уровню 0 Вольт) для заданного битового интервала. В этом алгоритме наличие данных определяется по наличию изменения уровня сигнала в начале битового интервала, и об отсутствии данных свидетельствует отсутствие изменений в сигнале.

Алгоритм кодирования "без возврата к нулю" (NRZ — nonreturn to zero) — метод, который обеспечивает постоянный уровень напряжения при отсутствии данных (сигнал не возвращается к уровню 0 Вольт) для заданного битового интервала.

Алгоритм представляет собой четко заданные правила или процесс решения определенной проблемы. В области сетевых технологий алгоритмы в основном используются для определения наилучшего маршрута потока данных от конкретного отправителя к заданному получателю.

AM (амплитудная модуляция) — процесс изменения высоты (амплитуды) несущей волны.

Американский стандартный код обмена информацией (American standard code for information interchange — ASCII). Наиболее распространенный код для представления буквенно-цифровых данных в компьютере, в котором используются двоичные числа для представления символов, набранных на клавиатуре.

Амплитуда (amplitude) электрического сигнала представляет его высоту, однако измеряется не в метрах, а в вольтах.

Анализатор спектра (spectrum analyzer) — электронное устройство, вычерчивающее графики зависимости различных величин от частоты. В инженерной практике используется для анализа спектра (т.е. составляющих) различных сигналов.

Аналоговая полоса пропускания (analog bandwidth) — этот термин обычно применяется по отношению к диапазону частот аналоговой электронной системы. Термин может также использоваться для описания диапазона частот, передаваемых радиостанцией или электронным усилителем.

Анонсы маршрутизации (routing update) — это сообщения, рассылаемые между маршрутизаторами объединенной сети, в которых содержится информация о достижимости сети и соответствующая оценка маршрута. Обновления маршрутизации обычно рассылаются с постоянными интервалами, а также в случае изменений в сетевой топологии. *Ср. с мгновенными изменениями (flash update).*

Ассоциация промышленности средств связи (Telecommunications Industry Association — TIA) — организация, которая разрабатывает стандарты для телекоммуникационной промышленности.

Ассоциация электронной промышленности (Electronics Industries Association — EIA) — это группа разработчиков стандартов для электрических систем передачи сигналов. Ассоциации EIA и TIA разработали большое количество известных стандартов для передачи информации, таких, как широко известный стандарт TIA/EIA-232.

Байт. Единица измерения, которая служит для описания размеров файлов данных, размера места на диске или другом носителе информации, для описания количества данных, переданных через сеть. 1 байт равен 8 битам.

Белый шум (white noise) — это шум, в равной степени затрагивающий все частоты передачи.

Бесклассовая междоменная маршрутизация (Classless InterDomain Routing — CIDR) — технология, поддерживаемая протоколом BGP (и многими другими) и основанная на агрегации маршрутов. Маршрутизация CIDR позволяет маршрутизаторам группировать маршруты, сокращая таким образом объем маршрутной информации, хранящейся в базовых маршрутизаторах. Благодаря использованию механизма CIDR несколько сетей могут быть сгруппированы и выступают в виде одного более крупного блока, который выглядит как единое целое для остальных сетей.

Бит. Наименьшая единица данных в компьютере. Бит принимает значение 1 или 0 и является цифрой двоичного формата данных, который используется компьютером для хранения, передачи и обработки данных. В компьютере таким цифрам соответствуют положения переключателей (включен/выключен) или наличие/отсутствие электрического сигнала, светового импульса или радиоволн.

Битовая корзина (bit bucket) используется для уничтожения отброшенных (или уничтоженных) маршрутизатором пакетов.

Блок питания. Блок, который обеспечивает электрическое питание компьютера.

Брандмауэр (firewall) — одно или более сетевых устройств, таких, как маршрутизаторы или серверы доступа, предназначенных для создания буферной зоны между соединенными открытыми и частными сетями. Для обеспечения безопасности частных сетей в брандмауэре используются списки управления доступом и другие методы.

Булева логика. В компьютерных операциях с двоичными значениями с помощью булевой логики вычисляются состояния электрических цепей (замкнутая или разомкнутая цепь) или электромагнитных состояний (наличие или отсутствие заряда). Компьютеры используют логические элементы "И" и "ИЛИ" для сравнения двух двоичных элементов, полученный результат используется для дальнейших вычислений.

Видеоплата, или видеокарта. Плата, устанавливаемая в компьютер, которая обеспечивает вывод графической информации.

Виртуальная частная сеть (Virtual Private Network — VPN) — частная сеть, создаваемая в открытой сетевой инфраструктуре, такой, например, как глобальная сеть Internet.

Внешние маршруты (exterior routes) представляют собой маршруты, ведущие к узлам, расположенным вне данной автономной системы и рассматриваемые в качестве возможного стандартного шлюза.

Внешние наводки (alien crosstalk) — наводки, вызываемые сигналами, проходящими вне кабеля.

Внешний маршрутизатор (exterior router) — в структуре брандмауэра это маршрутизатор, который подсоединен к сети Internet. Он перенаправляет все входящие пакеты на программный шлюз для их дальнейшей обработки и анализа.

Внешняя сеть (Extranet) — основанные на внутренней сети (Intranet) приложения и службы, позволяющие получать расширенный безопасный доступ к внутренней сети предприятия внешним пользователям или предприятиям.

Внутренние маршруты (interior routes) — это маршруты между подсетями некоторой сети, подсоединенной к интерфейсу маршрутизатора. Если подсоединенная к маршрутизатору сеть не имеет подсетей, то внутренние маршруты протоколом IGRP не анонсируются.

Внутренний маршрутизатор (interior router) — это маршрутизатор, который подсоединен ко внутренней сети. Внутренний маршрутизатор разрешает трафик только от программного шлюза. Шлюз контролирует сетевые потоки данных в обоих направлениях: как из внешней сети во внутреннюю, так и из внутренней наружу.

Внутренняя сеть (Intranet) — обычная конфигурация локальной сети LAN. Intranet-сети предназначены для того, чтобы к ним получали доступ только пользователи, имеющие привилегированный доступ к внутренней локальной сети предприятия.

Возврат (backoff) — задержка повторной передачи, вызванная произошедшей коллизией.

Волна (wave) представляет собой перемещение энергии из одного места в другое.

Время безотказной работы (uptime) — это промежуток времени, в течение которого сетевое устройство исправно функционировало и обрабатывало запросы пользователей.

Входные потери (insertion loss) представляют собой сочетание эффектов ослабления сигнала и разрывов импеданса в канале связи.

Герц (hertz) — единица измерения частоты электрического сигнала, отражающая количество полных циклов в секунду.

Гигабайт (ГБ). Приблизительно равен 1 миллиарду байтов. Иногда используется название "гиг". Емкость накопителей на жестких дисках в большинстве современных персональных компьютеров измеряется в гигабайтах.

Гигабиты в секунду (Гбит/с). Один миллиард битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Технология 10G Ethernet работает со скоростью 10 Гбит/с.

Гиперссылка. Управляющая команда, по которой осуществляется переход на другие HTML-файлы на Web-сервере или определенные точки в том же документе. Предоставляет ускоренную навигацию по документам.

Главный коммутационный узел (Main Cross-connect — MC) представляет собой точку кабельной структуры, откуда монтажники прокладывают магистральный кабель. В коммутационном узле обычно размещено большинство активного оборудования сети. Такой узел, как правило, размещается в главных телекоммуникационных узлах или серверных.

Горизонтальный кабельный узел (Horizontal Cross-connect — HC) обеспечивает соединения между горизонтальной и магистральной кабельной системами для одного этажа или небольшого здания. В качестве такого узла может выступать полнофункциональный телекоммуникационный узел, монтажный шкаф, навесной настенный шкафчик, мини-шкафчик, размещаемый под фальшполом или над подвесным потолком.

Граничный маршрутизатор (border router) — устройство, размещенное на границе сети и обеспечивающее функции защиты некоторой частной области сети от внешних сетей или от слабо контролируемых областей сети.

Двоичная система счисления. Система счисления с использованием цифр 0 и 1, которые в компьютерах соответствуют двум состояниям электрической цепи (разомкнутая и замкнутая).

Дейтаграмма (datagram) — логично связанный блок информации, передаваемой в сетевой среде в качестве модуля передачи сетевого уровня без предварительной установки виртуального соединения. IP-дейтаграммы являются основной единицей информации в сети Internet. Термины *ячейка*, *фрейм*, *сообщение*, *пакет* и *сегмент* также описывают способы логической группировки информации на разных уровнях модели OSI и разных технологических циклах.

Декапсуляция (de-encapsulation) — освобождение данных от заголовка конкретного протокола.

Децибел (decibel) — важный способ описания сетевых сигналов в единицах, отражающих уменьшение или увеличение энергии электромагнитной волны. Значение в децибелах обычно отрицательно, поскольку оно отражает потерю энергии по мере прохождения волны, однако оно может быть и положительным, отражая увеличение энергии сигнала, если он усиливается.

Динамическая маршрутизация (dynamic routing) представляет собой разновидность маршрутизации, в которой автоматически учитываются изменения сетевой топологии и характера потоков данных. Также называется адаптивной маршрутизацией. Для осуществления такой маршрутизации между маршрутизаторами должен функционировать протокол маршрутизации.

Динамический рефлектометр (Time-Domain Reflectometer — TDR) — это устройство, которое передает импульс по проводам кабеля и принимает и интерпретирует отраженный сигнал ("эхо"), по которому устанавливает, есть ли в кабеле проблемы. Рефлектометр позволяет определить в кабеле дефекты и распознать их: короткое замыкание это или разрыв. Данное устройство позволяет установить не только наличие дефекта, но и определить расстояние до него.

Дисперсия мод — при распространении по оптическому волокну нескольких мод, в зависимости от угла попадания лучей в оптическое волокно, эти лучи проходят различные расстояния, достигая точки назначения (принимающий конец оптического волокна) с небольшой разницей во времени.

Дисперсия — это расширение ("расплывание") светового импульса при прохождении по оптическому волокну.

Дистанционно-векторная маршрутизация представляет собой класс алгоритмов маршрутизации с последовательным подсчетом транзитных переходов пакета между маршрутизаторами на пути следования для расчета связующего дерева кратчайшего пути. Механизм обновления таблиц маршрутизации "дистанционно-векторный алгоритм" требует от каждого маршрутизатора из числа своих непосредственных соседей выслать свои полные таблицы маршрутизации. При использовании данного алгоритма маршрутизации возможно возникновение кольцевых маршрутов, однако механизм расчета маршрутов проще, чем у алгоритмов маршрутизации по состоянию канала. Этот тип маршрутизации основан на алгоритме Беллмана-Форда (Bellman-Ford).

Дистанционно-векторный протокол маршрутизации (distance vector routing protocol) относится к классу алгоритмов маршрутизации, последовательно анализирующих переходы на маршруте для построения связующего дерева кратчайшего пути. В дистанционно-векторных протоколах требуется, чтобы каждый маршрутизатор при каждом обновлении маршрутизации рассылал полностью свою таблицу маршрутизации, но только своим соседям. Алгоритмы дистанционно-векторной маршрутизации подвержены проблеме образования кольцевых маршрутов, однако в вычислительном отношении они проще алгоритмов маршрутизации по состоянию канала. Такие алгоритмы также называются алгоритмами маршрутизации Беллмана-Форда (Bellman-Ford).

