Майкл Палмер
Роберт Брюс Симмер

Проектирование и внедрение компьютерных сетей

УЧЕБНЫЙ КУРС

2-е издание

Протоколы, топологии и оборудование

Современные технологии локальных и глобальных сетей

Методы проектирования, интеграции и модернизации

Введение

На основе реальных ситуаций и примеров из жизни книга "Проектирование и внедрение компьютерных сетей. Учебный курс" позволит вам разобраться как с базовыми, так и с более сложными концепциями, применяемыми при создании компьютерных сетей. Вы познакомитесь с этими концепциями на практике, используя сетевые устройства и современные операционные системы Windows 2000 (Professional и Server), Windows XP Professional и Red Hat Linux 1.x. Чтобы процесс обучения был более эффективным, во всех главах книги имеется дидактический материал, позволяющий закрепить теоретический материал и проверить его в реальных условиях.

Книга содержит:

- подробные пошаговые инструкции по использованию сетевых устройств и конфигурированию сетевых возможностей операционных систем Windows 2000 (Professional и Server), Windows XP Professional и Red Hat Linux 7.x;
- обширный материал в конце главы (резюме, вопросы для повторения, учебные задачи и дополнительные задачи для групповой работы), позволяющий закрепить полученную информацию и поупражняться в ее практическом использовании;
- многочисленные блок-схемы и копии экранов для визуального представления излагаемого материала и практических заданий.

Для кого эта книга

Книга предназначена для заинтересованных людей и профессионалов в области информационных систем, желающих более подробно узнать о сетевых технологиях, в том числе о конфигурировании современных операционных систем и устройств для работы в сетях. В книге глубоко рассматриваются все сетевые концепции, включая протоколы, технологии локальных и глобальных сетей, методы реализации таких сетей в реальной жизни, телекоммуникационные системы, беспроводные сети и другие внедряемые технологии.

Структура книги

Изложение материала в книге сбалансировано, и каждая глава строится на приемах и знаниях, полученных в предыдущих главах. Ниже кратко описано содержание каждой главы.

Глава 1, "Обзор локальных и глобальных сетей", содержит базовые сведения о различных типах сетей, в ней рассматривается история развития локальных и глобальных сетей. Также вы познакомитесь с основными принципами интеграции сетевых протоколов и узнаете о подготовительных этапах проектирования сети.

В главе 2, "Взаимодействие локальных и глобальных сетей", описывается модель Open Systems Interconnection (OSI), которая является основой для] многих сетей и сетевых устройств. Также вы узнаете о топологиях локальных и глобальных сетей и методах передачи информации.

Глава 3, "Методы передачи физического сигнала", познакомит вас с коммуникационными средами и кабелями, а также со стандартами, описывающим* методы их применения. Рассматриваются высокоскоростные технологии использованием витой пары и оптоволокна, а также типы линий для построения глобальных сетей.

В главе 4, "Сетевое передающее оборудование", подробно описываются типы сетевых устройств, используемых в локальных и глобальных сетях: сетевые интерфейсы, повторители, модули множественного доступа, концентраторы мосты, маршрутизаторы, мосты-маршрутизаторы, коммутаторы, шлюзы мультиплексоры, группы каналов, модемы, серверы доступа и другие устройства. По мере знакомства с этими устройствами вы узнаете также и том, как их применять в реальных условиях.

Глава 5, "Протоколы локальных сетей", содержит исчерпывающее описание распространенных протоколов локальных сетей, включая IPX/SPX, NetBEUl AppleTalk,

TCP/IP, SNA, DLC и DNA. Каждый протокол рассматривается связи с той компьютерной операционной системой, в которой он применяется, поэтому вы получите реальное представление о том, как и почему конкретный протокол используется в сети. Также вы узнаете о методах повышения производительности сети с помощью правильного выбора протоколов.

В главе 6, "Прошлое, настоящее и будущее протокола TCP/IP", используются сведения, полученные в главе 5, однако эта глава целиком посвящена распространенному протоколу TCP/IP. В главе подробно описаны протоколы TCP, UDP и IP, а также IP-адресация. Вы познакомитесь с протоколами IPv4 и IPv6, а также со многими прикладными протоколами, входящими в стек TCP/IP.

Глава 7, "Методы передачи данных в глобальных сетях", познакомит вас с наиболее распространенными технологиями, используемыми в сетевых коммуникациях при большой удаленности узлов. В числе этих технологий X.25Ц frame relay, ISDN, SMDS, DSL, SONET и региональные сети Ethernet. Так же вы узнаете о способах использования протоколов глобальных сетей SLIP, PPP и SS7.

Глава 8, "Технологии ATM", подробно рассказывает о технологии Asynchronous Transfer Mode (ATM), применяемой в локальных и глобальных сетях. Вы познакомитесь со структурой ATM-ячейки, многоуровневых коммуникациях ATM, методах проектирования ATM-сетей и способах использования этой технологии в локальных и глобальных сетях.

В главе 9, "Технологии беспроводных сетей", вы познакомитесь с несколькими технологиями беспроводных локальных и глобальных сетей, а также с областями их применения. Вы узнаете о стандарте беспроводных сетей 802.11 и о спецификациях Bluetooth, HiperLAN и HomeRF Shared Wireless Access Protocol. Также в главе рассказывается о сетях, использующих инфракрасное излучение, волны СВЧ-диапазона и спутники Земли.

В главе 10, "Совместная передача речи, видеоизображений и данных", рассматриваются сети, в которых сочетаются технологии передачи речи, видеоизображений и данных. Вы узнаете о мультимедийных приложениях и о том, как создавать сети, в которых они могли бы работать. В главе имеется раздел, посвященный спецификации Voice over IP (передача речи по IP-сети). Так же рассказывается о том, как подготовить сети для перспективных мультимедийных приложений.

Глава 11, "Базовые принципы проектирования локальных и глобальных сетей", суммирует весь материал, изложенный в предыдущих главах, и показывает, как реализовать приобретенные знания при проектировании и реализации локальных и глобальных сетей. Также уделяется внимание структурированным кабельным системам и сетям на их основе.

Помимо перечисленных глав, в книге имеются Список аббревиатур, Глоссарий и Предметный указатель.

Особенности книги

Для того чтобы процесс обучения был более успешным, в книге имеются специальные дидактические элементы.

- Назначение главы. Каждая глава в книге начинается с подробного списка тем, которым посвящена эта глава. Этот список позволяет быстро ознакомиться с содержанием главы, а также с целями, поставленными перед учащимися.
- Иллюстрации, копии экранов и таблицы. Блок-схемы сетей, копии экранов и поясняющие иллюстрации позволяют визуально представить теоретические вопросы, концепции и принципы проектирования. Помимо этого, многие сравнительные таблицы подробно представляют как практическую, так и теоретическую информацию. Их можно также использовать для быстрого повторения материала.
- Практические задания. Для закрепления полученной информации о локальных и глобальных сетях лучше всего практически поработать с сетевыми устройствами и сетевыми операционными системами, а также создать собственные блок-схемы сети. В каждой главе имеется множество практических заданий для экспериментальной проверки полученной информации. Эти задания содержат различные упражнения, которые можно

выполнять в любое время или использовать для построения более сложных учебных проектов.

- Дополнительный материал к главе. Для закрепления материала в конце каждой главы имеются следующие разделы:

- резюме – список, содержащий краткое, но достаточно полное изложение всех тем, раскрытых в главе, который можно использовать как учебный справочник;
- основные термины – важные термины, встречавшиеся в главе и собранные в одном месте для быстрого просмотра и запоминания;
- вопросы для повторения – список вопросов, позволяющих проверить понимание наиболее важных концепций, рассмотренных в главе;
- учебные задачи – в каждом описанном случае вы выступаете как консультант, работающий в вымышленной компании, названной Network Design Consultants. Каждая задача содержит несколько требований и условий, которые позволят вам применить полученные знания в реальных ситуациях;
- дополнительные учебные задачи для групповой работы – эти задания позволят вам поработать в небольшой команде, собранной из учащихся для решения реальных задач или для глубокого изучения некоторой темы. Эти задания дают опыт работы в коллективе, т. е. в условиях которые обычно существуют во многих фирмах и корпорациях.

Графические обозначения и выделения в тексте

Там, где это показалось уместным, в книгу были добавлены дополнительные данные и упражнения, помогающие лучше понять материал глав. Служебные значки оповещают читателя о появлении в тексте дополнительной информации. Назначение этих значков объясняется ниже.

Примечание – Дополнительная полезная информация, относящаяся к описываемой теме.

Совет – Рекомендации, основанные на опыте авторов и снабжающие читателя дополнительными сведениями о способах решения конкретных проблем или советами, помогающими ориентироваться в реальных ситуациях.

Все новые термины (которые также включены в глоссарий) выделяются в тексте.

Прочтите, прежде чем начинать читать

Поскольку ваш учебный класс может быть оборудован разными операционными системами, в книге имеются практические задания для Windows 2000 Professional, Windows 2000 Server, Windows XP Professional и Red Hat Linux 7.x. Вы можете использовать эти операционные системы в любых сочетаниях. Интерфейсы для этих систем нужно настроить следующим образом:

- в Windows 2000 (Professional и Server) работайте с графическим пользовательским интерфейсом, заданным по умолчанию;
- для Windows XP Professional используйте новый графический интерфейс (стиль) Windows XP, а на панели управления — вид Category View (По категориям) (не применяйте стиль Windows Classical и вид панели управления Classic View);
- в Red Hat Linux 7.x используйте рабочий стол X Window GNOME.

Во многих практических заданиях предусмотрены развернутые ответы на вопросы, поэтому авторы рекомендуют учащимся завести лабораторный журнал или текстовый файл, в который будут заноситься эти ответы или полученные сведения. Периодически преподаватели могут интересоваться успехами учащихся и просматривать записи в журналах или файлах.

Помимо упомянутых операционных систем, для выполнения практических заданий требуются следующие компоненты, программы и оборудование:

- лаборатория с компьютерами, объединенными в сеть;

- рабочие станции, имеющие веб-браузеры для доступа к Интернету;
- графические пакеты (например, VISIO, Smart Draw, AutoCAD или Microsoft Paint);
- сеть Ethernet или Token Ring, в которой можно изучать устройства и способы их использования;
- сеть на базе протокола TCP/IP;
- сетевой концентратор или коммутатор и сетевой кабель;
- образцы "тонкого" коаксиального кабеля, витой пары и оптоволоконного кабеля;
- компоненты и материалы, из которых изготавливаются кабели на основе витой пары и коаксиальные кабели (установите на кабели коннекторы);
- примеры различных сетевых устройств для изучения (или возможность увидеть такие устройства на экскурсии);
- доступ к сети кампуса или местной компании, которая имеет соединения с глобальными сетями.