Длина волны — расстояние от одной точки одной волны до соответствующей точки следующей (соседней) волны. Длина волны света обычно измеряется в нанометрах (нм).

Домен коллизий (collision domain): в сетях Ethernet — область сети, в которой распространяются столкнувшиеся и поврежденные фреймы. Повторители и концентраторы не отфильтровывают такие поврежденные фреймы, в то время как коммутаторы локальных сетей LAN, мосты и маршрутизаторы их не пропускают.

Домен коллизий — область сети Ethernet, внутри которой распространяются сталкивающиеся фреймы. Концентраторы и повторители пропускают коллизии, коммутаторы локальных сетей, мосты и маршрутизаторы — нет.

Дочерняя плата (daughter card) подобна платам расширения, однако получает доступ непосредственно к компонентам маршрутизатора (памяти и центральному процессору) вместо использования медленной шины расширения.

Дуплексная передача (full duplex) — это возможность одновременной передачи данных между отправляющей и принимающей станциями в двух направлениях.

Заголовок (header) — управляющая информация, размещаемая перед модулем передачи верхнего уровня при инкапсуляции данных для передачи по сети.

Задержка распространения (propagation delay) — это время, которое требуется данным, чтобы пройти по сети от отправителя до конечного получателя. Часто этот термин заменяют радиотехническим термином *запаздывание (latency)*, который описывает процесс передачи сигнала.

Задержка — интервал времени между моментом получения фрейма устройством и моментом, когда фрейм пересылается через порт назначения.

Закон о технике безопасности и гигиене труда (Occupational Safety and Health Administration — OSHA). Организация OSHA отвечает за защиту работников и соблюдение законов о труде США и является подразделением Министерства охраны труда США. Она определяет правила безопасности и охраны труда, развития и сопровождения стандартов, проведения обучения персонала, поддерживает программы помощи неимущим и нуждающимся, обеспечивает взаимодействие между разными ведомствами и, в конечном итоге, отвечает за улучшение условий труда и усовершенствование техники безопасности на рабочем месте.

Зарезервированные порты (well-known ports) определены документом RFC 1700 и зарезервированы и в протоколе TCP, и в протоколе UDP. Зарезервированные порты могут определять приложения, выполняемые над протоколами транспортного уровня.

Затухание сигнала (attenuation) представляет собой уменьшение амплитуды сигнала по мере его прохождения по каналу.

Затухание — уменьшение энергии сигнала при его прохождении через среду передачи данных.

Зацикливание пакета (count to infinity) — проблема, которая может возникнуть в некоторых алгоритмах маршрутизации с низкой скоростью конвергенции и состоящая в том, что маршрутизаторы бесконечно увеличивают метрику количества переходов к какой-либо сети. Для предотвращения такой проблемы обычно устанавливается максимально допустимое количество переходов.

Защищенная витая пара (Shielded Twisted Pair — STP) — тип кабеля витой пары, в которой каждая пара имеет свой экран, а весь кабель защищен общим экраном.

Звездообразная топология (star topology) — наиболее часто используемая физическая топология локальных сетей Ethernet. Сеть со звездообразной топологией имеет центральную точку соединений, которая может быть концентратором, коммутатором или маршрутизатором; в этой точке сходятся все кабельные сегменты.

Звуковая плата. Плата расширения, которая обеспечивает вывод аудиоинформации.

Иерархическая топология (hierarchical topology) — эта топология создается аналогично расширенной звездообразной топологии. Основным отличием является отсутствие в ней центрального узла. Вместо него используется магистральный узел, от которого расходятся ветви к другим узлам.

Именованный список управления доступом (named ACL) — это стандартный или расширенный список управления доступом, в котором вместо номера используется имя.

Импеданс (impedance) — величина, характеризующая сопротивление кабеля переменному току (AC), измеряется в омах.

Импульс (pulse) характеризует значение передаваемых данных. Если возмущение вызвано целенаправленно и имеет фиксированный и предсказуемый характер, оно называется импульсом.

Инкапсуляция (encapsulation) — упаковка данных в заголовок некоторого конкретного протокола. Например, данные протоколов высокого уровня перед передачей помещаются в заголовок Ethernet. Аналогичным образом при соединении посредством мостов разнородных сетей весь фрейм из одной сети может быть помещен после заголовка, используемого протоколом канального уровня другой сети.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers — IEEE) — профессиональная организация, одним из направлений работы которой является разработка стандартов для передачи данных и сетей. Доминирующими стандартами для построения локальных сетей являются стандарты организации IEEE.

Инструментальный барабан представляет собой катушку большого диаметра, которая используется в механических кабелеукладчиках.

Интеллектуальный концентратор (intelligent hub) — иногда такой концентратор называют “умным”. Устройства данного типа обычно функционируют как активные концентраторы, однако имеют дополнительные микропроцессоры и обладают функциями диагностики. Они дороже активных концентраторов и имеют полезные функции обнаружения неисправностей.

Интерфейс командной строки (Command-Line Interface — CLI) — интерфейс, который позволяет пользователям взаимодействовать с операционной системой посредством ввода специализированных команд и их аргументов.

Интерфейс подключаемых (сетевых) устройств (Attachment Unit Interface — AUI) — интерфейс 15-контактного физического разъема между сетевой картой компьютера и кабелем среды Ethernet.

Интерфейс представляет собой соединение между двумя системами или устройствами. В терминологии маршрутизаторов интерфейс — это сетевое соединение.

Интерференция в радиочастотном диапазоне (RFI — radio frequency interference) представляет собой шум от сигналов, передаваемых вблизи кабеля.

Кабелепровод — это канал, в котором размещены кабели. К кабелепроводам относятся как коробы систем питания, так и коробы сетей передачи данных различных типов: сплошные, декоративные, металлические, трубчатые и сетчатые, настенные и встроенные коробы и приспособления для укладки кабелей.

Кабельная подставка служит для размещения нескольких небольших бобин кабеля одновременно. Она позволяет монтажнику прокладывать по одному и тому же маршруту несколько сегментов кабеля одновременно.

Канальный уровень (data link layer) — второй уровень эталонной модели OSI. Обеспечивает передачу данных по физическому каналу. Канальный уровень отвечает за физическую адресацию, анализ сетевой топологии, контроль канала, уведомление об ошибках, упорядоченную доставку фреймов и управление потоками.

Карта сетевого интерфейса (Network Interface Card — NIC) представляет собой плату, которая позволяет осуществлять передачу и прием данных компьютерной системой в сети.

Килобайт (КБ). 1024 байта, при оценочных вычислениях используется значение 1000 байтов.

Килобайты в секунду (Кбайт/с). Одна тысяча байтов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.

Килобит (Кб). 1024 бита, при оценочных вычислениях используется значение 1000 битов.

Килобиты в секунду (Кбит/с). Одна тысяча битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.

Класс IP-адреса — 32-битовый адрес, делится на сетевую и узловую части. Бит или последовательность битов в начале любого адреса задают его класс.

Коаксиальный кабель состоит из внешнего цилиндрического проводника, который окружает центральный проводник.

Кодирование — процесс представления битов при помощи различных уровней напряжения.

Коллизия (collision): в сетях Ethernet коллизия — столкновение фреймов, произошедшее вследствие попытки одновременной их передачи. В результате оба фрейма повреждаются при встрече в физической среде.

Кольцевая топология (ring topology) — тип сетевой топологии, при использовании которого рабочие станции объединяются в кольцо одним или двумя кабелями. В отличие от физической шинной топологии, в кольцевой нет начала и конца, поэтому необходимость в терминаторе отсутствует.

Комитет CENELEC (European Committee for Electrotechnical Standardization — Европейский комитет по стандартизации электротехнических средств) — некоммерческая организация Бельгии. Ее основной задачей является разработка электротехнических стандартов Европы.

Коммутатор (switch) — устройство, соединяющее сегменты локальной сети LAN и использующее таблицу MAC-адресов для определения сегментов, в которые следует переслать фреймы. Такой принцип работы позволяет существенно уменьшить объем нецелесообразно рассылаемых данных. Коммутаторы работают с гораздо бо́льшими скоростями, чем мосты. Коммутаторы работают на канальном уровне эталонной модели OSI.

Коммутационная панель (patch panel) — это объединение определенного количества разъемов и портов, которое можно установить в монтажную стойку либо настенный шкаф в кабельном узле. Коммутационные панели выступают в роли пассивного коммутационного оборудования и используются для быстрого изменения топологии подключения устройств. Задняя стенка панели предназначена для подключения и фиксации кабелей, передняя стенка представляет собой промышленный блок контактных разъемов определенного типа.

Коммутация каналов (circuit switching) представляет собой технологию, в которой во время сеанса связи должен существовать физический канал между отправителем и получателем. Широко используется в сетях телефонных компаний. С технологической точки зрения коммутацию каналов можно рассматривать как противоположность коммутации пакетов и сообщений, а с точки зрения методов доступа — как противоположность методу конкуренции и передачи маркеров. Примером сетевой технологии с коммутацией каналов является ISDN.

Коммутация пакетов (packet switching) представляет собой сетевую технологию, в которой разные узлы обмениваются друг с другом пакетами данных по одному разделяемому каналу связи.

Конвергенция (convergence) — это способность группы устройств объединенной сети, использующих конкретный протокол маршрутизации, согласовать друг с другом информацию о топологии сети после того, как в ней произошли изменения. Требуемое для этого время определяет скорость конвергенции.

Конвертер гигабитового интерфейса (Gigabit Interface Converter — GBIC) представляет собой устройство ввода/вывода, подключаемое к порту Gigabit Ethernet и допускающее замену без выключения системы.

Конечное оборудование линии передачи данных (Data Circuit-terminating Equipment — DCE) — это устройство, используемое для конвертирования данных пользователя из цифрового формата DTE в форму, приемлемую для оборудования служб распределенной сети.

Концевик (trailer) — это управляющая информация, добавляемая во фрейм при инкапсуляции после данных для последующей передачи фрейма по сети.

Концентратор (hub) — общая точка соединений устройств сети. Обычно концентраторы используются для подсоединения к локальной сети отдельных сегментов. Концентратор может иметь несколько портов. Когда на один из них поступает пакет, он копируется и направляется на все остальные порты концентратора, поэтому такой пакет поступает во все сегменты LAN-сети.

Лавинная рассылка (flooding) представляет собой способ передачи данных, применяемый коммутаторами и мостами, при использовании которого данные, полученные на некотором интерфейсе, рассылаются через все интерфейсы устройства, за исключением того, на котором они были первоначально получены.

Логарифм — это число, показывающее, в какую степень надо возвести основание для получения заданного числа.

Логическое подключение. Логическое подключение использует стандарты, называемые протоколами.

Локальная сеть (local-area network — LAN) — высокоскоростная сеть передачи цифровых данных с низким уровнем ошибок, охватывающая относительно небольшую географическую область (до нескольких километров). Локальные сети включают в себя рабочие станции, периферийные устройства, терминалы и другие устройства, расположенные в одном здании или в другой географически ограниченной области.

Магистраль (backbone) — применительно к структурированной кабельной сети — кабельный маршрут между телекоммуникационными узлами или зданиями.

Магистральная, или вертикальная, кабельная система используется для подключения промежуточных и главных кабельных узлов, расположенных на разных этажах здания.

Максимальный модуль передачи данных (Maximum Transmission Unit — MTU) — это максимальный размер пакета в байтах, который может быть обработан конкретным интерфейсом.

Манчестерское кодирование (Manchester encoding) — это цифровая схема кодирования, используемая в стандарте IEEE 802.3 в сетях Ethernet, в которой междубитовые переходы используются для синхронизации; бинарному числу 1 соответствует высокий уровень сигнала в первый полупериод битового интервала.

Маршрутизатор — устройство сетевого уровня, использующее одну или несколько метрик для определения оптимального пути, по которому следует передавать поток данных. Маршрутизаторы передают пакеты между сетями на основе информации сетевого уровня, содержащейся в маршрутных обновлениях. Иногда такие устройства также называются *шлюзами (gateway)*, однако подобное определение шлюза на сегодняшний день является устаревшим.

Маршрутизация (routing) представляет собой процесс нахождения маршрута к узлу-получателю. В крупных сетях маршрутизация является весьма сложным процессом, поскольку на пути следования пакета к конечному узлу-получателю может находиться большое количество промежуточных узлов.

Маршрутизируемый протокол — любой сетевой протокол, предоставляющий достаточно информации в адресе сетевого уровня, необходимой для передачи пакета от одного узла другому на основе принятой схемы маршрутизации. Примерами маршрутизируемых или сетевых протоколов могут служить протоколы AppleTalk, IPX и IP.

Маска подсети — 32-битовые маски в протоколе IP, служат для указания битов IP-адреса, использующихся в адресе подсети. Иногда их называют просто *маской*.

Материнская плата. Основная печатная плата компьютера.

Мгновенные изменения (triggered update) представляют собой сообщения об изменении маршрутизации, рассылаемые в случае изменения топологии сети, не дожидаясь истечения времени таймера анонсов.

Мегабайт (МБ). Равен 1 048 576 байтам, при оценочных вычислениях используется значение 1 миллион байтов. Мегабайт иногда называют "мег". Объем оперативной памяти в большинстве компьютеров обычно измеряется в мегабайтах. Большие файлы имеют размер порядка нескольких мегабайтов.

Мегабайты в секунду (Мбайт/с). Один миллион байтов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение.

Мегабит (Мб). Приблизительно равен 1 миллиону битов.

Мегабиты в секунду (Мбит/с). Один миллион битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Обычное соединение Ethernet работает со скоростью 10 Мбит/с.

Международная Ассоциация производителей плат памяти для персональных компьютеров (Personal Computer Memory Card International Association — PCMCIA). Организация, которая разработала стандарт небольших устройств размером с кредитную карту, называемых PCMCIA-картами (иногда — PC-картами). Стандарт, изначально разработанный для расширения памяти портативных компьютеров, в последующем был расширен несколько раз и в текущий момент используется для подключения многих типов устройств.

Метрика (metric) — это числовое значение, вырабатываемое каким-либо алгоритмом для каждого маршрута в сети. Обычно чем меньше метрика, тем предпочтительнее маршрут.

Метрика маршрутизации (routing metric) — метод, с помощью которого алгоритм маршрутизации сравнивает маршруты. Информация о метрике маршрутов хранится в таблицах маршрутизации и рассылается в сообщениях обновления маршрутизации. В качестве параметров метрики могут использоваться ширина полосы пропускания, затраты на передачу, задержка, количество переходов, загрузка канала, максимальный модуль передачи (MTU), стоимость маршрута и надежность канала. Чаще всего ее называют просто метрикой, опуская вторую часть термина.

Механизм скользящего окна (windowing) — механизм управления потоком, который требует, чтобы устройство-получатель получало подтверждение от устройства-отправителя после передачи определенной порции данных.

Механизм скользящего окна (windowing) управляет потоками данных. Получатель сообщает отправителю, какого размера окно (сколько октетов) он способен обработать в данный момент. После этого отправитель отправляет получателю указанное количество октетов.

Механизм создания подсетей (subnetting) — метод деления полного адреса любого из классов на более мелкие части. Этот механизм позволил избежать полного исчерпания доступных IP-адресов (версии 4).

Микропроцессор. Кремниевый кристалл, содержащий интегральные схемы.

Микросегментация (microsegmentation) позволяет создавать в локальной сети частные или выделенные сегменты, в которых на каждый сегмент приходится только одна рабочая станция. В этом случае каждая станция получает мгновенный доступ ко всей полосе пропускания, и ей не приходится конкурировать с другими за доступ к доступной полосе пропускания.

Многоадресатный адрес (multicast address) — уникальный сетевой адрес, позволяющий направить пакеты предопределенной группе узлов.

Многомодовое оптическое волокно — волокно, в котором существует более одного пути для прохождения световых лучей.

Многопортовые блоки розеток (Multiuser Telecommunications Outlet Assemblies — MUTOA) — это приспособление, которое за счет модульной структуры позволяет перемещать и добавлять устройства без дополнительной прокладки кабеля. В такие блоки обычно подключают компьютерное оборудование и телефоны.

Множественный доступ с обнаружением коллизий (Carrier Sense Multiple Access/ Collision Detect — CSMA/CD) представляет собой механизм доступа к среде передачи, при использовании которого устройства, готовые к передаче данных, предварительно прослушивают канал для выяснения, не занят ли он. Если в течение заданного промежутка времени канал не занят, начинается передача. Если два устройства начинают передачу одновременно, происходит коллизия, которая регистрируется всеми участвующими в коллизии устройствами. Такая коллизия вызывает у устройств задержку повторной передачи в течение некоторого случайным образом выбираемого промежутка времени. Метод доступа CSMA/CD используется в сетях спецификаций Ethernet и IEEE 802.3.

Модем (модулятор-демодулятор — Modulator-demodulator, modem) — это устройство, преобразующее цифровые сигналы в аналоговые и наоборот. На станции-отправителе модем преобразует цифровые сигналы в форму, соответствующую каналам аналоговой связи. В пункте назначения аналоговые сигналы преобразуются в цифровую форму. Модемы позволяют передавать информацию по обычным телефонным линиям.

Модули памяти. Микросхемы оперативной памяти, расположенные на панелях памяти, вставляемые в материнскую плату.

Модуль данных мостового протокола (Bridge Protocol Data Unit — BPDU) представляет собой специальное сообщение, используемое в протоколе STP и рассылаемое через определенные интервалы времени для обмена информацией между мостами в сети.

Мост (bridge) — устройство второго уровня, предназначенное для создания двух или более сегментов локальной сети LAN, каждый из которых является отдельным доменом коллизий.

Мультиметр — это прибор для тестирования электрических цепей, с его помощью можно убедиться, что напряжение в телекоммуникационной линии отсутствует. Большинство мультиметров позволяет измерить постоянное и переменное напряжение, ток, сопротивление, проверить целостность линии и работоспособность диода или транзистора.

Наводки — это воздействие электромагнитных волн, излучаемых одним проводником, на другой близлежащий проводник.

Национальный институт стандартизации США (American National Standards Institute — ANSI) — это некоммерческая организация, в которую входят представители государственных ведомств, крупных корпораций и других организаций и которая координирует деятельность, связанную со стандартами. Она утверждает стандарты в США, разрабатывает позицию Штатов в международных организациях по стандартизации и дает рекомендации по применению международных стандартов внутри страны. Институт принимает участие в разработке как международных, так и национальных стандартов, в частности, тех, которые относятся к телекоммуникациям и сетевым технологиям.

Неполносвязная топология (partial-mesh topology) — в сети с такой топологией, по крайней мере, одно устройство имеет несколько соединений с другими устройствами сети, однако при этом сеть не обладает полносвязной структурой. Вместе с тем неполносвязная топология обеспечивает определенный уровень избыточности за счет наличия нескольких альтернативных маршрутов.

Неэкранированная витая пара (Unshielded Twisted Pair — UTP) — среда передачи данных, представляющая собой четыре пары свитых медных проводников в пластиковой оболочке без металлизированного экрана. Широко используется в различных сетях.

Объединительная плата (backplane). Большая печатная плата, которая содержит разъемы для карт расширения.

Одноадресатная рассылка (unicast) представляет собой сообщение, отправляемое одному сетевому получателю.

Одномодовое оптическое волокно — такое волокно, в котором существует только один путь для распространения светового луча; по своей сути противоположно многомодовому оптическому волокну.

Одноранговая связь (peer-to-peer communication) — форма связи устройств в сети, в которой каждый уровень эталонной модели OSI источника вступает в связь с аналогичным уровнем получателя.

Одноранговая сеть (peer-to-peer network) — это сеть, в которой компьютеры выступают по отношению друг к другу как равноправные партнеры. При необходимости каждый из них может принимать на себя как функции сервера, так и функции клиента.

Октет — 8 битов. В области сетевых технологий термин октет часто используется (чаще, чем байт) по причине того, что в некоторых структурах используют байт, который не равен 8 битам.

Оперативная память (random-access memory — RAM) — это память, которая функционирует только при включенном питании, ее содержимое может записываться и считываться микропроцессором.

Опорная сеть, или магистраль (backbone) — часть сети, по которой проходит весь трафик, предназначенный для различных участков сети.

Оптоволоконный кабель — среда передачи данных для модулированного светового луча. По сравнению с другими средами передачи данных, он является более дорогим, но нечувствительным к электромагнитной интерференции кабелем. Иногда его называют просто оптическим волокном.

Осциллограф (Oscilloscope) — электронное устройство, используемое для наблюдения электрических сигналов, таких, как волны и импульсы напряжения.

Отказ в обслуживании (DoS — denial-of-service) представляет собой тип сетевой атаки, призванной заблокировать сеть, завалив ее потоком бесполезного трафика.

Отладка (debugging) используется для поиска и устранения ошибок и багов[2] в программах или моделях.

Отражение лучей света, падающих на границу раздела двух физических сред, происходит под тем же углом (углом падения), но в обратном направлении.

[2] *Существует легенда, что термин* bar *(от англ.* bug *— насекомое, жук, клоп) появился достаточно давно, еще на заре вычислительной техники, когда в узлы первых электронно-механических вычислительных машин попадали насекомые, которые приводили к отказам. В настоящее время этот термин используется в программировании для обозначения ошибок в программном коде и иногда — применительно к аппаратным ошибкам. — Прим. ред.*

Очередь (queue) — механизм, позволяющий задать с помощью списков управления доступом такой принцип обработки трафика, что определенные потоки данных, например, на основании номера протокола, будут отправлены прежде всех остальных. Очередность является настраиваемым механизмом, который позволяет указать, по какому именно признаку следует передавать некоторые данные раньше: например, трафик можно разделить по адресам, по протоколам и т.п.

Ошибка выравнивания (alignment error) фрейма происходит, когда конец сообщения не совпадает с границей октета.

Ошибка выхода за границы фрейма (range error) возникает в том случае, когда фрейм содержит разрешенное значение в поле длины фрейма (Length field), однако это значение не совпадает с количеством октетов, находящихся в поле данных (Data field) полученного фрейма.