Благодарности

Написание книги является весьма увлекательным занятием, поскольку позволяет поработать со многими замечательными людьми. Мы благодарны Уилу Питкину, редактору по работе с авторами, за его интерес и предложение о выпуске второго издания этой книги. Лора Хильдебранд, управляющая выпуском, сопровождала процесс создания этой книги от начала до конца и приложила значительные усилия и свой опыт, превратив авторский текст в законченный переплетенный том. Джил Батистик, наш научный редактор, внесла неоценимый вклад по переработке исходного материала B; организованный и хорошо понятный текст. Кроме того, она поддерживала нас и дала множество ценных советов. И, наконец, мы благодарим Дейва Джорджа, который любезно замещал Джил Батистик во время ее отпуска.

Приносим наши благодарности рецензентам Энди Уиверу и Келли Каудл, а также выпускающим редакторам Бруку Буту и Мелисе Панагос. Возглавляемая Николь Эштон группа по качеству в составе Криса Шривера и Кристиана Кунчив обеспечила качественную проверку текста и практических заданий.

Посвящение

Я посвящаю эту книгу Эдварду Палмеру — замечательному брату, другу человеку.

Майкл Палмер

Глава 1

Обзор локальных и глобальных сетей

По прочтении этой главы и после выполнения практических заданий вы сможете:

- разбираться в определениях и идентифицировать различные типы сетей;
- рассказать об истории развития локальных и глобальных сетей;
- обсуждать вопросы интеграции локальных и глобальных сетей, включая основные принципы работы мостов, маршрутизаторов, шлюзов и коммутаторов;
- описать методы интеграции сетевых протоколов;
- рассказать о предварительных этапах процесса проектирования сети.

Компьютерные информационные сети играют в нашей жизни самые разные роли, позволяя решать как бытовые задачи, так и серьезные проблемы. Каждый день с их помощью мы можем обмениваться сообщениями электронной почты, узнавать последние новости, скачивать программное обеспечение и совершать коммерческие операции. В более ответственных случаях с помощью сетей можно находить жизненно важную информацию, например, необходимую для медиков, спасателей или транспортных служб, а также оперативно передавать срочные и нужные документы.

Задачи общения людей и идеи информационных сетей отражают многовековую потребность людей в средствах коммуникации. В VII веке до нашей эры древние греки использовали приручeнных голубей для организации простейшей службы доставки сообщений. Спустя много лет, в 1819 году, Ханс Эрстед (Hans Oersted) обнаружил, что проволока, через которую пропускается электрический ток, отклоняет намагниченную стрелку, что послужило основой для создания сетей проволочного телеграфа. В настоящее время компьютерные информационные сети доступны миллионам людей, находящимся в разных уголках нашей планеты.
В этой главе вы познакомитесь с основными сетевыми терминами и концепциями, используемыми в книге. Также вы узнаете об истории возникновения и эволюции технологий локальных и глобальных сетей. И, наконец, в главе будет рассказано о способах объединения информационных сетей малого и большого радиуса действия, а также о подходах к проектированию сетей.

Виды сетей. Основные понятия

Простейшей "сетью" является речевой обмен, при котором слова передаются от одного человека к другому. Этой "технологией" люди овладевают сразу же, как только начинают говорить. Другим типом сетей, с которым люди знакомятся с детского возраста, является телефон. Два телефона отделяют друг от друга многие километры провода и разнообразное коммуникационное оборудование. Телефонные линии, связывающие дома и города, легко увидеть вдоль улиц и дорог, в то время как сотовые телефоны могут взаимодействовать через спутниковые сети.

По сути, компьютерные сети представляют собой более сложный случай тех элементов, которые лежат в основе речевых и телефонных коммуникаций. Как и при речевом диалоге, компьютерная сеть передает информацию от одного человека (или группы людей) другому. Помимо этого, как и телефонные системы, для передачи информации от одного узла к другому компьютерные сети используют коммуникационный кабель и радиоволны, при) этом специальное оборудование между узлами обеспечивает гарантированную доставку каждого сообщения.

Компьютерная сеть – это совокупность компьютеров, устройств печати, сетевых устройств и компьютерных программ, связанных между собой кабелями или радиоволнами. Большинство первых сетей передавали данные по медному проводу, а сегодня они могут обеспечивать обмен данными, речевыми и видеосигналами, используя провода, оптоволоконную среду, радио и УКВ-волны, что проиллюстрировано на рис. 1.1. Компьютерные сети развиваются со скоростью света, если сравнивать их с другими коммуникационными технологиями, такими как радио, телевидение и телефония.

Компьютерные сети, обычно классифицируемые по их радиусу действия и сложности, делятся на три группы: локальные сети, региональные сети и глобальные сети (рис. 1.2). На одном конце этой классификации находятся *локальные сети* (local area network, LAN), состоящие из связанных между собой компьютеров, принтеров и другого компьютерного оборудованиям причем все эти устройства совместно используют аппаратные и программные ресурсы, расположенные на небольшом удалении друг от друга. Радиус действия (область обслуживания) локальной сети может представлять небольшой офис, этаж здания или все здание целиком. Примером такой сети может служить химический факультет университета, в котором компьютеры, расположенные в офисах и лабораториях, соединены коммуникационным кабелем, как показано на рис. 1.3.