Пакет — логически сгруппированная единица информации, включающая заголовок, который содержит контрольную информацию, и (зачастую) пользовательские данные. Чаще всего о пакете говорят как о модуле передачи информации сетевого уровня. Термины *дейтаграмма*, *фрейм* и *сегмент* также описывают различные логические единицы информации на разных уровнях модели OSI и на разных технологических стадиях.

Пакеты многоадресатной рассылки (multicast) — это пакеты, которые копируются в сети и рассылаются по заданному набору сетевых адресов.

Память с произвольным доступом (Random-access memory — RAM). Так называют оперативную память, в которую можно записывать новые данные и считывать сохраненные. При выключении питания содержимое памяти пропадает.

Параллельный порт. Интерфейс, через который может передаваться более одного бита информации одновременно. Используется для подключения различных внешних устройств, например, принтера.

Передача маркера (token passing) — метод доступа, при использовании которого устройства сети получают доступ к физической среде передачи упорядоченным образом, на основе обладания небольшим фреймом, называемым маркером.

Перекрестные наводки (crosstalk) — это передача сигнала от одной проводной пары близлежащим. Смежные проводные пары того же кабеля при этом действуют как антенны, генерируя слабый, но подобный передаваемому электрический сигнал, который может интерферировать передаваемые по этим парам собственные сигналы.

Перекрестные наводки на ближнем конце (NEXT — near-end crosstalk) — величина, измеряемая как отношение амплитуд напряжений тестового сигнала и возникающих помех при измерении на одном и том же конце канала.

Перекрестные наводки на дальнем конце (FEXT — far-end crosstalk) представляют собой наводки, возникающие в том случае, когда сигналы одной витой пары вступают во взаимодействие с сигналами другой пары при поступлении на дальний конец кабельной системы с несколькими парами.

Перекрестные наводки равного уровня на дальнем конце (ELFEXT — equal-level far-end crosstalk) — тест, в котором замеряется значение FEXT.

Перекрещенный кабель (crossover cable) — это кабель, в котором перекрещена пара, для того чтобы правильно подать, передать и получить сигналы между однотипными устройствами.

Переход (hop) — прохождение пакетом данных расстояния от одного сетевого узла, обычно маршрутизатора, к другому.

Печатная плата (Printed circuit board — PCB). Тонкая плата, на которой расположены микросхемы и другие электрические компоненты.

Плата сетевого интерфейса (Network Interface Card — NIC) — печатная плата, вставляемая в гнездо расширения на материнской плате компьютера. Также может быть отдельным периферийным устройством.

Пленум (plenum) — ниша системы отопления, вентиляции или кондиционирования воздуха.

Повторитель (repeater) — сетевое устройство, функционирующее на первом (физическом) уровне эталонной модели OSI. Назначение повторителя состоит в регенерации и ресинхронизации сетевых сигналов на битовом уровне, что позволяет передавать их по передающей среде на бо́льшее расстояние.

Подключаемые программы. Программы, которые устанавливаются как часть Web-браузера и используются для отображения различной мультимедийной информации.

Подсеть. 1. В IP-сетях — часть сети с общим адресом подсети. Сеть делится на подсети произвольно сетевым администратором; при этом обеспечивается многоуровневая, иерархическая структура маршрутизации, в то же время нет необходимости в сложной адресации присоединенных сетей. 2. В сетях OSI — набор систем ES и IS, находящихся под контролем одного административного домена и использующих один протокол сетевого доступа.

Полное сопротивление (импеданс) — сопротивление движению электронов в цепи с переменным током (включает в себя активное и реактивное сопротивление).

Полносвязная топология (full-mesh topology) — разновидность сетевой топологии, в которой все устройства (узлы) соединены друг с другом, что обеспечивает высокий уровень избыточности и устойчивости при отказах отдельных каналов.

Полудуплексная передача (half duplex) представляет собой возможность передачи данных между передающей и принимающей станциями в каждый конкретный момент времени только в одном направлении.

Порт (Port). В IP-терминологии представляет собой процесс верхнего уровня, который принимает данные от нижних уровней. Порты нумеруются и привязываются к конкретным процессам. Например, протокол SNMP приписан к порту с номером 25. Номер порта такого типа называется *зарезервированным портом, или адресом.*

Порт клавиатуры. Используется для подключения клавиатуры к компьютеру.

Порт мыши. Используется для подключения устройства типа "мышь" к компьютеру.

Порт универсальной последовательной шины (Universal Serial Bus port — USB port). Интерфейс для подключения внешних устройств, таких, как "мышь", модемы, клавиатуры, сканеры и принтеры, которые могут подключаться и отключаться без перезагрузки системы.

Последовательный порт. Интерфейс, используемый для последовательной передачи данных, в котором за единицу времени передается только один бит.

Постоянное запоминающее устройство (Read-only memory — ROM). Тип компьютерной памяти, в которой данные предварительно записаны.

Преломление — эффект изменения направления распространения светового луча при переходе через границу раздела двух физических сред.

Привилегированный режим используется для копирования и выполнения других действий с файлами конфигурации и настройки устройства.

Привод компакт-дисков (CD-ROM). Оптический привод, который считывает информацию с компакт-дисков.

Привод накопителей на гибких дисках (Floppy disk drive — FDD). Устройство, которое может считывать и записывать информацию на гибкие диски.

Привод накопителей на жестких дисках (Hard disk drive — HDD). Считывает и записывает данные на жесткий диск, является основным устройством для хранения данных компьютера.

Прикладные программы. Программное обеспечение, которое интерпретирует данные, отображает информацию в доступном формате и является последним звеном в процессе установки соединения. Прикладные программы работают с протоколами для передачи и получения данных через сеть Internet.

Приложение (Application) — это программа, которая выполняет какую-либо функцию непосредственно для пользователя. Примерами сетевых приложений являются клиентские части протоколов FTP и telnet.

Промежуточный коммутационный узел (Intermediate Cross-connect — IC) — это узел, который подключен к главному и в котором размещено оборудование здания или территориальной сети. Он соединяет между собой магистраль и главные узлы с горизонтальными.

Пропускная способность сети (throughput) — объем информации, поступающей в конкретную точку сетевой системы или проходящей через нее.

Простейший протокол передачи файлов (Trivial File Transfer Protocol — TFTP) — упрощенная версия протокола FTP, позволяющая передавать по сети файлы от одного компьютера на другой, обычно без какой-либо аутентификации клиента (например, запроса имени пользователя и пароля).

Простой протокол управления сетью (Simple Network Management Protocol — SNMP) представляет собой протокол, используемый почти исключительно в TCP/IP-сетях. Протокол SNMP обеспечивает средства для мониторинга и управления сетевыми устройствами, а также для управления конфигурациями, сбором статистических данных, производительностью и защитой информации.

Протокол (protocol) — формальное описание набора правил и соглашений, управляющих обменом информацией между устройствами сети.

Протокол ARP (Address Resolution Protocol — протокол преобразования адресов) — представляет собой протокол сети Internet, используемый для преобразования IP-адресов в MAC-адреса.

Протокол FTP (File Transfer Protocol) — протокол пересылки файлов. Прикладной протокол, являющийся частью группы протоколов TCP/IP и используемый для пересылки файлов между узлами сети. Протокол FTP описан в документе RFC 959.

Протокол HTTP — протокол передачи гипертекста (Hypertext Transfer Protocol). Протокол, используемый Web-браузерами и Web-серверами для передачи файлов, например, текстовых и графических.

Протокол Internet (Internet Protocol — IP). Протокол сетевого уровня в стеке протоколов TCP/IP; обеспечивает передачу данных между сетями без предварительной установки соединения.

Протокол IP версии 6 (IPv6) — замена текущей версии протокола IP версии 4 (IPv4). Протокол IPv6 включает поддержку механизма идентификации потока (flow ID) в заголовке пакета. Изначально его называли IPng (IP next generation — IP нового поколения).

Протокол RARP (Reverse Address Resolution Protocol — протокол обратного преобразования адресов) представляет собой — протокол в стеке TCP/IP, предоставляющий возможность по известным MAC-адресам найти IP-адреса.

Протокол TCP (Transmission Control Protocol — протокол управления передачей) — протокол транспортного уровня с установлением соединения, который обеспечивает надежную дуплексную передачу. Протокол TCP относится к стеку TCP/IP.

Протокол UDP (User Datagram Protocol) — протокол передачи пользовательских дейтаграмм. Он является протоколом транспортного уровня без установления соединения из группы протоколов TCP/IP. UDP — это простой протокол, который обеспечивает обмен дейтаграммами без подтверждений или гарантий доставки, требуя, чтобы обработку ошибок и повторную передачу контролировал какой-либо другой протокол. Этот протокол описан в документе RFC 768.

Протокол внешнего шлюза (Exterior Gateway Protocol — EGP) — Internet-протокол, использующийся для обмена маршрутной информацией между автономными системами. Протокол граничного шлюза (Border Gateway Protocol — BGP) является наиболее распространенным протоколом класса EGP.

Протокол внутреннего шлюза (Interior Gateway Protocol — IGP) — Internet-протокол, использующийся для обмена маршрутной информацией внутри автономных систем. Примерами широко используемых протоколов класса IGP являются IGRP, OSPF и RIP.

Протокол доступа к подсети (Subnetwork Access Protocol — SNAP) представляет собой межсетевой протокол, который работает между сетевым объектом подсети и сетевым объектом в конечной системе. Протокол SNAP определяет стандартный метод инкапсуляции IP-дейтаграмм и ARP-сообщений в IEEE-сетях. SNAP-объект в конечной системе использует услуги, предоставляемые подсетью, и выполняет три ключевые функции: передачу данных, управление соединением и выбор параметров качества обслуживания (QoS).

Протокол маршрутизации (routing protocol) — это протокол, осуществляющий реализацию какого-либо алгоритма маршрутизации. Примерами протоколов маршрутизации могут служить протоколы IGRP, OSPF и RIP.

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP) — это протокол внутреннего шлюза (IGP), разработанный корпорацией Cisco для решения проблем, возникающих при осуществлении маршрутизации в крупных неоднородных сетях. *Ср. с протоколом EIGRP. См. также IGP, OSPF и RIP.*

Протокол маршрутизации по состоянию канала (link-state routing protocol) — это алгоритм маршрутизации, в котором каждый маршрутизатор выполняет широковещательную или многоадресатную рассылку информации о стоимости маршрута к каждому из своих соседей всех остальных узлов сети. Алгоритмы состояния канала создают связную картину всей сети, поэтому они практически не подвержены проблеме возникновения циклических маршрутов. Однако такое поведение достигается ценой большего объема и сложности вычислений и большего объема служебных сообщений, чем у дистанционно-векторных протоколов.

Протокол маршрутной информации (Routing Information Protocol — RIP) — протокол IGP-типа, поставлявшийся с BSD UNIX-системами. Это наиболее широко распространенный протокол маршрутизации в локальных сетях. Протокол RIP использует в качестве метрики счетчик транзитных узлов.

Протокол обеспечения безопасности для беспроводных сетей (Wired Equivalent Privacy — WEP) — механизм обеспечения безопасности, описанный в стандарте 802.11, предназначен для защиты процесса взаимодействия сетевой платы и точки доступа от несанкционированного прослушивания.

Протокол обнаружения устройств Cisco (Cisco Descovery Protocol — CDP). Протокол CDP используется для получения информации о соседних устройствах, такой, как тип присоединенных устройств, интерфейсы маршрутизатора, которые в настоящий момент присоединены, и номера моделей устройств.

Протокол распределенного связующего дерева (STP — Spanning Tree Protocol) представляет собой используемый в мостах и коммутаторах протокол, в котором задействован алгоритм связующего дерева для обеспечения динамического самообучения мостов и предотвращения образования кольцевых маршрутов. Мосты обмениваются BPDU-сообщениями, которые позволяют обнаружить кольцевые маршруты и устранить их посредством отключения отдельных интерфейсов.

Протокол удаленного копирования (Remote Copy Protocol — RCP) представляет собой механизм, который позволяет копировать файлы как с удаленного сервера на локальный узел, так и в обратном направлении.

Протокол управления передачей/протокол Internet (Transmission Control Protocol/Internet Protocol — TCP/IP). Название набора протоколов, разработанных Министерством обороны США в 1970-х годах для построения всемирной сети. TCP и IP — два наиболее известных протокола из этого стека.

Протокол управляющих сообщений сети Internet (Internet Control Message Protocol — ICMP) представляет собой Internet-протокол сетевого уровня, сообщающий об ошибках и предоставляющий другую информацию относительно обработки IP-пакетов. Описан в документе RFC 792.

Протокол. Формальное описание набора правил и соглашений, которые описывают, как именно устройства в сети обмениваются данными.

Процедура начальной самозагрузки (bootstrap) представляет собой последовательность действий, выполняемых устройством после включения питания, в частности, в такую процедуру может входить установка IP-адресов Ethernet-интерфейсов маршрутизатора, которая влияет на дальнейшую загрузку системы (например, загрузка операционной системы выполняется по сети).

Прямой кабель (straight-through cable) — это кабель, в котором сохранен порядок следования контактов на обоих концах. Если провод подсоединен к контакту с номером 1 на одном конце кабеля, то и на другом конце он будет подсоединен к аналогичному контакту 1.

Прямоугольные волны (square waves) — график величины, которая не изменяется непрерывно во времени. Такие величины остаются постоянными в течение некоторого времени, затем внезапно изменяют свое значение, снова сохраняют новое значение, а затем внезапно возвращаются к первоначальному значению.

Рабочая область (work area) представляет собой часть помещения или офиса, в которой используется компьютерное, сетевое и телефонное оборудование.

Радиочастотная интерференция — шумы, возникающие в проводниках из-за воздействия на них радиочастотных сигналов.

Разъем расширения. Разъем в компьютере, обычно на материнской плате, в который вставляются карты расширения для добавления новых возможностей компьютера.

Распределение нагрузки (load sharing). Под распределением нагрузки понимается направление данных одного и того же сеанса связи по нескольким маршрутам в сети для повышения эффективности системы передачи информации.

Распределенная сеть (Wide-Area Network — WAN) представляет собой сеть передачи данных, охватывающую значительное географическое пространство. В ней часто используются передающие устройства, предоставленные открытыми операторами связи, например, местными или государственными телефонными компаниями.

Распределенный интерфейс передачи данных оптоволоконного канала (FDDI — Fiber Distributed Data Interface) представляет собой стандарт 3T9.5 для LAN-сетей, установленный Американским национальным Институтом стандартизации (American National Standards Institute — ANSI), определяющий сеть с передачей маркера со скоростью передачи 100 Мбит/с по оптоволоконному кабелю на расстояние до 2 км. Для обеспечения резервирования в протоколе FDDI используется структура двойного кольца.

Расширение спектра сигнала прямой последовательности (Direct-Sequence Spread Spectrum — DSSS) — технология, в которой передача данных является более надежной, поскольку каждый бит (0 или 1) представляется некой последовательностью нулей и единиц, которая называется элементарной последовательностью.

Расширение спектра со скачкообразным изменением частоты (Frequency-Hopping Spread Spectrum — FHSS) — процесс расширения спектра и передачи данных методом скачкообразного изменения несущей частоты по случайному закону. Такой тип передачи данных позволяет избежать влияния узкополосных шумов, в результате чего сигнал будет более чистым и увеличится надежность передачи данных.

Расширение спектра — особая техника модуляции сигнала, разработанная в 1940-х годах, позволяющая расширить передаваемый сигнал на широкий диапазон радиочастот. Этот термин описывает модуляцию, которая пренебрегает пропускной способностью, для того чтобы получить более высокое соотношение сигнал/шум.

Расширенная звездообразная топология (extended-star topology) — сеть, в которой классическая звездообразная топология расширена и в нее включены дополнительные сетевые устройства, подсоединенные к главному сетевому устройству.

Расширенный список управления доступом (Extended Access Control List — Extended ACL) — список управления доступом, который позволяет проверять адреса отправителя и получателя, а также другие критерии, установленные в правилах расширенного списка управления доступом.

Расщепление горизонта (split horizon) — это механизм маршрутизации, с помощью которого предотвращается рассылка информации о маршруте через интерфейс маршрутизатора, через который она была получена. Расщепление горизонта является одним из способов предотвращения образования петель маршрутизации.

Региональная или городская сеть (Metropolitan-Area Network — MAN) —сеть, охватывающая область крупного города, включая пригороды. В целом MAN-сети, как правило, охватывают большую географическую область, чем локальные сети LAN, но меньшую, чем распределенные сети WAN.

Режим бесфрагментной коммутации (Fragment-free switching) — это режим коммутации, при котором перед пересылкой фреймов фильтруются фрагменты коллизий, являющиеся основным источником ошибок в сети.

Режим глобальной конфигурации (global configuration mode) используется для введения команд в одной строке и команд, которые вносят изменения в глобальную конфигурацию маршрутизатора.

Режим коммутации с промежуточным хранением (Store-and-forward switching) — это техника коммутации, при которой фрейм перед пересылкой в порт назначения полностью записывается в память устройства и обрабатывается. Обработка включает в себя подсчет контрольной суммы и проверку адреса получателя. Дополнительно фрейм должен быть временно сохранен до тех пор, пока сетевые ресурсы (например, канал) не станут доступны для пересылки фрейма.

Режим сквозной коммутации (Cut-through switching). Устройства, использующие этот метод коммутации, читают, обрабатывают и пересылают фреймы сразу после того, как будет прочитан адрес получателя и определен порт назначения. См. также *режим коммутации с промежуточным хранением*.

Самотестирование при включении питания (Power-On Self-Test — POST) — набор диагностических средств, которые проверяют функционирование аппаратуры при включении питания.

Сбалансированный гибридный протокол маршрутизации (balanced hybrid routing protocol) — это протокол маршрутизации, использующий элементы дистанционно-векторного протокола и протокола маршрутизации по состоянию канала.

Сбойный пакет (jabber). В стандарте 802.3 сбойный пакет несколько раз определяется как передача длительностью от 20000 до 50000 битовых интервалов. Однако большинство средств диагностики регистрирует и сообщает о сбойных пакетах каждый раз, когда обнаруживается передача блока длительностью, превышающей максимально допустимый размер фрейма, который значительно меньше 20000–50000 битовых интервалов.

Сборник национальных электротехнических нормативов (National Electrical Code — NEC) представляет собой собрание документов, регулирующих правила охраны населения и имущества от несчастных случаев, связанных с пользованием электричеством. Данная организация финансируется национальной Ассоциацией по пожарной безопасности (National Fire Protection Association — NFPA) и находится под протекцией Национального института по стандартизации США (American National Standards Institute — ANSI).

Светодиодный индикатор (Light-Emitting Diode — LED) — полупроводниковое устройство, которое способно излучать свет при подаче на него напряжения. Обычно используется для отображения состояния в аппаратных устройствах.

Сеансовый уровень (session layer) — пятый уровень эталонной модели OSI. Устанавливает, поддерживает и прекращает сеансы связи между приложениями и управляет обменом данными между уровнями представления данных.

Сегмент (segment). 1. Часть сети, ограниченная мостами, маршрутизаторами или коммутаторами. 2. В спецификации протокола TCP — логически сгруппированная информация на транспортном уровне эталонной модели OSI.

Серверная (серверная комната) — это помещение, в котором размещено оборудование. Зачастую такое помещение является также телекоммуникационным узлом.

Сетевой адаптер (NIC). Печатная плата, которая предоставляет возможность обмениваться данными с сетью.

Сетевой уровень (network layer) — третий уровень эталонной модели OSI. Обеспечивает соединения и выбор маршрутов между конечными системами. На данном уровне происходит маршрутизация.

Сеть Ethernet со скоростью передачи 10 Гбит/с (10-Gb Ethernet). Созданная на базе технологий, используемых в большинстве современных LAN-сетей, технология 10 Гбит/с Ethernet описывается как новая технология, предлагающая боле эффективный и менее дорогой подход к передаче данных по магистральным соединениям между отдельными сетями, оставаясь при этом цельной технологией на протяжении всего маршрута перемещения данных. В настоящее время есть возможность поднять скорость в сетях Ethernet до 10 Гбит/с.

Сеть Internet. Крупнейшая глобальная сеть, объединяющая десятки тысяч сетей по всему миру. Сеть Internet постоянно развивается, стандартизируется, а ее услуги постепенно проникают в сферу быта.

Сеть Token Ring — это локальная сеть, в которой для управления доступом используется передача маркера. Разработана и поддерживается корпорацией IBM. Сеть Token Ring работает со скоростями от 4 до 16 Мбит/с и использует кольцевую топологию.

Сеть с использованием толстого коаксиального кабеля (thicknet) — это один из самых старых типов локальных сетей, реализованных на базе стандарта 10BASE5. Единственным преимуществом таких сетей является возможность передачи данных на расстояния до 500 м без использования усилителей.

Сеть с использованием тонкого коаксиального кабеля (thinnet) — это сеть с использованием простого тонкого коаксиального кабеля, базирующаяся на стандарте 10BASE2. В таких сетях возможна передача данных на расстояния до 185 м, но довольно сильно упрощается работа с кабельным хозяйством.

Сеть хранилищ данных (Storage-Area Network — SAN) — высокопроизводительная выделенная сеть, осуществляющая обмен данными между серверами и устройствами хранения данных.

Сигнал подтверждения (Acknowledgment) — извещение, посылаемое одним сетевым устройством другому, о том, что произошло некоторое событие (например, прием сообщения). Иногда он сокращенно обозначается как ACK.

Симплексный режим передачи (simplex) — это режим передачи, при котором возможна передача данных от передающей станции принимающей только в одном направлении. Примером симплексной технологии может служить обычное широковещательное телевидение.

Синусоидальные волны (sine waves) — графическое изображение математических функций, описывающих многие природные явления, регулярно происходящие во времени, такие, например, как изменение расстояния от Земли до Солнца, расстояние до земли точки вращающегося "чертового колеса" или время восхода солнца.