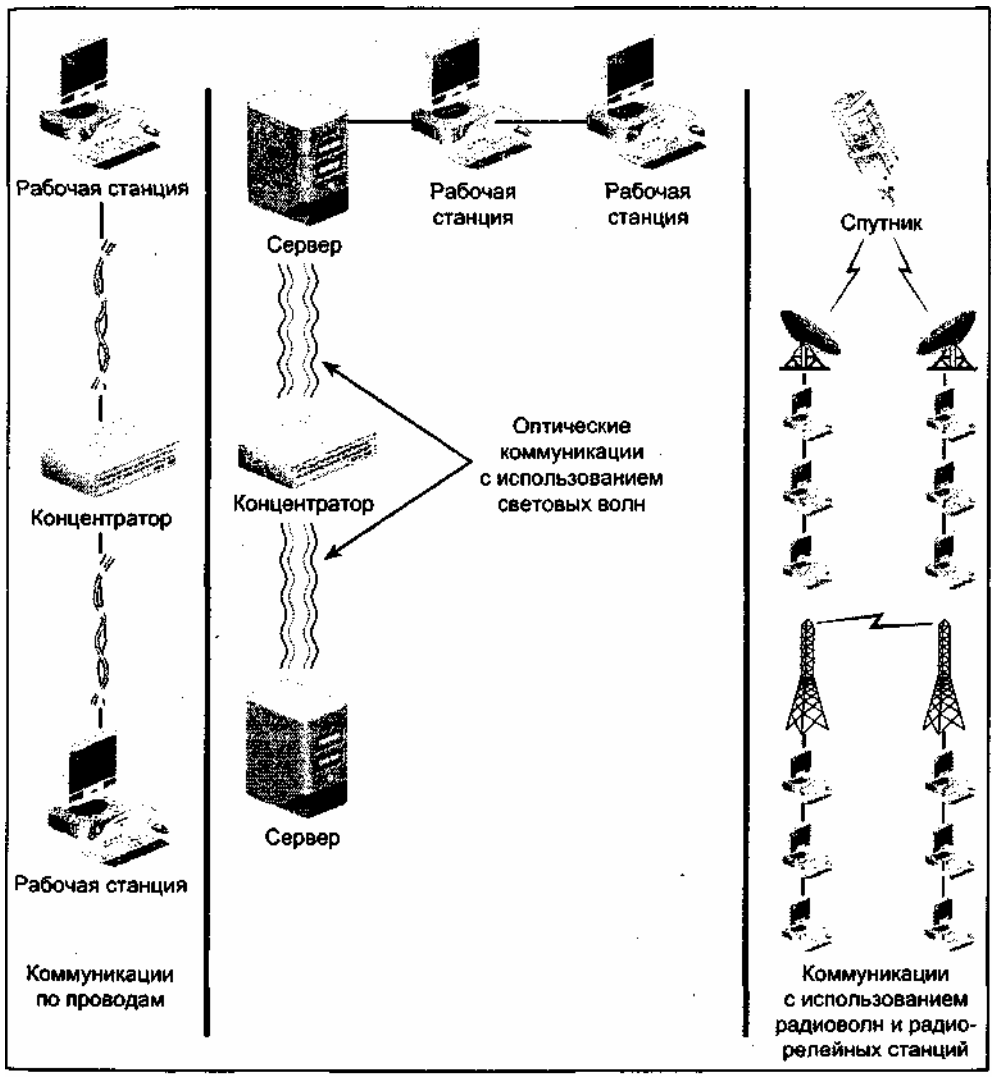


Рис. 1.1. Сетевые коммуникации с использованием кабеля, оптоволокна и радиоволн

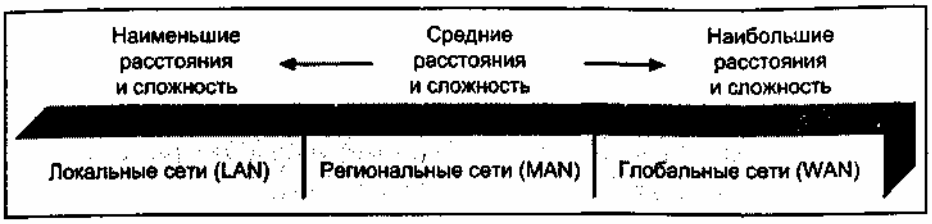


Рис. 1.2. Сравнение локальных, региональных и глобальных сетей

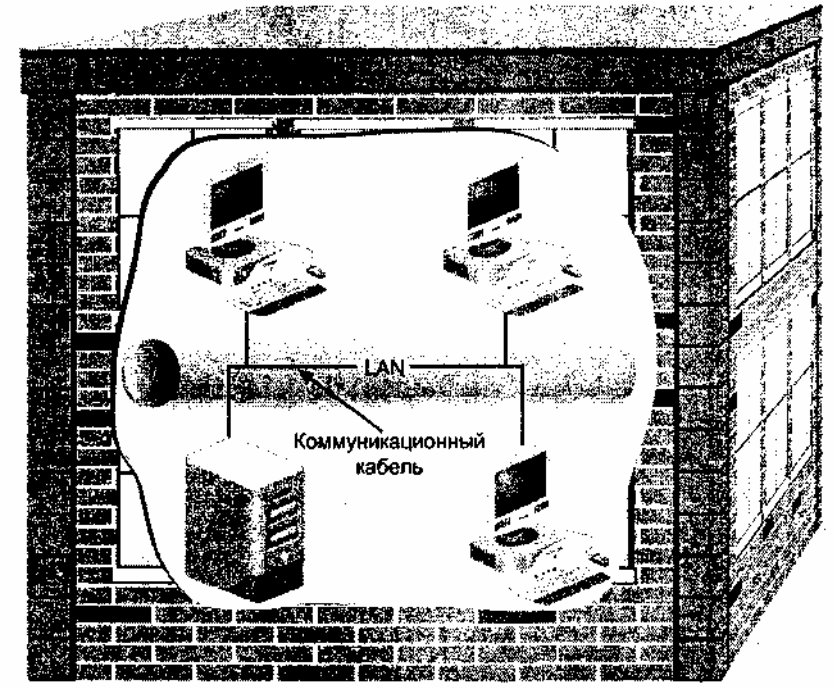


Рис. 1.3. Локальная сеть (LAN) в здании факультета

Региональная, или *городская сеть* (metropolitan area network, MAN) имеет большую область обслуживания, чем локальная сеть, и обычно в ней для обеспечения передачи данных на средние расстояния используется более сложное сетевое оборудование. Региональная сеть объединяет несколько локальных сетей, находящихся в большом городе или некотором регионе, и обычно простирается на расстояния не более 40-50 километров. Например, описанная выше локальная сеть химического факультета университета может быть связана с локальной сетью исследовательской клиники и сетью фармацевтической компании, расположенной в том же городе, что в совокупности составляет региональную сеть, показанную на рис. 1.4. Отдельные локальные сети, образующие региональную сеть, могут принадлежать как одной организации, так и нескольким различным организациям. Высокоскоростные каналы между локальными сетями в составе региональной сети обычно выполняются с использованием оптоволоконных соединений.

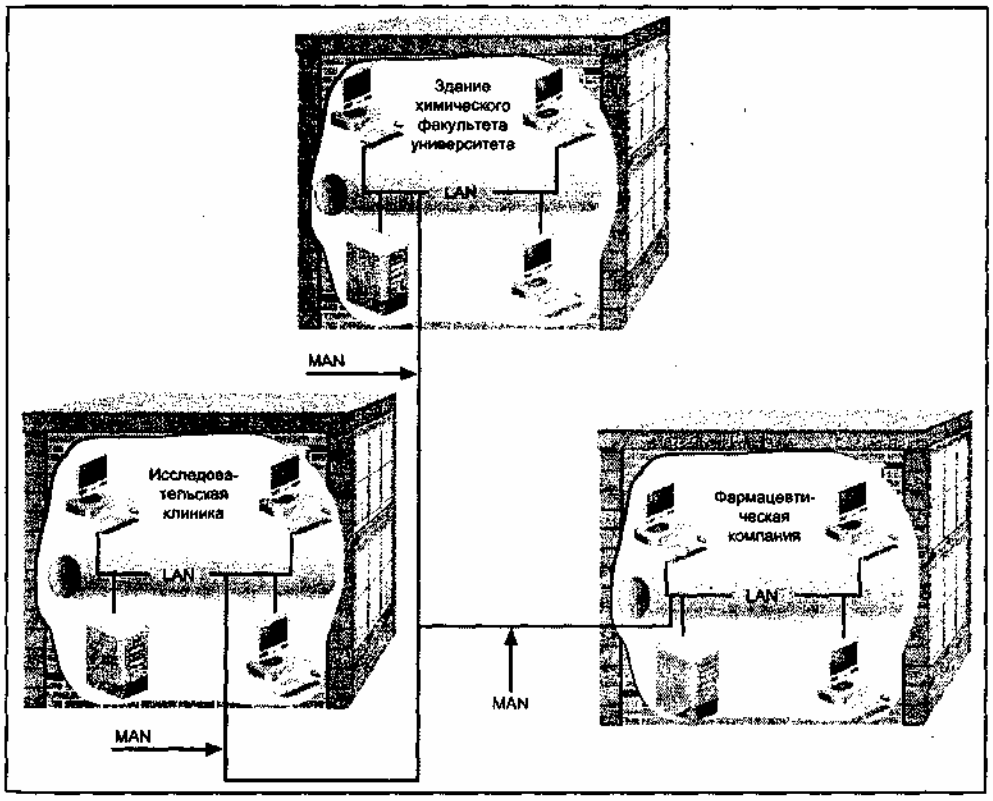


Рис. 1.4. Региональная (городская) сеть (MAN), соединяющая три здания в одном городе

Глобальная сеть (wide area network, WAN) представляет собой наивысший уровень в классификации сетей, поскольку она является крупномасштабной системой сетей, образующих единое целое со сложной структурой. Глобальная сеть образуется из нескольких локальных (или региональных) сетей, охватывающих расстояния свыше 40-50 километров. В состав крупных глобальных сетей могут входить множество локальных и региональных сетей, находящихся на разных континентах.

Совет

Примером простейшей глобальной сети может служить модемное подключение к поставщику сетевых услуг по обычным телефонным линиям. Более сложная глобальная сеть – спутниковый мост между локальными сетями, расположенными в разных странах. Самой известной всемирной глобальной сетью является *Интернет,* состоящий из тысяч локальных и региональных сетей, связанных между собой с помощью разнообразных технологий глобальных коммуникаций.

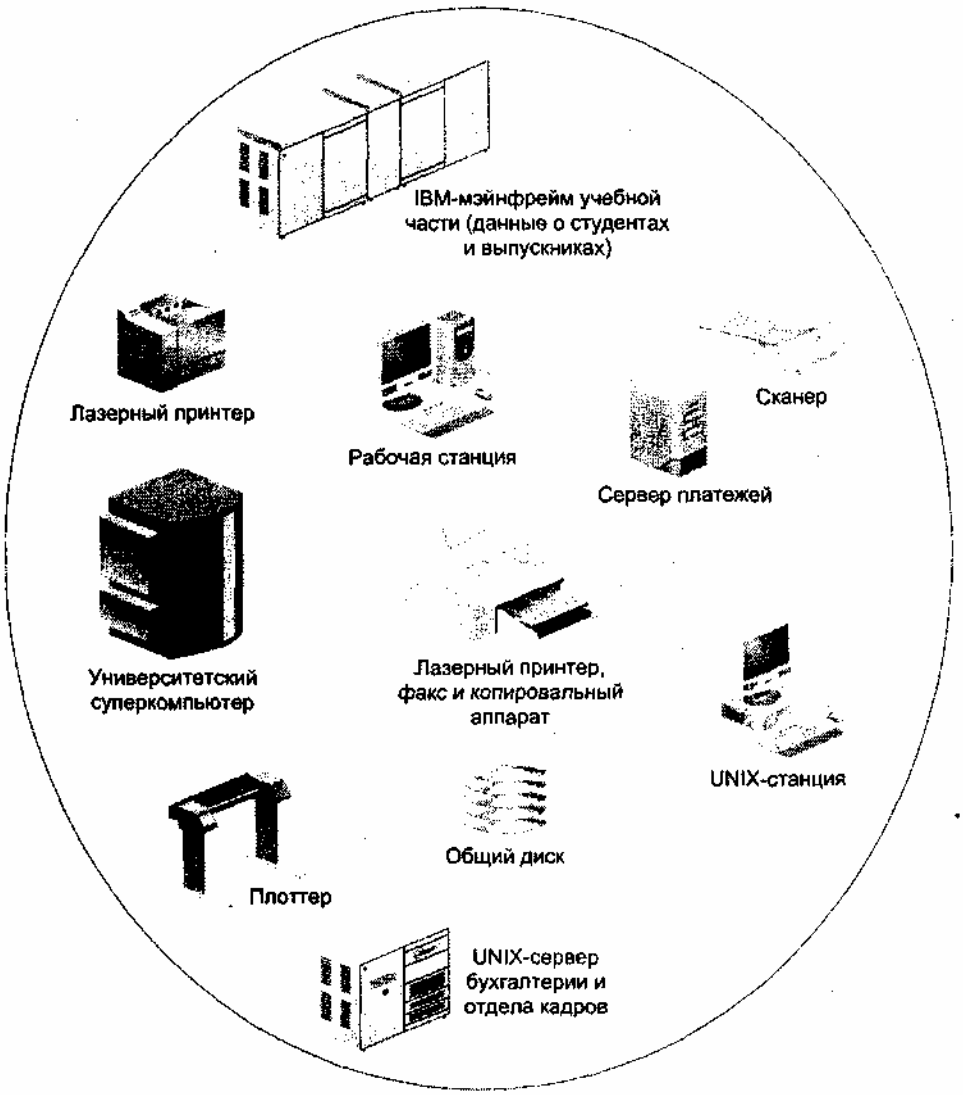


Рис. 1.5. Пример ресурсов корпоративной сети

Помимо рассмотренной классификации сетей, существует еще один тип – *корпоративная сеть.* Подобные сети объединяют различных пользователей в пределах одной или нескольких организаций и предоставляют им множество ресурсов. Несмотря на то, что большую локальную сеть можно рассматривать как корпоративную, все же корпоративная сеть обычно состоит из нескольких локальных сетей, образующих региональную или глобальную сеть.

Одной из главных характеристик корпоративной сети является наличие разных ресурсов, позволяющих пользователям решать офисные, исследовательские и образовательные задачи. Примером корпоративной сети может служить университет, объединяющий в своем составе самые различные службы, представленные на рис. 1.5, и имеющий в локальной сети множество различных компьютеров и устройств печати. В практическом задании 1-1 вы познакомитесь с ресурсами, имеющимися *в* корпоративной сети университетского кампуса.

Определение типа сети

Иногда различия между локальными, региональными и глобальными сетями (или границы между рабочей группой или корпоративной сетью) являются размытыми, бывает трудно определить, где заканчивается одна сеть и начинается другая. Однако тип сети чаще всего можно определить по результатам анализа следующих четырех сетевых характеристик:

- коммуникационная среда;
- протокол;
- топология;
- тип использования сети (частная или общедоступная).

Рассмотрим первую характеристику. В качестве коммуникационной среды может выступать токопроводящий кабель, оптоволокно, радио или УКВ-волны. С ее помощью компьютеры и сети соединяются между собой. Нередко локальная сеть может заканчиваться там, где одна передающая среда меняется на другую (например, обычный кабель переходит в оптоволоконный). Часто отдельные локальные сети на основе медных кабелей с помощью оптоволоконного кабеля подключаются к другим локальным сетям, образуя глобальную сеть. В других случаях граница сети может пролегать там, где происходит переход от оптоволокна к УКВ-волнам.

Перейдем ко второй характеристике. Границу локальных и глобальных сетей можно определить по типу используемых протоколов. *Протокол* определяет способ форматирования сетевых данных в виде пакетов или фреймов, а также методы передачи каждого блока данных и способы интерпретации Данных на принимающем узле. *Пакет* — это модуль данных, имеющий определенный формат, пригодный для передачи информации по сети в виде некоторого сигнала.

В сетевых коммуникациях каждый пакет состоит из двоичных разрядов, располагающихся в информационных полях, представляющих команды управления обменов, адреса источника и назначения, полезные данные и контрольные суммы для обнаружения ошибок. Пакеты соответствуют сетевой информации, передаваемой на Сетевом уровне (Уровне 3) эталонной модели OSI (Open Systems Interconnection), который определяет выбор маршрута, по которому пакет следует к узлу назначения. Подробнее этот уровень рассматривается в *главе 2.*

Иногда информационные поля в модуле данных, передаваемом по сети, не содержат сведений о маршрутизации, поскольку соответствующий протокол или устройство функционируют на Канальном уровне *(см. главу 2).* В этом случае подобный модуль данных называется не пакетом, а *фреймом.*

Примечание

Среди специалистов по сетям существует разногласие по поводу точных определений терминов "пакет" и "фрейм". Некоторые не делают различия между этими понятиями, однако многие специалисты соглашаются с тем, что фреймы представляют информацию, используемую на Уровне 2 модели OSI, а пакеты относятся к Уровню 3 модели OSI.

Обратите внимание на то, что в одной локальной сети могут существовать несколько протоколов, однако границу сетей определяет только изменение типа используемых протоколов или увеличение их количества. Например, для сетей Ethernet используется один протокол, а для сети с маркерным кольцом — другой; подробнее об этом рассказывается в *главе 2.* Такие сети можно объединить, однако на границе сетей необходимо поместить устройства, преобразующие фреймы или пакеты Ethernet во фреймы или пакеты маркерного кольца, и наоборот.

Третьей характеристикой, позволяющей определить границы сетей, является *топология.* Сетевая топология имеет две составляющих: физическую разводку кабеля и логические маршруты, по которым следуют пакеты или фреймы, передаваемые по сетевому кабелю. Разводка кабеля определяется реальным расположением кабеля в коробах на потолке и стенах. Логический маршрут соответствует направлению передачи пакетов или фреймов, и это направление может как соответствовать, так и не соответствовать физической разводке.

Рассмотрим пример, когда физическая конфигурация сети совпадает с логической. Физическая разводка может иметь звездообразную форму, при этом в центре звезды располагается сетевое устройство. Логические маршруты могут соответствовать звездообразной конфигурации, когда пакеты и фреймы передаются всем конечным узлам одновременно. Это напоминает одновременное зажигание всех лампочек в иллюминации.

Описанную топологию можно изменить и посылать фреймы и пакеты в некоторой логической последовательности (притом, что физическая разводка по-прежнему представляет собой звезду). Фреймы или пакеты могут поступать сначала одному узлу, а потом другому. Такая конфигурация будет напоминать "бегущий огонь" в иллюминации, когда лампочки зажигаются поочередно.

Изменения топологии определяются изменениями физической конфигурации и/или логических маршрутов. Например, пакеты и фреймы в сети могут физически перемещаться в шинной

топологии, имеющей конечные точки, а затем через некоторое сетевое устройство могут подключаться к топологии, где они будут передаваться по кольцу, у которого конечные точки отсутствуют.

Четвертой характеристикой, определяющей границы сетей, является тип их использования; например, граница проходит там, где заканчивается частная сеть и начинается сеть общего пользования, или наоборот. *Частная сеть* принадлежит одной организации и поддерживается ею; примером может служить университетская сеть, которой управляет один из колледжей. *Общедоступной* называется такая сеть, которая предлагает свои услуги всем членам некоторого сообщества (например, сеть, поддерживаемая телекоммуникационной компанией или компанией кабельного телевидения).

Для понимания классификации деления сетей по типу использования рассмотрим пример некоторой компании, имеющей локальные сети в трех своих подразделениях, связанных между собой через региональную телефонную службу. Граница между частными локальными сетями и общедоступной глобальной сетью будет проходить там, где локальные сети подключаются к региональной телефонной сети. В другом случае компания может предложить своим сотрудникам *виртуальную частную сеть* (virtual private network, VPN), передающую данные через Интернет и позволяющую им обращаться к конфиденциальным данным и файлам так, будто они работают в сети из дома, используя компьютер и модем. VPN – это частная сеть, функционирующая как туннель через большую сеть (такую как Интернет или корпоративная сеть), и доступная только для авторизованных клиентов. Границы сетей будут рассматриваться при выполнении практических заданий 1-2, 1-3 и 1-4.

Совет

Понимание границ между сетями может быть чрезвычайно важно при разработке мер безопасности, поскольку, например, для защиты сети от вторжения или вирусов вы можете поместить сетевые устройства в некоторые или во все точки пересечения этих границ.

Причины, обусловившие появление локальных и глобальных сетей

История и развитие сетевых технологий отражают запросы общества, которое нуждается в быстрых средствах связи, используемых в деловой сфере, образовании, для развлечений и взаимного общения. Несмотря на появление все новых и новых, более совершенных коммуникаций, основные требования к ним остаются одними и теми же необходимо иметь простые и быстрые средства взаимодействия со многими людьми, находящимися в разных точках. В 1800 году требовались месяцы на то, чтобы передавать новости или пересылать продукцию между США и Европой. Сегодня можно в течение минуты переслать сообщение по электронной почте из Висконсина в Норвегию, после чего компания в Атланте сможет через Интернет послать разнарядку в компанию, расположенную в Торонто, которая после этого обработает заявку и отпустит товар прямо в этот же день.

Два последующих раздела описывают наиболее значимые события в истории компьютерных сетей. Некоторые сведения взяты из хронологии Роберта Закона "Hobbes' Internet Timeline" (Hobbes[1] Internet Timeline Copyright! (c) 1993-2003 by Robert H Zakon); ее можно найти в Интернете по адресу **http://www.zakon.org/robert/internet/timeline/.** Хронологию событий можно также найти в *запросе на комментарии* (Request for Comments, RFC) RFC 2235.»

Примечание

Запрос на комментарии (RFC) — это некоторый документ, подготовленный и распространенный одним человеком или группой людей с целью продвижения идей по развитию сетей, Интернета и компьютерных коммуникаций. Каждый RFC имеет уникальный номер. После того как некоторый RFC получает широкое одобрение в компьютерном и сетевом сообществе, он зачастую принимается в качестве стандарта. В настоящее время документами RFC управляет Проблемная группа проектирования Интернета (Internet Engineering Task Force, IETF). Это международная организация, участвующая в подготовке стандартов для Интернета. Документы RFC призваны укрепить

взаимодействие между равноправными разработчиками, и играют значительную роль в продвижении сетевых технологий.

В процессе чтения хронологии событий вы увидите, что в ней представлена не просто технологические открытия, а последовательность взаимосвязанных, социальных, политических и научных событий, отражающих человеческую потребность в более быстрых коммуникациях. Первый раздел описывает историю событий, которые постепенно привели к изобретению локальных глобальных сетей, а второй непосредственно охватывает этапы их развития. Эта хронология весьма наглядно показывает, насколько быстро сокращались интервалы между следующими друг за другом достижениями.

Хронология основных событий, предшествующих появлению компьютерных сетей

1819

Ханс Эрстед (Hans Oersted) пропускает электрический ток по проволоке для того, чтобы отклонить намагниченную иглу, открывая тем самым путь изобретению телеграфа.

1837

Сэмьюэль Морзе (Samuel F.B. Morse) в США, а также Чарльз Уитстоун (Charles Wheatstone) и Уильям Кук (William Cooke) в Англии, изобретают электрический телеграф. Уитстоун и Кук патентуют телеграф в Англии и используют его для передачи информации на железных дорогах.

1844

Морзе посылает телеграмму с текстом "What hath God wrought!" ("Как сотворил Господь!") из Балтимора в Вашингтон. Морзе использует код, состоящий из коротких и длинных импульсов, которые представляют собой буквы и слова. Этот код был назван азбукой Морзе и явился основой для повсеместно применяемого ныне международного кода Морзе (International Morse Code).

1858

Канада и Ирландия делают первые попытки передачи сигналов через Атлантический океан по подводному кабелю. Из-за сильных фоновых шумов и относительно слабого 600-вольтового сигнала за несколько часов можно передать лишь несколько слов. После усиления сигнала до 2000 вольт плавится изоляция кабеля, что делает его непригодным к использованию.

1860

Компания Pony Express начинает доставку почты между штатами Калифорния и Миссури, при этом каждая поездка длится 10 дней и требует усилий 80 ездовых.

1861

В октябре компания Pony Express выполняет последний почтовый рейс, будучи не в силах конкурировать со скоростью передачи нового телеграфного оборудования фирмы Pacific Telegraph Company.

1876

Александр Белл (Alexander Graham Bell) Создает первую телефонную систему, состоящую из передатчика и приемника, подключенных к проводу. Качество передаваемого сигнала достаточно для того, чтобы ассистент Белла услышал сообщение "Мистер Уотсон, идите сюда, я жду вас".

1877

Первый коммерческий телефон введен в эксплуатацию банкиром Росвеллом Даунером (Roswell Downer), который установил связь на расстоянии трех миль между своим домом и офисом в банке. В том же году E. T. Holmes (Холмс) конструирует первый телефонный коммутатор, соединивший завод и четыре банка в Бостоне. Поскольку Холмс был производителем охранных сигнализаций, коммутатор по ночам работал так же как банковская сигнализация.

1906

Ли Дефорест (Lee Deforest) изобрел вакуумную лампу-триод и использовал ее для усиления тока.

1915

Исследователи компании AT&T осуществили первый трансконтинентальный телефонный звонок между Нью-Йорком и Сан-Франциско. Эта компания также начинает исследования по трансатлантическим передачам голоса
по радио.
i

1927

Компания AT&T открывает коммерческую трансатлантическую телефонную связь с Лондоном. Звонки стоят 75 долларов за 5 минут.

1937

Алекс Ривз (Alex Reeves) разрабатывает метод дискретизации голосового сигнала, названный импульсно-кодовой модуляцией (Pulse Code Modulation, PCM), этот метод впоследствии применяется в телефонных сетях в США. ИКМ-модуляция для передачи голоса использует 8-разрядную схему кодирования, являющуюся предшественницей методов кодирования данных, созданных в 1960-х годах. На основе ИКМ-модуляции реализуется базовый коммуникационный канал, являющийся основой для разработки метода высокоскоростной передачи сигналов с уплотнением каналов, который ныне известен как 24-канальная ИКМ-система типа T (T-carrier).