Системные маршруты (system routes) — это маршруты между отдельными сетями, входящими в одну автономную систему. Программное обеспечение Cisco IOS создает системные маршруты на основе информации интерфейсов непосредственно подсоединенных сетей и информации, предоставляемой другими IGRP-маршрутизаторами или серверами доступа. Системные маршруты не содержат информацию о подсетях.

Системный блок. Основная часть персонального компьютера.

Служба telnet — стандартный протокол эмуляции терминала из группы протоколов TCP/IP. Протокол telnet используется для организации соединений с удаленного терминала и позволяет пользователям входить в удаленную систему и использовать ее ресурсы так, словно они подключены к локальной системе. Описан в RFC 854.

Служба без установления соединения представляет собой механизм передачи данных без создания виртуального канала.

Служба с установлением соединения представляет собой механизм передачи данных, требующий установления виртуального канала.

Службы с коммутацией ячеек (cell-switched service) предоставляют механизмы передачи данных, которые работают на основе технологии коммутации ячеек, но при этом позволяют создавать виртуальные каналы. Передаваемые данные разбиваются на ячейки фиксированной длины и потом передаются по каналам связи с помощью цифровых технологий передачи сигналов.

Смежное устройство (adjacent neighbor) — так называются два непосредственно соединенных маршрутизатора, обменивающиеся друг с другом информацией маршрутизации.

Смещение задержки (delay skew) — величины задержки распространения в различных парах одного и того же кабеля могут несколько отличаться ввиду различного количества оборотов скручивания и различий электрических параметров пар. Под смещением задержки понимаются такие различия задержки между парами.

Соединительный кабель (patch cord) представляет собой сегмент кабеля с разъемами на концах, который используется для подключения оборудования.

Сообщения о состоянии канала (link-state advertisement — LSA) представляют собой небольшие пакеты, содержащие информацию о маршрутизации, которые рассылаются между маршрутизаторами.

Сообщения удаления маршрутов в обратном направлении (poison reverse updates) представляют собой анонсы маршрутизации, используемые для предотвращения протяженных петель маршрутизации. Чаще всего увеличение метрики маршрута, как правило, свидетельствует о возникновении петель. В таком случае сообщения удаления рассылаются для удаления маршрута из таблицы маршрутизации и перевода его в режим удержания.

Сопротивление — свойство материалов препятствовать прохождению через них электрического тока.

Спектральное уплотнение сигнала (WDM — Wavelength-Division Multiplexing) — метод, позволяющийт одновременно передавать несколько световых импульсов с разной длиной волны в оптическом кабеле. Спектр каждого канала должен быть адекватным образом отделен от остальных.

Спецификация Ethernet — базовая LAN-спецификация, созданная корпорацией Xerox и впоследствии развивавшаяся корпорациями Xerox, Intel и Digital Equipment. Сети Ethernet используют метод доступа CSMA/CD и разнообразные типы кабелей со скоростями передачи 10, 100 и 1000 Мбит/с. Стандарты Ethernet и IEEE 802.3 аналогичны.

Спецификация Gigabit Ethernet — стандарт высокоскоростных Ethernet-сетей, одобренный комитетом стандартизации IEEE 802.3z в 1996 году.

Спецификация IEEE 802.2 — протокол IEEE для локальных сетей LAN, определяющий реализацию подуровня LLC канального уровня эталонной модели OSI. Стандарт IEEE 802.2 задает методы обработки ошибок и интерфейс службы сетевого (третьего) уровня.

Спецификация IEEE 802.3 — протокол Института IEEE для LAN-сетей, определяющий реализацию MAC-подуровня канального уровня (т.е. физическую часть последнего). В спецификации IEEE 802.3 используется метод доступа CSMA/CD для набора возможных скоростей передачи данных в разнообразных физических средах. Расширения стандарта IEEE 802.3 определяют различные реализации технологии Fast Ethernet. Физические модификации первоначальной спецификации IEEE 802.3 включают в себя версии 10BASE2, 10BASE5, 10BASE-F, 10BASE-T и 10BROAD36. Физическими модификациями технологии Fast Ethernet являются 100BASE-TX и 100BASE-FX.

Список управления доступом (Access Control List — ACL) — способ контроля или ограничения трафика сети, который отвечает различным критериям, установленным определенными правилами.

Справочник по безопасности материалов (Material Safety Data Sheet — MSDS) представляет собой набор документов, в которых содержится информация о правилах хранения, использования и перевозки опасных для здоровья материалов. В нем представлена подробная информация о том, какое влияние на здоровье человека окажет воздействие определенных веществ и материалов и как обезопасить себя при работе с ними.

Среда передачи данных относится к многочисленным типам физического окружения, через которое происходит передача сигнала. Наиболее распространенные среды передачи данных включают в себя витую пару, коаксиальный кабель, оптическое волокно и атмосферу (через которую происходит передача данных с помощью микроволн, лазеров и инфракрасных сигналов).

Стандарт TIA/EIA-568-B определяет десять тестов, которые должен пройти медный кабель для того, чтобы быть пригодным к использованию в современных высокоскоростных локальных сетях Ethernet.

Стандарт — набор широко используемых либо официально рекомендованных правил и процедур.

Стандартный список управления доступом (Standard Access Control List — Standard ACL) — список управления доступом, осуществляющий фильтрацию на основе сравнения адреса отправителя пакетов с заданными в нем правилами.

Статическая маршрутизация (static routing) — это процесс определения и конфигурирования маршрутов вручную.

Стек, или набор протоколов (protocol suite) — это группа связанных, работающих совместно коммуникационных протоколов, обслуживающих взаимодействия на нескольких или всех семи уровнях модели OSI. Не все протоколы стека охватывают все уровни модели, и часто один протокол обслуживает одновременно несколько уровней. Типичным примером стека протоколов является набор TCP/IP.

Структурированная кабельная система, СКС (Structured Cabling System — SCS) — универсальная кабельная система, построенная в соответствии со стандартами, описывающими длину кабелей, типы кабелей и терминирующие устройства. Она представляет собой комплексный проект кабельной системы, в котором стандартизированы и сертифицированы все ее части: разъемы, схемы разводки и распайки контактов, центры распределения линий и методы установки кабеля.

Суммарная мощность помех на ближнем конце (PSNEXT — power sum near-end crosstalk) — величина, характеризующая кумулятивный эффект потерь NEXT от всех проводных пар кабеля.

Суммарная мощность помех равного уровня на дальнем конце (power sum equal-level far-end crosstalk — PSELFEXT) описывает суммарный эффект потерь ELFEXT от всех проводных пар.

Счетчик переходов (hop count) — это метрика маршрутизации, использующаяся для расчета расстояния между отправителем и получателем. Протокол RIP использует счетчик в качестве своей единственной метрики.

Таблица маршрутизации (routing table) — представляет собой некоторую разновидность базы данных, хранящуюся в маршрутизаторе или другом устройстве объединенной сети, в которой содержится информация о маршрутах к конкретным сетям-получателям и, в большинстве случаев, метрики, связанные с этими маршрутами.

Таймер действительности маршрута (invalid timer). Значение этого таймера задает время, в течение которого маршрутизатор в случае отсутствия сообщений об обновлении некоторого маршрута ожидает, перед тем как объявить этот маршрут недействительным. В протоколе IGRP стандартным значением этого таймера является утроенный период анонсов маршрутизации.

Таймер обновлений маршрутизации (update timer). Период этого таймера задает частоту рассылки обновлений маршрутизации. В протоколе IGRP стандартно значение этого таймера устанавливается равным 90 секундам.

Таймер сброса маршрутов (flush timer). Период этого таймера задает время, которое проходит до того, как маршрут будет удален из таблицы маршрутизации. В протоколе IGRP стандартное значение этого таймера равно значению периода обновлений маршрутизации, умноженному на семь.

Таймер удержания информации (hold-time timer) задает время, в течение которого новые сообщения об обновлениях маршрутизации игнорируются. В протоколе IGRP стандартное значение таймера удержания равно утроенному значению периода обновлений маршрутизации, к которому добавляется 10 секунд.

Телекоммуникационный узел (Telecommunications Room — TR) представляет собой помещение или область в здании, где размещено телекоммуникационное оборудование и кабельное хозяйство.

Терабайт (ТБ). Приблизительно 1 триллион байтов. Емкость накопителей на жестких дисках в высокопроизводительных системах измеряется в терабайтах.

Терабиты в секунду (Тбит/с). Один триллион битов в секунду. Распространенная единица измерения количества передаваемых данных через сетевое соединение. Некоторые высокоскоростные магистральные узлы сети Internet работают на скорости более 1 Тбит/с.

Терминальное оборудование (Data Terminal Equipment — DTE) — это устройство, расположенное на пользовательском конце интерфейса пользователь-сеть, которое может выступать в качестве источника данных, получателя данных или в качестве и того, и другого. Устройство DTE соединяется с сетью данных посредством устройства DCE (например, модема) и для синхронизации зачастую использует временные сигналы, генерируемые DCE. Терминальное оборудование включает в себя такие устройства, как компьютеры, трансляторы протоколов и мультиплексоры.

Тестовый пакет (keepalive) — это сообщение, отправляемое одним сетевым устройством, которое сигнализирует другому сетевому устройству о работоспособности виртуального канала между ними.

Технология Fast Ethernet. Этот термин используется в отношении любой из ряда Ethernet-спецификаций, которые работают со скоростью передачи данных 100 Мбит/с. Технология Fast Ethernet обеспечивает скорость передачи, в 10 раз бо́льшую, чем спецификация Ethernet 10BASE-T, сохраняя при этом такие характеристики 10BASE-T, как формат фрейма, MAC-механизмы и размер блока MTU. Эта общность механизмов позволяет использовать существующие приложения и средства управления сетью технологии 10BASE-T в сетях Fast Ethernet. Технология Fast Ethernet является расширением спецификации IEEE 802.3.

Технология передачи данных без установки соединения (connectionless) представляет собой метод передачи данных без установки виртуального канала.

Топологическая база данных (topological database) — это совокупность информации, полученной из сообщений LSA.

Точечно-десятичная запись. Синтетическое представление 32-битовых чисел, которое состоит из четырех 8-битовых чисел, записанных в десятичном эквиваленте, и каждая группа из 8 битов разделяется точкой. Используется для представления IP-адресов в сети Internet, например, 192.67.67.20.

Точкой демаркации, или демарком (demarc), называют узел, в котором кабель провайдера службы подключается к кабельной системе организации или здания.

Транспортный уровень (transport layer) — четвертый уровень эталонной модели OSI. Он отвечает за надежность связи между конечными узлами. Транспортный уровень имеет механизмы установки, поддержки и отключения виртуальных каналов, обнаружения и устранения ошибок при передаче данных, а также управляет информационными потоками.

Трехэтапное квитирование (three-way handshake) — последовательность сообщений, которыми обмениваются два или более сетевых устройства для согласования и синхронизации параметров передачи данных перед началом передачи.

Угол отражения — угол между отраженным лучом и нормалью к поверхности.

Угол падения — угол между падающим лучом и нормалью к поверхности.

Удлиненный фрейм (long frame) — фрейм, длина которого превосходит максимально допустимую, с учетом возможного добавления тега.

Узкополосная интерференция (narrowband interference) представляет собой помехи, затрагивающие лишь узкий диапазон частот.