1939

Получив грант в размере 7000 долларов, Джон Атанасов (John Atanasoff) и, Клиффорд Бэрри (Clifford Berry) из Университета штата Айова изобретают электронный цифровой компьютер, названный в их честь – Atanasoff-Berry Computer.

1945

Ванневар Буш (Vannevar Bush), советник по науке президента Рузвельта во время Второй мировой войны, разрабатывает компьютер Метех, способный хранить большие объемы информации.

1946

Первый электронный цифровой компьютер появился на свет благодаря усилиям Эккерта (J. Presper Eckert) и Мошли (John W Mauchly), и команды разработчиков из Школы инженеров-электротехников имени Мура Университета штата Пенсильвания. Их компьютер, названный Electronic Numerical Integrator and Computer (ENIAC) (Электронный цифровой интегратор и вычислитель), состоял из 18 000 электронных ламп и занимал площадь, равную 1500 квадратным футам (приблизительно 135 кв. м).

1947

Джон Бардин (John Bardeen), Уолтер Братейн (Walter Brattain) и Уильям Шокли (William Shockley) из лаборатории Bell Labs изобрели транзистор. Их открытие принесло им Нобелевскую премию по физике 1956 года.

1956

Проложен первый успешно работающий трансатлантический кабель, TAT1, и компания IBM создала первый накопитель на жестком диске. Привод имел размеры двух холодильников и запоминал 5 Мбайт данных при стоимости хранения 10 000 долларов за мегабайт.

1957

Советский Союз запустил в космос первый искусственный спутник Земли (Sputnik). Обеспокоенные отставанием в области науки и для обеспечения своего лидерства, США в составе Министерства обороны (Department of Defense, DoD) образуют Управление перспективных исследовательских программ (Advanced Research Projects Agency, ARPA). В последующие годы это

управление играет важную роль в развитии сетевых технологий.

1958

Открывая путь для оптоволоконных коммуникационных средств, лаборатория Bell Labs разрабатывает первый лазер (laser, Light Amplification by Stimulated Emission of Radiation – усиление света посредством принудительного генерирования излучения). Джек Килби (Jack Kilby) из Texas Instrument демонстрирует первую интегральную схему (ИС), состоящую из шести транзисторов на кремниевой подложке размером с ноготь.

1960

США запускают первый спутник связи, названный Echo ("Эхо"). В этом же году Иозеф Ликлидер (Joseph Licklider) публикует книгу "Man-Computer Symbiosis" ("Симбиоз человека и компьютера"), которая предвосхищает появление "консолей домашних компьютеров". Также в 1960 году усовершенствуются методы кодирования для передачи данных, что создает почву для разработки 8-разрядного кода для отдельных символов, например, букв и цифр. В 1960-х годах также входят в обиход электронно-лучевые трубки (ЭЛТ – Cathode Ray Tube, CRT), используемые в мониторах для интерактивной работы с компьютерными системами.

1961

Леонард Клайнрок (Leonard Kleinrock) из Массачусетского технологического института (Massachusetts Institute of Technology, MIT) публикует первую статью по сетям с коммутацией пакетов - "Information Flow in Large Communication Nets" ("Информационные потоки в больших коммуникационных сетях").

1962

Компания AT&T запускает на орбиту вокруг Земли первый коммерческий спутник связи – Telstar I. Также в 1962 году компания IBM создает стандарт кодирования, известный как *Extended Binary Coded Decimal Interchange Code (EBCDIC)* (Расширенный двоично-десятичный код обмена информацией) и определяющий 256 различных 8-разрядных символов.

1963

В качестве альтернативы коду EBCDIC разрабатывается другой метод кодирования символов, названный *American Standard Code for Information Interchange (ASCII)* (Американский стандартный код обмена информацией). Код ASCII i содержит 96 заглавных и строчных символов и цифр, а также 32 непечатных символа. Также в 1963 году Дуг Энгельбарт (Doug Engelbart) изобретает компьютерную мышь.

1964

Гордон Мур (Gordon Moore) предсказывает удвоение производительности компьютеров каждые 18 месяцев, и это предсказание в целом оправдывается до сих пор. Позже, в 1968 году, Мур становится одним из основателей компании Intel. Компания Digital Equipment Corporation (DEC) создает первую серийную мини-ЭВМ – PDP-8. Поль Бэрэн (Paul Baran) из компаний RAND Corporation публикует основополагающую статью по сетям с коммутацией пакетов, названную "On Distributed Communications Networks" ("О распределенных коммуникационных сетях").

История локальных и глобальных сетей

1965

Томас Меррил (Thomas Merrill) и Лоуренс Роберте (Lawrence Roberts) создают первую глобальную сеть между Массачусетским технологическим инстатутом и компанией System Development Coiporation (SDC). Тед Нельсон (Ted Nelson) впервые использует термин "гипертекст".

1966

Исследователи впервые используют волоконную оптику для передачи телефонных сигналов. Дональд Дэйвис (Donald Davies) применяет термины "пакеты" и "коммутация пакетов" при описании метода использования нескольких цепей (маршрутов) для передачи пакетов. Боб Тейлор (Bob Teylor), сотрудник ARPA, получает средства на создание экспериментальной сети между несколькими университетами США, и этот проект через три года развития получает имя *Advanced Research Projects Agency Network (ARPANET)*.

1967

На конференции исследователей ARPA Уэс Кларк (Wes Clark) предлагает идею использования специализированных аппаратных средств для выполнения сетевых функций. Позднее эти устройства были названы "интеллектуальными процессорами сообщений" (Interface Message Processors, IPM). В этом же году Лоуренс Роберте публикует первый проектный документ по ARPANET — "Multiple Computer Networks and Intercomputer Communications" ("Межкомпьютерные сети и коммуникации").

1968

Национальная исследовательская лаборатория Великобритании (National Research Laboratory, NRL) испытывает первую глобальную сеть, использующую коммутацию пакетов. В августе управление ARPA распространяет среди производителей коммерческие предложения на реализацию ARPANET. IBM и другие крупные компании отказываются их рассматривать, поскольку не верят в возможность создания сетей такого типа. Контракт получает небольшая консалтинговая фирма Bolt Beranek and Newman (BBN), расположенная в Кэмбридже, штат Массачусетс. Фирма получает менее года времени и 1 миллион долларов на создание работающей сети. Кен Томпсон (Ken Thompson) и Дэннис Ритчи (Dennis Ritchie) из AT&T Bell Labs разрабатывают операционную систему UNIX, которая впоследствии становится одной из основных серверных операционных систем, используемых в информационных сетях.

1969

Производители телефонного оборудования просят у компании AT&T разрешения на подключение к ее телефонной сети устройств сторонних разработчиков. Федеральная комиссия связи США (Federal Communications Commission, FCC) решает, что телекоммуникационные устройства независимых производителей могут использоваться, если эти устройства не нарушают работу телефонной сети. Решение комиссии открывает путь на рынок телекоммуникационного оборудования производителям модемов и компаниям, выпускающим средства передачи данных.

Первый прототип интеллектуального процессора сообщений (IMP), модификация компьютера Honeywell 516, был создан компанией Honeywell и передан фирме BBN. Этот прототип, названный IMP 0, функционировал неправильно, на повторный монтаж потребовалось несколько недель. Также в этом году Стивом Крокером (Steve Crocker) был написан первый запрос на комментарий (Request for Comment, RFC), озаглавленный "Host Software" ("Программное обеспечение хоста"). (Вы можете прочесть текст этого RFC в практическом задании 1-5.) RFC 1 описывает интерфейс между IMP-устройствами и хост-компьютерами.

В это время хосты представляют собой мини-ЭВМ, доступные через сеть. (В структуре сети *хост* (host) является узлом сети: это компьютер или сетевое устройство, имеющее уникальный собственный адрес.) Каждая вычислительная система, входящая в ARPANET, отвечает за создание базового программного обеспечения для подключения своих компьютеров к IMP-J устройствам сети ARPANET.

В сентябре сетевые инженеры фирмы BBN устанавливают первый 1MP-узел ARPANET в Калифорнийском Университете Лос-Анжелеса (UCLA), и этот узел без проблем стыкуется с университетским компьютером Sigma-7. В октябре в Стэндфордском исследовательском институте (SRI) создают второй узел, который подключают к своему компьютеру SDS 940. После некоторых настроек оба вновь созданных узла ARPANET оказываются связанными меж собой каналом со скоростью передачи свыше 50 Кбит/с. В ноябре Калифорнийский Университет в Санта-Барбаре (UCSB) становится третьим узлом сети, а Университет штата Юта в декабре создает четвертый узел.

1970

Норманн Абрахамсон (Norman Abrahamson) из Университета штата Гавайи на средства ARPA создает сеть ALOHAnet, которая передает данные со скоростью не быстрее 4,8 Кбит/с, однако создает основу для популярного транспортного сетевого протокола *Ethernet.* Кроме этого, главный офис фирмы BBN становится пятым узлом ARPANET. Протокол, используемый хост-компьютерами для подключения к ARPANET, называется Network Control Protocol (NCP) (Протокол управления сетью). Его не нужно путать I совершенно другим протоколом — NetWare Control Protocol, который также имеет аббревиатуру NCP.

1971

Сеть ARPANET охватывает 15 вычислительных систем и в общей сложности 23 хост-компьютера в следующих организациях: UCLA, SRI, Университет штата Юта, UCSB, MIT, BBN, RAND Corporation, System Development Corporation, Lincoln Lab, Стэнфорд, Гарвард, Университет штата Иллинойс, центр NASA в Эймсе (Ames), Case Western Reserve University и Central Michigan University. Дневной сетевой трафик достигает 700 000 пакетов. Кроме того, RFC 172 определяет спецификацию протокола передачи файлов File Transfer Protocol (FTP).

1972

Рей Томлинсон (Ray Tomlinson) из BBN создает электронную почту, которая вскоре становится самой популярной программой в сети ARPANET. Также, Ион Постел (Jon Postel) в FRC 318 предлагает сетевую *эмуляцию терминала* (terminal emulation) при помощи прикладного протокола Telnet. Позднее в этом же году Боб Канн (Bob Kahn) демонстрирует сетевое взаимодействие 40 компьютеров по сети ARPANET на Международной конференции по компьютерным коммуникациям, а для создания стандартов ARPANET и сетей образуется Inter-Networking Group (INWG).

1973

Английский University College of London и норвежская организация Royal Radar Establishment реализуют первое международное подключение к ARPANET. К этому моменту ARPANET передает более трех миллионов пакетов в день. В марте Винтон Серф (Vinton Cerf) создает эскизный проект шлюза, а в мае Роберт Меткалф (Robert M. Metcalfe) предлагает применение Ethernet-коммуникаций как тему своей докторской диссертации в Гарварде. Позднее Меткалф и Дейвид Боггс (David Boggs) создали первую сетевую операционную систему с использованием протокола Ethernet, имеющую скорость передачи около трех миллионов бит в секунду. Экспериментальные компьютеры в их сети назывались Michelson и Morley – в честь ученых XIX века, доказавших, что эфир не существует[1]. Шестью годами позже Меткалф стал основателем компании 3Com Corporation, производящей сетевые устройства.

[1]Эфир – ether; Ethernet - "эфирная сеть", сеть с использованием эфира

1974

Серийное цифровое оборудование и устройства, выпускаемые компанией Dataphone Digital Service (DDS), подталкивают фирму Bell Systems к переходу от аналоговых телекоммуникационных сетей к цифровым. Винтон Серф и Боб Канн в своей статье "A Protocol for Packet Network Internetworking" ("Протокол для взаимодействия пакетных сетей") предлагают протокол Transmission Control Protocol (TCP) и впервые используют термин "Internet".

1975

Ответственность за регулярное функционирование сети ARPANET перекладывается на Управление связи Министерства обороны США (Defense Communications Agency), которое отныне называется Агентством по оборонным информационным системам (Defence Information System Agency). Кроме того, компания Northen Telecom выпускает первый цифровой телефонный коммутатор, названный SL-1.

1976

Идея коммутации получает признание специалистов по компьютерным сетям, благодаря работе Леонарда Клейрока (Leonard Kleinrock) "Queuing Systems Volume II – Computer Applications" ("Системы массового обслуживания, Том 2 – Компьютерные приложения"). Также создается новый протокол для общедоступных сетей с коммутацией пакетов, названный X.25; к концу 1970-х годов этот протокол получает широкое распространение в открытых сетях Tymnet и Telenet.

1977

Компания Tymshare развертывает общедоступную сеть Tymnet. Позже в этом же году к сети ARPANET подключается первый шлюз беспроводной связи. Эта система передает пакеты с помощью радиоволн, используя технологию, называемую "пакетной радиосвязью" и применяемую до настоящего времени.

1978

Винтон Серф, Стив Крокер и Дэнни Коэн (Danny Cohen) начинают разрабатывать протокол Internet Protocol (IP). Он предлагается как средство маршрутизации, отдельное от TCP. В последующие годы протоколы TCP и IP становятся жизненно важными компонентами коммуникаций Интернета. В этом же году в Массачусетском технологическом институте демонстрируется первый гипермедиа-видеодиск.

1979

Организуется Internet Configuration Control Board (ICCB) (Совет по управлению структурой Интернета), работа которого направлена на проблемы сетевых шлюзов. Том Траскот (Tom Truscott), Стив Белловин (Steve Bellovin) и Джим Эллис (Jim Ellis) создают сеть USENET, связывающую Университет Дюка (Duke University) и Университет штата Северная Каролина. Также в конце 1970-х годов интегральные микросхемы (integrated circuits, 1C) применяются во всех типах электронных устройств. Создаются сложные кристаллы, использующие интеграцию высокого (large scale integration, LSI) и сверхвысокого (very large scale integration, VLSI) уровней (БИС и СБИС). БИС и СБИС прокладывают путь более быстрым и дешевым цифровым устройствам, таким как компьютеры и компьютерные терминалы, после чего открывается дверь для появления персональных компьютеров.

1981

Аира Фукс (Ira Fucks) и Грейдон Фриман (Greydon Freeman) создают академическую сеть Because It's Time NETwork[2] (BITNET), соединившую Городской Университет Нью-Йорка и Йельский Университет. К концу 1989 года сеть BITNET является обширным и успешно работающим объединением колледжей и университетов всех районов США. В этом же году рыночная стоимость Personal Computer (PC) фирмы IBM снижается до 4500 долларов, и этот продукт пользуется неожиданным успехом. Компания Microsoft разрабатывает версию MS-DOS, названную PC DOS, что означает "операционная система, используемая на IBM PC". Кроме того, 1981 год отмечен как начало быстрого развития технологии модемов для коммутируемых линий передачи.

[2]Это название можно перевести как "Потому что время работать в сети!"

1982

Протоколы TCP и IP принимаются как основной набор протоколов для ARPANET. Для использования в военных целях в США начинает работу сеть Defense Data Network, впоследствии названная Milnet (Military Network) (Военная сеть). На Национальной компьютерной конференции в июне Дрю Мэйжер (Drew Major), Кэйл Пауэл и Дейл Нейбор представляют первую локальную сеть персональных компьютеров, используя при этом программное обеспечение, явившееся основой для сетевой операционной системы Novell NetWare.

1983

ARPANET становится по-настоящему общедоступной сетью, в то время как сеть Milnet развивается своим путем и ориентируется на использование в военных целях. Разделение

этих сетей знаменует появление Интернета. В сети ARPANET протокол NCP заменяется на TCP/IP, а система Berkeley UNIX начинает поддерживать TCP/IP. Количество хостов, подключенных к ARPANET, достигает 500.

1984

К Интернету подключено свыше 1000 хостов, и в романе Уильяма Гибсона (William Gibson) "Neuromancer"[3] появляется термин "киберпространство". Разукрупнение компании AT&T Bell Systems стимулирует новые телекоммуникационные компании усилить конкурентную борьбу на рынке коммерческих коммуникаций. Особенно острая конкуренция в области высокоскоростных технологий, что приводит к появлению ИКМ-систем типа T, работающих на скорости 1,544 Мбит/с.

[3] Можно перевести как "Нейромант".

1986

Число хостов Интернета превышает 5000. Национальный научный фонд США (National Science Foundation) выделяет средства на создание пяти университетских суперкомпьютерных центров, расположенных в разных частях США. Эти центры соединяются каналами 56 Кбит/с в рамках новой сети NSFNET. Суперкомпьютеры и NSFNET открывают возможность выполнения широкомасштабных исследовательских проектов для множества колледжей и университетов США, уже подключенных к сетям, таким как BITNET и Интернет.

1987

Интернет соединяет свыше 10 000 хост-компьютеров. Компания Apple Computer выпускает на рынок первую систему для создания гипермедиа, что означает начало эры авторских средств для настольных компьютеров и продуктов мультимедиа. Управление сетями является предметом интересов Джефа Кейса (Jeff Case), Марка Федора (Mark Fedor), Мартина Шофстала (Martin Schoffstall) и Джеймса Дейвина (James Davin), которые создают протокол Simple Gateway Monitoring Protocol (SGMP) (Простой протокол управления шлюзом), впоследствии интегрированный со стеком TCP/IP и названный Simple Network Management Protocol (SNMP) (Простой протокол сетевого управления). По стечению обстоятельств первая демонстрация протокола SGMP срывается из-за широкомасштабной аварии Интернета, что подчеркивает важность сетевого управления.

1988

Число хостов Интернета превышает 60 000, и сеть NSFNET работает со скоростью 1,544 Мбит/с, что увеличивает трафик в этой сети до 75 миллионов пакетов в день. В этом же году Европа и Северная Америка соединяются первым трансатлантическим оптоволоконным кабелем, способным одновременно передавать 40 000 телефонных звонков. Internet Worm, первый вирус, созданный Робертом Моррисом младшим (Robert Morris Jr.) специально для Интернета, поражает около 10 процентов интернет-хостов.

1989

Еще 40 000 хостов подключается к Интернету, что в конечном результате дает цифру 100 000. Тим Бернерз Ли (Tim Berners-Lee) распространяет среди интернет-сообщества первый проект "всемирной паутины" – сети World Wide Web. К концу 1980-х годов локальные сети распространены повсеместно, обеспечивая передачу данных как в отдельных помещениях, так и в целых зданиях. Пользователи компьютеров осознают тот факт, что они могут в любой точке обращаться к любым ресурсам – компьютерам, принтерам и глобальным сетям, таким как Интернет, и что они получили в свое распоряжение феноменальные технологические и программные технологии. Новое сетевое оборудование во все возрастающей степени способно расширить область обслуживания локальных сетей и увеличить скорость передачи данных. Хосты Интернета и сетей перемещаются с мэйнфреймов на небольшие рабочие станции и персональные компьютеры, поскольку распространяются сетевые операционные системы UNIX и NetWare.

1990

Сеть ARPANET, вытесненная Интернетом, официально прекращает существование. В общедоступных телефонных сетях в качестве протокола цифровой коммутации внедряется Signaling System 7 (SS7), которая обеспечивает работу нескольких абонентских служб и позволяет быстро локализовать проблемы в телефонных сетях, а также перестраивать сетевые маршруты. США и Швеция среди первых реализуют SS7 в телекоммуникациях, используя новую технологию, названную сигнализацией по общему каналу (common channel signalling) и позволившую использовать в сочетании с телекоммуникационными серверами следующие возможности:

- ✓ динамическую переадресацию вызова, проведение телеконференций и ожидание вызова;
- ✓ автоматический повторный вызов и обратный звонок;
- ✓ несколько телефонных адресов по одной активной телефонной линии;
- ✓ голосовую почту;
- ✓ идентификатор абонента (caller ID);
- ✓ речевой набор номера;
- ✓ переадресацию при необходимости вызова служб "800", что необходимо при чрезмерной нагрузке.

1990 год знаменует начало десятилетия разработки технологий быстрых локальных и глобальных сетевых коммуникаций. Одиннадцать стран становятся новыми членами сети NSFNET.

1991

Количество хостов Интернета превышает 600 000, при этом каждый месяц включаются в работу тысячи новых хостов. Сеть NSFNET становится доступной для коммерческого использования – кардинальный шаг, изменивший характер ее применения. Теперь NSFNET работает со скоростью 44,736 Мбит/с, обеспечивая передачу 10 миллиардов пакетов за месяц. На индивидуальных хостах Интернета можно размещать службы Gopher и World Wide Web, что инициирует гонку за лидерство той или иной технологии.

1992

Имеется свыше миллиона хостов Интернета и 13 новых стран – от холодной Антарктики до жаркого Эквадора — подключаются к Интернету. Теперь пользователи по новому выражению, придуманному Жаном Армором Полли (Jean Armour Polly), занимаются "веб-серфингом" (surfing the net).