Управление потоком (flow control) представляет собой методику, благодаря которой не допускается ситуация, когда передающий объект переполняет данными принимающий объект. При полном заполнении буферов принимающего устройства посылающему устройству отправляется сообщение о необходимости отложить передачу данных до завершения обработки данных в буферах. В IBM-сетях этот метод называется *выравниванием скоростей.*

Уровень представления данных (presentation layer) — шестой уровень эталонной модели OSI. Он обеспечивает совместимость форматов (читабельность) данных разных систем.

Уровень приложений (Application Layer) — это седьмой уровень эталонной модели OSI, обслуживающий прикладные процессы (такие, как электронная почта, пересылка файлов и эмуляция терминала), которые являются внешними по отношению к модели OSI. Уровень приложений идентифицирует и устанавливает доступность предполагаемых партнеров по коммуникации (и ресурсов, необходимых для их соединения), синхронизирует взаимодействующие приложения и устанавливает согласованный порядок выполнения процедур восстановления после сбоев и управления целостностью данных.

Уровень сетевого доступа (network access layer) — уровень, обслуживающий все запросы, связанные с организацией физической связи между IP-пакетами и средой передачи.

Физический уровень (physical layer) — первый уровень эталонной модели OSI. Определяет электрические, механические, процедурные и функциональные спецификации активизации, поддержки и отключения физических каналов между конечными системами.

Физическое подключение. Физическое соединение с сетью осуществляется через подключение к компьютеру специализированных карт расширения, таких, как модем или сетевой адаптер, и кабеля.

Флуктуации фазы (дребезжание сигнала, jitter) представляют собой малые отклонения времени получения сигнала или его фазы, которые могут привести к ошибкам в передаваемых данных или потере синхронизации. Чем длиннее кабель, тем бо́льшие отклонения могут в нем присутствовать. Отклонения также зависят от величины затухания сигнала, скорости передачи и частот. В телефонии этим термином обозначают дребезг контактов.

ФМ (фазовая модуляция) — изменение фазы несущего сигнала.

Фрейм (frame) — логически сгруппированная информация, пересылаемая в виде блока данных канального уровня по среде сети.

Фрейм-призрак (ghost). Этот термин был предложен корпорацией Fluke Networks для обозначения энергии (шума), которая обнаруживается в кабеле и выглядит подобно фрейму, однако не имеет действительного поля SFD. Для того чтобы быть квалифицированным как фрейм-призрак, такой "псевдофрейм" должен иметь длину не менее 72 октетов, в противном случае он идентифицируется как удаленная коллизия.

Центр обработки данных (data center) — глобально координируемая сеть, состоящая из устройств, предназначенных для ускорения доставки данных по инфраструктуре сети Internet.

Центральный процессор (Central Processing Unit — CPU). Процессор — это "мозг" компьютера, в котором выполняется большинство вычислений.

Цифровая полоса пропускания (digital bandwidth) описывает объем информации, который может быть передан изь одного места в другое за определенное количество времени.

Частота (frequency) — промежуток времени между отдельными волнами.

Чертеж, или схема (blueprint) — это архитектурный план здания или технический рисунок, по которому можно выяснить особенности конструкции здания и схему размещения помещений, а также оценить необходимое количество кабеля и измерить расстояния.

ЧМ (частотная модуляция) — изменение частоты несущей волны.

Шина (Bus). Набор электрических цепей, через которые передаются данные от одной части компьютера другой.

Шинная топология (bus topology) — топология, в которой все устройства соединены одним кабелем; часто называется линейной шиной. Этот кабель можно сравнить с автобусным маршрутом, проходящим от одной остановки к другой.

Ширина полосы пропускания (bandwidth) — объем информации, проходящей через сетевое соединение за определенный период времени.

Широковещание (broadcast) — процесс рассылки пакетов данных всем узлам сети. Широковещательные пакеты имеют специальный широковещательный адрес.

Широковещательные пакеты (broadcast) — это пакеты данных, рассылаемые всем узлам сети.

Широковещательный адрес используется для широковещательной рассылки пакетов всем сетевым устройствам.

Широковещательный домен (broadcast domain) — это совокупность всех устройств, которые получают широковещательные фреймы от любого из устройств этой совокупности. Границы широковещательного домена обычно определяются маршрутизаторами (или, в коммутируемых сетях, виртуальными сетями VLAN), поскольку маршрутизаторы не пересылают широковещательные фреймы.

Шнур питания. Кабель для подключения электрического устройства к электрической розетке для подачи напряжения.

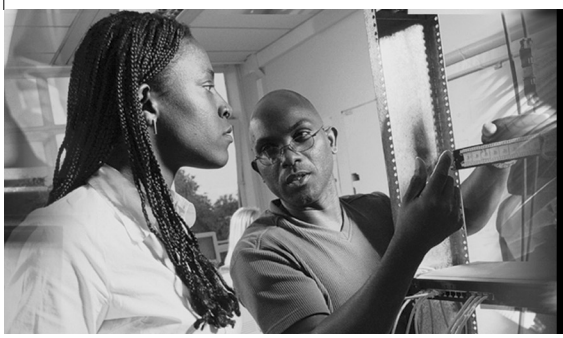
Шум (noise) — в сфере коммуникации под шумом понимаются нежелательные сигналы. Шумы могут вызываться естественными или технологическими источниками и в коммуникационных системах добавляются к полезному сигналу.

Электромагнитная интерференция (ElectroMagnetic Interference — EMI) — это взаимодействие электрического поля с электронными компонентами, устройствами и системами, негативно влияющее на их работу.

Энергонезависимая оперативная память (NonVolatile Random-Access Memory — NVRAM) представляет собой память RAM (Random-Access Memory — оперативная память), содержимое которой сохраняется при отключении питания.

Эталонная модель взаимодействия открытых систем (Open System Interconnection — OSI reference model) — структурная модель сети, разработанная международной организацией по стандартизации (ISO). Эта модель включает в себя семь уровней, каждый из которых выполняет свои специфические функции, такие, как адресация, управление потоком, контроль ошибок, инкапсуляция и надежная передача сообщений. Эталонная модель OSI используется как универсальный метод обучения сетевых специалистов для понимания ими функций компьютерной сети.

Язык гипертекстовой разметки (HyperText Markup Language — HTML). Простой язык гипертекстового форматирования документов, в котором используются теги (неотображаемый текст разметки документа) для указания способа представления частей документа программами-просмотрщиками, такими, как Web-браузеры.



Предметный указатель

Л

М

Н

О

П

P

C

Научно-популярное издание

Корпорация Cisco Systems, Inc.

Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-издание, исправленное

Литературный редактор *Н.В. Саит-Аметова*
Верстка *М.А. Смолина*
Художественные редакторы *В.Г. Павлютин и Т.А. Тараброва*

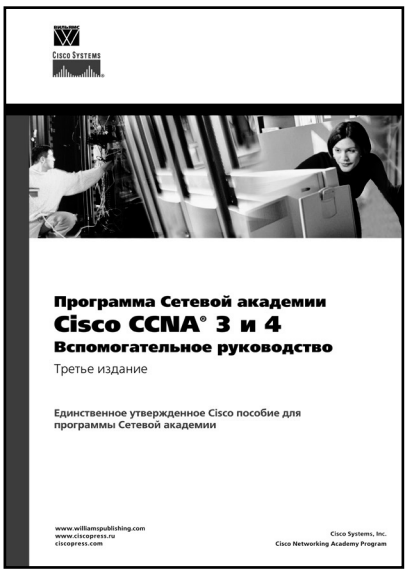
Издательский дом "Вильямс"
127055, г. Москва, ул. Лесная, д. 43, стр. 1

Подписано в печать 11.04.2007. Формат 70x100/16.
Гарнитура Times. Печать офсетная.
Усл. печ. л. 94,17. Уч.-изд. л. 72,50.
Доп. тираж 1500 экз. Заказ № 0000.

Отпечатано по технологии CtP
в ОАО "Печатный двор" им. А.М. Горького
197110, Санкт-Петербург, Чкаловский пр., 15.

ПРОГРАММА СЕТЕВОЙ АКАДЕМИИ CISCO CCNA 3 И 4
ВСПОМОГАТЕЛЬНОЕ РУКОВОДСТВО
3-е издание

Cisco Systems, Inc



www.williamspublishing.com

Эта книга представляет собой одобренное Cisco пособие, дополняющее учебный Web-курс программы Сетевой академии Cisco. Рассмотренные в ней темы предоставляют учащимся необходимый объем знаний для подготовки к экзамену на получение сертификата CCNA и для начала работы в качестве сетевого администратора. В ней также освещаются темы распределенных сетей (WAN), маршрутизации по протоколу Inetrnetwork Packet Exchange (IPX), работы усовершенствованного протокола внутреннего шлюза (Enhanced Interior Gateway Protocol — EIGRP), поиска ошибок и устранения неисправностей в сетях. Кроме того книга позволяет учащемуся расширить свои познания в вопросах проектирования, конфигурирования и поддержки цифровой сети интегрированных служб (Inegrated Services Data Network — ISDN), протоколов “точка точка” (Point-To-Point) и Frame Relay.

ISBN 5-8459-1120-6

в продаже

СИСТЕМА СИГНАЛИЗАЦИИ №7 (SS7/ОКС7)
ПРОТОКОЛЫ, СТРУКТУРА И ПРИМЕНЕНИЕ

Ли Драйберг,
Джефф Хьюитт

www.williamspublishing.com

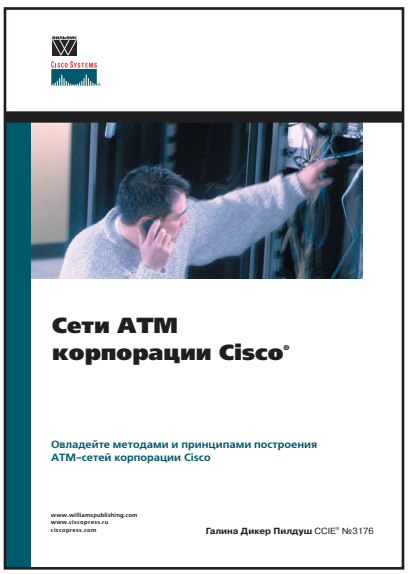
SS7/C7 — это и сеть передачи служебных сигналов и набор протоколов, используемых во всем мире для построения телекоммуникационных сетей как наземных, так и сотовых. Соединение вызовов, мобильный роуминг, передача сообщений, и комплексные службы передачи голоса и данных, как, например, службы перенаправления вызовов и ожидания звонка при передаче данных, — это только малая часть огромного набора расширенных возможностей, которые предоставляют механизмы SS7/C7 в телекоммуникационных сетях. Каждый, кто занимается телекоммуникациями, должен хорошо знать систему сигнализации SS7/C7. Слияние технологий передачи голоса и данных привело к тому, что специалист должен иметь представление об обеих технологиях и понимать, как внедрить голосовые службы в сетях передачи обычных данных. Для специалистов, работающих на узлах связи, эта книга будет достаточно интересной в плане транзитного обмена и межсигнализационного взаимодействия. Однако, одной из завлекающих сторон издания, является и тот факт, что книга может быть применена, как сборник стандартов для разработчиков ПО различных устройств и систем связи.