1993

Количество интернет-хостов переваливает за 2 миллиона и 17 стран из Африки, Азии, Центральной Америки и Европы становятся новыми членами сети NSFNET. Президент и вице-президент США начинают пользоваться Интернетом и получают адреса электронной почты. В начале года имеется 50 веб-серверов, к концу года их количество достигает 500. Выпускается веб-браузер Mosaic.

1994

Имеется свыше 3 миллионов хостов Интернета и к нему подключаются 20 новых стран: от Армении до Узбекистана. Скорость передачи по сети NSFNET достигает 155 Мбит/с, что позволяет за месяц передавать свыше 10 триллионов (10^{12}) пакетов. Начинает работу первый кибербанк "First Virtual", а также компания Mosaic Communications Corporation, предшественница фирмы Netscape Communications.

1995

Количество хостов Интернета равно 4 миллионам, а наибольший Интернет-трафик приходится на долю обращений к веб-ресурсам. Сеть NSFNET прекращает работу и Национальный научный фонд США преобразует ее в специализированную исследовательскую сеть, названную "very high-speed Back bone Network Service" (vBSN) (Суперскоростная магистральная сетевая служба). Национальный и международный сетевой трафик в основном создается различными

поставщиками услуг, называемыми провайдерами Интернета (Internet service provider, ISP); совокупность провайдеров, пользователей и хостов рассматривается как "Интернет".

1996

В Интернете *9* миллионов хостов, подключаются 30 новых стран, телекоммуникационная компания MCI достигает скорости передачи, равной 622 Мбит/с.

Закон о телекоммуникациях (Telecommunications Act) от 1996 года поддерживает развитие новых интерактивных коммуникационных функций, включая сетевые операции по телевизионным кабелям и кабелям связи.

1997

Количество хостов в Интернете превысило 16 миллионов, 20 новых стран подключилось к Интернету.

1998

Трафик в Интернете удваивается каждые 100 дней, значительно расширяется использование Интернета в бизнесе. Свыше 10 миллионов человек в США и Канаде вовлечены в Интернет-бизнес, покупая авиабилеты, книги, аппаратуру и домашнюю технику, компьютеры и автомобили. Также в 1998 году поставщики сетевого оборудования начали широко предлагать 1-гигабитные коммуникационные устройства.

1999

Академическая и исследовательская сеть Internet2 начинает охватывать университетские сети в Европе и США. В Интернете создан первый полноценный банк, базирующийся в штате Индиана и предлагающий весь спектр услуг. Для ускорения сетевого взаимодействия фрагменты интернет-магистрали США начинают передачу данных со скоростью 2,5 Гбит/с. *Магистраль* (backbone) состоит из высокопроизводительных коммуникационных каналов, объединяющих сети в одном здании, в пределах кампуса или на больших расстояниях.

Кроме того, законодательство США закрепляет право собственности за доменными именами.

2000

Для магистральных каналов сети Internet2 используется новая версия протокола IP – IPv6. Европейские страны определяют основу для реализации новой межгосударственной гигабитной сети, названной Geant. Кроме того, многие новые сети позволяют просматривать по Интернету видеоклипы, а множество радиостанций вещает через Интернет.

2001

Поставщики предлагают 10-гигабитные сетевые коммуникационные устройства. Кроме этого, дается толчок развитию беспроводной телекоммуникации. Некоторые компании (например, Microsoft) реализуют в своих кампусах широкополосные беспроводные сети. Многие радиостанции прекращают вещание через Интернет из-за юридических проблем с отчислениями за использование интеллектуальной собственности (в данном случае — музыки). Высшие школы (университеты) в США получают доступ к исследовательской и академической сети Internet2.

Выполнив практические задания 1-6 и 1-7, вы узнаете больше об истории компьютерных сетей.

2002

Утверждение стандартов на 10-гигабитные сети откладывается, поскольку соответствующим уполномоченным организациям необходимо переписать процедуры тестирования таких сетей, а полное тестирование оказалось сложнее, чем предполагалось изначально. Тем не менее, цены на 1-гигабитные устройства значительно упали, т. к. на рынок вышло много производителей, включая новые компании. Усовершенствования в 1-гигабитных средствах передачи данных, осуществляемых по обычным медным проводам, позволили использовать эту передающую среду во многих существующих сетях. Кроме того, основные компании, выпускающие кредитные карты,

развернули свои сети и информационные центры в Европе, на Дальнем Востоке и в Латинской Америке, что стимулировало более широкое использование протокола TCP/IP в сетевой среде этих районов.

Интеграция локальных и глобальных сетей

С 1960-х и до начала 1980-х годов процедура передачи цифровых данных подразумевала непосредственное подключение неинтеллектуальных (без своего центрального процессора) терминалов к мэйнфреймам и мини-ЭВМ с использованием протокола *Systems Network Architecture (SNA)* компании IBM. На рис. 1.6 изображена простая сеть, в которой терминалы непосредственно подключены к мэйнфрейму через шлюз SNA (шлюзы будут рассматриваться в *данной главе* позже). В настоящее время SNA является проверенным традиционным методом коммуникаций, однако с началом распространения локальных сетей в 1982 году пользователи персональных компьютеров и рабочих станций применяют для сетевого подключения к мэйнфреймам как протокол SNA, так и более совершенные методы доступа. Кроме того, хотя мэйнфреймы могли одновременно выполнять множество задач, в настоящее время серверы меньшей мощности, такие как файловые серверы, серверы приложений, баз данных и электронной почты, выполняют те же задачи. Устаревший метод непосредственного подключения к мэйнфреймам почти повсеместно заменен сетями, которые позволяют соединяться с любыми устройствами, в число которых входят следующие:

- ✓ серверы;
- ✓ мэйнфреймы и мини-ЭВМ;
- ✓ равноправные компьютеры, например, рабочие станции, работающие под управлением операционных систем Windows XP или UNIX;
- ✓ дисковые устройства централизованного хранения данных;
- ✓ массивы приводов CD-ROM;
- ✓ принтеры;
- ✓ факсимильные аппараты.

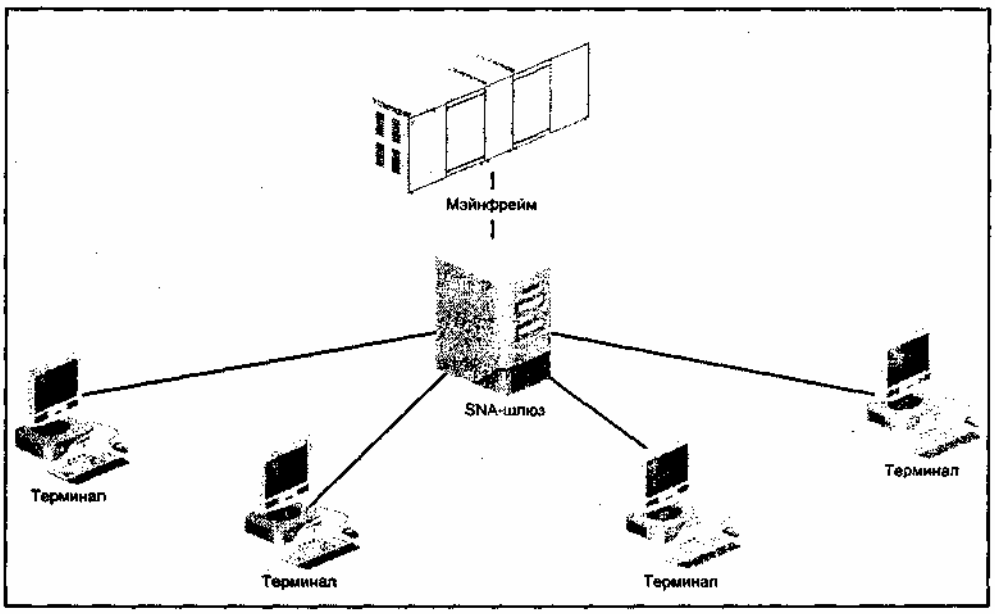


Рис. 1.6. Использование протокола SNA для непосредственного подключения к компьютеру без использования сети

Компьютерные сети также позволяют реализовать *клиент-серверные вычисления,* при которых вычислительные мощности распределяются между серверами и клиентскими рабочими станциями. Такой тип обработки данных позволяет объединить мощности новых настольных персональных компьютеров и специализированных серверов, которые не всегда превосходят по параметрам эти настольные компьютеры. Мэйнфреймы по-прежнему позволяют компаниям сохранять их средства,

вложенные в программное обеспечение 10-20-летней давности, в то время как клиент-серверные системы поддерживают самые современные технологии обработки данных, позволяя при этом использовать графический пользовательский интерфейс (GUI) и новые возможности обращения к базам данных. Оба типа организации вычислительных мощностей сосуществуют в локальных и глобальных сетях, чтобы пользователи могли работать с жизненно важными программами и данными.

Дальнейшим развитием клиент-серверных систем является архитектура .NET, разработанная компанией Microsoft. Она взаимодействует с Интернетом и предназначена для такой интеграции данных и пользовательских функций, чтобы их выполнение могло осуществляться в любой точке и на многих типах устройств, включая карманные компьютеры и сотовые телефоны. Кроме того, архитектура .NET позволяет объединять различные языки программирования и использовать их для построения крупномасштабных приложений. Например, некоторая компания может применять существующий, давно проверенный программный код и объединять его с новым кодом, который может использоваться веб-сервером, отдельным персональным компьютером или устройством с перьевым вводом. С внедрением архитектуры .NET граница между настольными компьютерами и серверами становится менее заметной, поскольку настольные компьютеры могут, в принципе, выполнять те же роли в совместном использовании данных и ресурсов, которые имеются у существующих серверных систем.

Каждый день растут требования к комплексным сетям, которые могли бы связать организации, находящиеся в разных странах или на разных континентах. Перед сетевыми администраторами ставится множество задач, в т. ч. подключение к различным локальным и глобальным сетям, обеспечение деятельности надомных сотрудников, развертывание служб мультимедиа, а также поддержка старых и новых компьютеров в пределах одной сети. Другой важнейшей задачей является увеличение пропускной способности магистральных каналов локальных и глобальных сетей с целью удовлетворения потребностей возросшего сетевого трафика.

Построение локальных, региональных, глобальных и корпоративных сетей возможно благодаря использованию сетевых устройств, позволяющих расширять область охвата сети, связывать сети воедино, преобразовывать протоколы, а также направлять фреймы и пакеты в нужные сети, т. е. выполнять все операции по *межсетевому обмену* (internetworking). Несмотря на наличие большого количества типов сетевых устройств, имеются четыре группы устройств, играющих основную роль при объединении сетей:

- ✓ мосты;
- ✓ маршрутизаторы;
- ✓ шлюзы;
- ✓ коммутаторы.