ISBN 5-8459-1037-4

в продаже

СЕТИ ATM КОРПОРАЦИИ CISCO

Галина Пилдуш



www.williamspublishing.com

Данная книга является как учебником для инженеров для подготовки к экзамену CCIE, так и хорошим справочным пособием для специалистов, желающих получить новые или пополнить уже имеющихся знания в области технологии ATM. Она не ориентирована на определенный уровень читателя: специалист любого профессионального уровня сможет пополнить свои знания о принципах работы среды ATM. Поскольку в первой части книги рассматриваются только общие положения технологии ATM, книга может служить справочным пособием для оборудования любого производителя

ISBN 5-8459-0632-6

в продаже

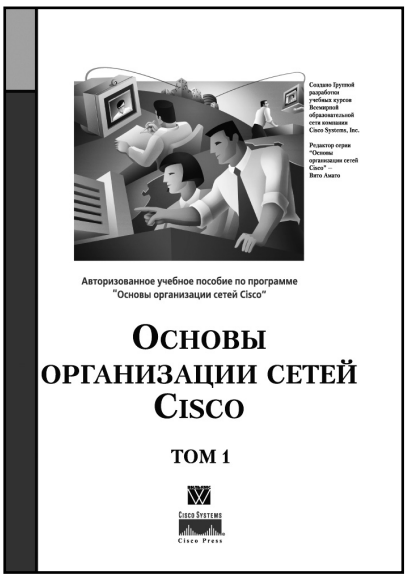
СОЗДАНИЕ МАСШТАБИРУЕМЫХ СЕТЕЙ CISCO

Кэтрин Пакет,
Дайана Тир

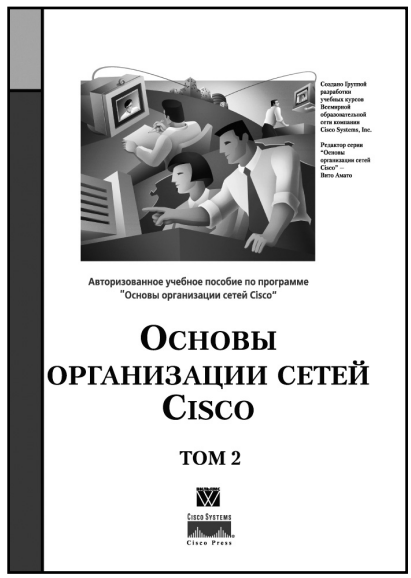
www.williamspublishing.com

Эта книга одна из немногих, предназначенных не столько для широкого круга пользователей, сколько для экспертов по глобальным и локальным сетям. Изложенный здесь материал будет полезен как для профессионалов, так и для тех, кто еще только постигает тонкости этой науки. Другими словами, перед вами достаточно полный учебный материал, в котором подробно описаны многие приемы работы сетями Cisco, используемые опытными сетевыми администраторами на практике. Как настроить маршрутизаторы, исключить возникновение маршрутных петель, оптимизировать трафик и организовать работу в корпоративных сетях — ответы на эти и многие другие важные вопросы вы получите в данной книге. Книга снабжена большим количеством примеров, упражнений и проверочных вопросов, непосредственно относящихся к вопросам администрирования сетей.

в продаже



Данная книга является учебным пособием по курсу *"Основы организации сетей Cisco, часть 1"* и соответствует учебному плану версии 2.1 Сетевой академии Cisco. В соответствии с концепцией курса излагаемый материал полностью структурирован вокруг эталонной модели OSI. Книга рекомендуется для подготовки к тесту CCNA и сертификационному экзамену CompTIA Net+. Разделы о коллизиях и сегментации являются также очень важными для экзамена CCNA. Вышесказанное относится и к технологии Ethernet, которая является домирующей в области локальных сетей. Главы, посвященные IP-адресации, возможно, являются наиболее трудными, но все же очень важными, особенно для экзамена CCNA. Наконец, главы, посвященные кабельным сетевым носителям и электрическим сигналам, будут полезны при рассмотрении кабельных сетей.

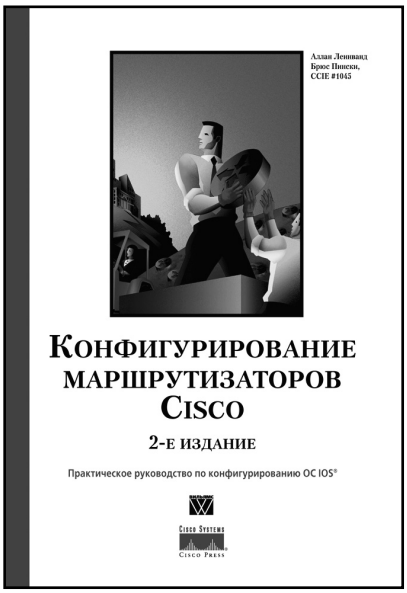


Во 2-ом томе учебного пособия *"Основы организации сетей Cisco, часть 2"* изложены основы построения IP-сетей на базе маршрутизаторов Cisco и описаны способы конфигурирования маршрутизаторов. В книге рассмотрены основополагающие вопросы теории сетей, в частности, эталонная модель OSI, физические основы передачи данных и сигналов, IP-адресация, технология Ethernet и много другое. Большое внимание уделяется поиску неисправностей и устранению конфликтов сети. Книга рекомендуется для подготовки к тесту CCNA и сертификационному экзамену CompTIA Net+.

www.williamspublishing.com

КОНФИГУРИРОВАНИЕ МАРШРУТИЗАТОРОВ CISCO, 2-е издание

Аллан Леинванд, Брюс Пински



www.williamspublishing.com

в продаже

Книга посвящена вопросам практического конфигурирования операционной системы IOS в устройствах межсетевого взаимодействия компании Cisco Systems, Inc. (США). После описания первых шагов по конфигурированию устройства, каким оно извлекается из заводской упаковки, дальше в книге осуществляется переход к конфигурированию ОС IOS для трех наиболее широко используемых сегодня сетевых протоколов: TCP/IP, AppleTalk и IPX. Она также знакомит с основами конфигурирования средств администрирования и управления, включая управление доступом посредством использования протоколов TACACS+ и RADIUS, управление сетью по протоколу SNMP и управление системным временем с помощью протокола NTP. Второе издание существенно обновлено по сравнению с предыдущим за счет введения описания новых функций и команд конфигурирования ОС IOS версии 12.1T. Обновления в этом издании также коснулись решений по конфигурированию ОС IOS для локальных сетей Gigabit Ethernet, цифровых абонентских линий (DSL-сети), DHCP-служб и доступа к работающим под управлением ОС IOS устройствам с использованием оболочки Secure Shell. Данная книга будет полезна специалистам, работающим в области сетевых технологий, которые впервые решают задачу построения работоспособной сети, использующей мосты, коммутаторы и маршрутизаторы компании Cisco.

ПРИНЦИПЫ КОММУТАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ CISCO

Кеннеди Кларк,
Кевин Гамильтон.

www.williamspublishing.com

В книге описаны методы проектирования, применения и внедрения коммутирующих устройств в локальных сетях, а также технологии, используемые в современных территориальных сетях. Материал книги выходит далеко за рамки основных концепций коммутации и содержит примеры моделей сетей, а также описание различных стратегий поиска неисправностей. В этой книге представлены темы, которые помогут как гораздо точнее понять основные концепции коммутации, так и подготовиться к квалификационному экзамену на звание CCIE. В дополнение к обсуждению практических аспектов реализации самых современных методов коммутации, книга также содержит примеры реально существующих сетей, вопросов связанных с их внедрением и управлением, а так же практические упражнения и контрольные вопросы.

ISBN 5–8459–0464–1

в продаже

СОЗДАНИЕ СЕТЕЙ УДАЛЕННОГО ДОСТУПА CISCO

Кэтрин Пакет

www.williamspublishing.com

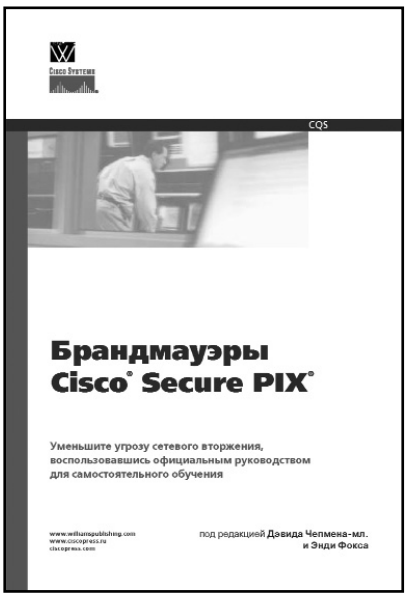
В этой книге представлена основная техническая информация о различных технологиях, используемых при организации удаленного доступа к сети предприятия. Книга основана на одноименном специализированном курсе для подготовки и сертификации специалистов и представляет собой учебник, содержащий сведения о том, как разрабатывать, настраивать, управлять и расширять сеть удаленного доступа, которая построена на основе оборудования корпорации Cisco. Данное справочное руководство может послужить как основой для изучения и внедрения современных технологий удаленного доступа, так и в качестве учебника для подготовки к сдаче сертификационных экзаменов CCNP™ и CCDP™.

ISBN 5–8459–0443–9

в продаже

БРАНДМАУЭРЫ CISCO SECURE PIX

Дэвид В. Чепмен, мл., Энди Фокс



www.williamspublishing.com

В данной книге представлена информация о семействе брандмауэров Cisco Secure PIX, а в частности о моделях 506, 515, 520, 525 и 535. На основе этих брандмауэров показана настройка механизма преобразования адресов, учета, протоколирования, протокола IPSec, виртуальных частных сетей (VPN), аутентификации, а также работа со службами SNMP и DHCP. Книга представляет собой полноценную документацию по брандмауэрам Cisco Secure PIX, которая будет полезна для администраторов и специалистов по сетевым технологиям, а также, несомненно, для хакеров, на что следует обратить особое внимание. Книга может использоваться как вместе с другими книгами из серии Cisco Press для подготовки к экзаменам на получение сертификата Cisco Security Specialist 1, так и в качестве самостоятельного пособия.

в продаже

РУКОВОДСТВО ПО ПОИСКУ НЕИСПРАВНОСТЕЙ В ОБЪЕДИНЕННЫХ СЕТЯХ

Корпорация Cisco Systems, Inc. и др.

www.williamspublishing.com

Данная книга предназначена для использования в качестве основного источника информации при решении задач, связанных с устранением нарушений в работе сети. Она может применяться в качестве пособия, позволяющего быстро находить решения проблем, возникающих в процессе функционирования сети. В книге значительное внимание уделено профилактике нарушений в работе сети. В частности, описано, какие данные должны быть собраны в процессе нормальной эксплуатации сети для подготовки к устранению возможных аварийных ситуаций, и приведены рекомендации, позволяющие обеспечить бесперебойное функционирование сети.При описании процесса поиска неисправностей в каждой конкретной сетевой среде приведены основные сведения о рассматриваемой сетевой технологии. В предметном указателе даны расшифровки всех сокращений, применяемых в книге.

ISBN 5-8459-0411-0

в продаже