Мосты (bridge) — это сетевые устройства, которые позволяют удлинить локальную сеть или объединить несколько локальных сетей, соединяя таким образом многочисленные рабочие станции, серверы и другие сетевые устройства, которые иначе не смогли бы взаимодействовать. Как показано на рис. 1.7, мосты могут соединять две или несколько локальных сетей, использующих один и тот же протокол.

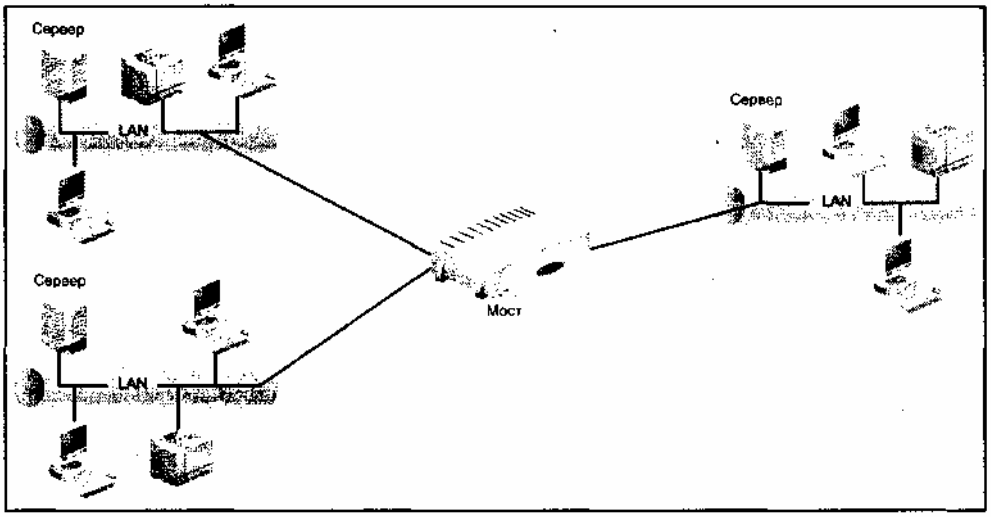


Рис. 1.7. Мост, связывающий локальные сети

Сетевые администраторы также применяют мосты для разбиения локальной сети на небольшие подсети с целью повышения производительности, при этом можно распределять сетевой трафик, локализовать сетевые проблемы и управлять доступом к каждой подсети. Для решения этих задач мосты проверяют адреса принимающих и передающих устройств в тех фреймах, которые на них поступают, и, используя соответствующее программное обеспечение, определяют – передавать фрейм дальше или отбросить его. Также мосты могут соединять разные локальные сети, в которых применяются различные типы передающей среды. Например, они могут подключать кабель к оптоволокну или УКВ-оборудованию и, следовательно, могут использоваться для связи локальной сети с глобальной.

Маршрутизаторы (router) — это устройства межсетевого обмена, работающие на более высоком уровне сетевого взаимодействия по сравнению с мостами. Как показано на рис. 1.8, они позволяют локальным и глобальным сетям направлять (маршрутизировать) данные в указанные места назначения.

Маршрутизаторы соединяют сети, которые могут использовать различные протоколы, и обеспечивают больше коммуникационных функций, чем мосты. Например, маршрутизаторы могут определять кратчайший путь между двумя компьютерами, разделенными локальной или глобальной сетями. Они также могут устанавливать разные сетевые маршруты, соответствующие типу передаваемых данных (например, для видеоданных может выбираться маршрут с высокой стоимостью, а для символьной информации – с низкой).

Маршрутизаторы регулярно взаимодействуют друг с другом и динамически изменяют информацию о сетевых маршрутах по мере того, как меняется топология сети или условия передачи информации.

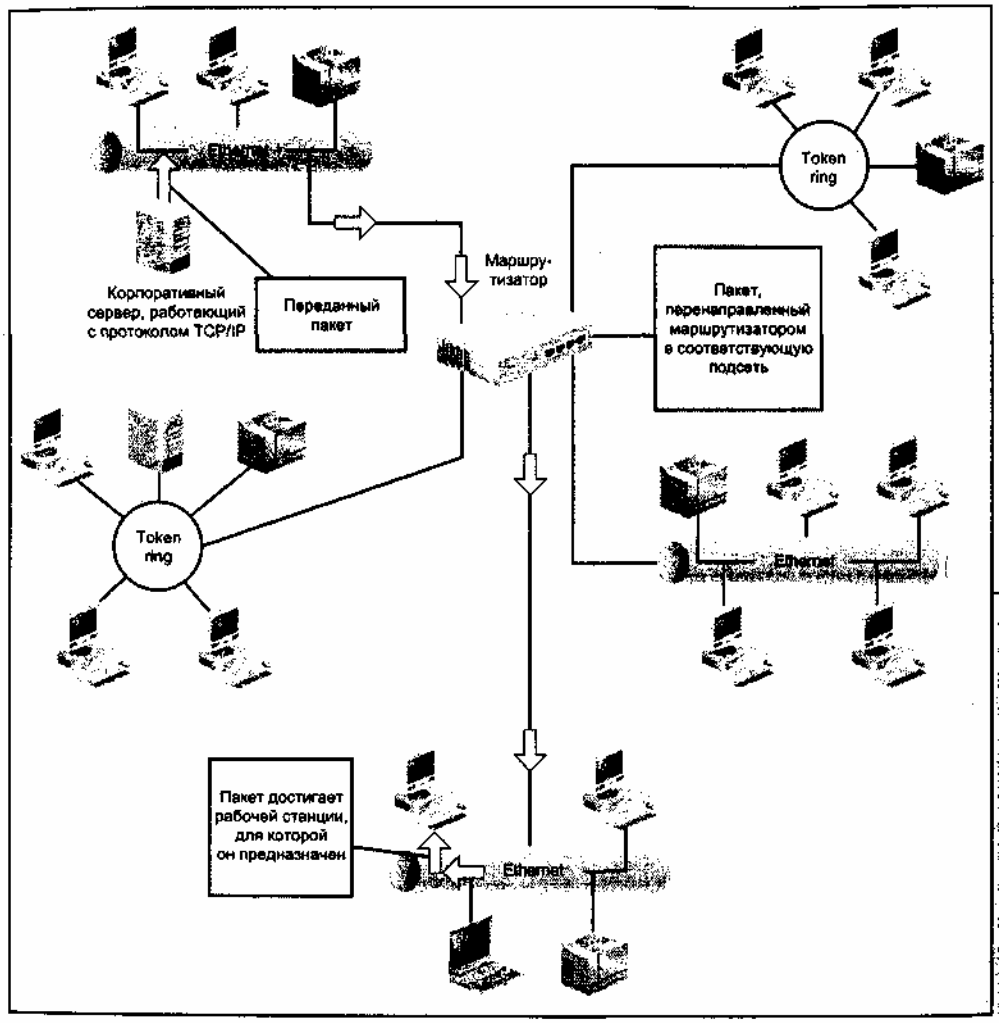


Рис. 1.8. Маршрутизатор, управляющий передачей пакетов

Примечание

Маршрутизатор может быть специализированным устройством или компьютером с программным обеспечением, выполняющим функции маршрутизации. Например, в качестве маршрутизатора может использоваться компьютер под управлением операционных систем NetWare, Windows 2000, Windows Server 2003 или UNIX. Практические задания 1-8 и 1-9 демонстрируют настройку опций маршрутизации в системах Windows 2000 и Server Red Hat Linux 7.2.

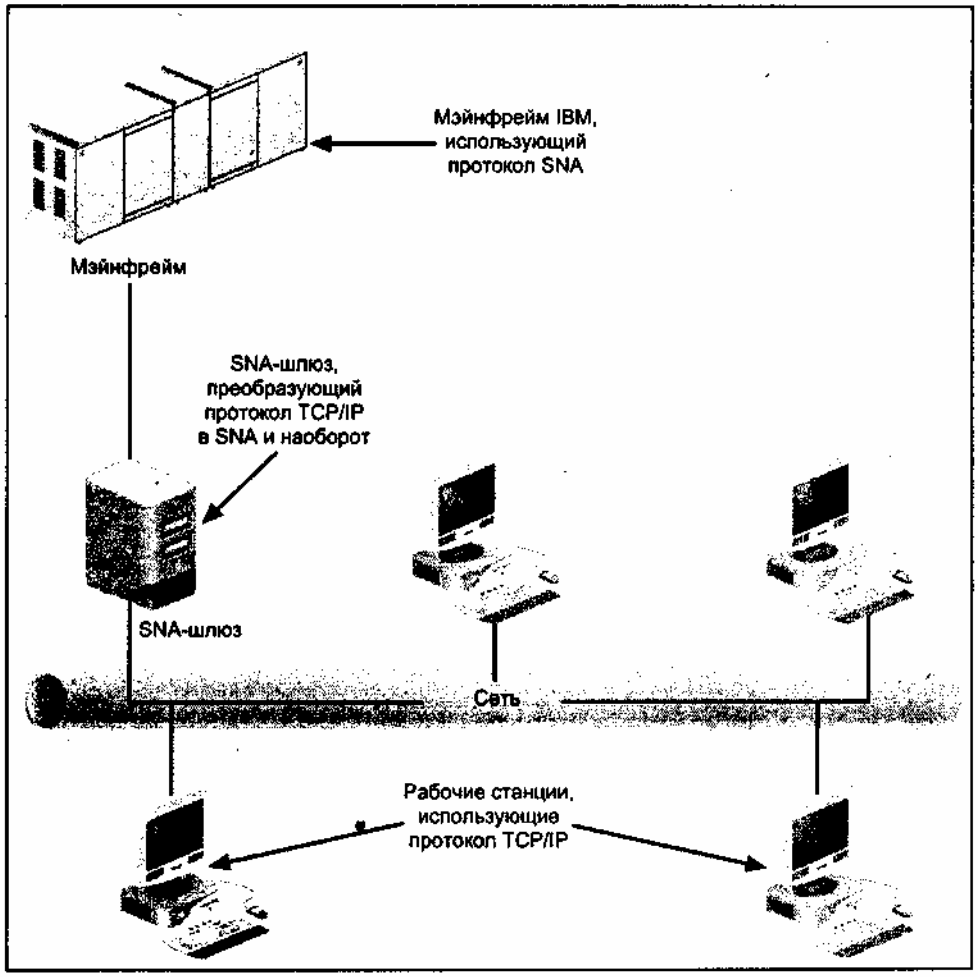


Рис. 1.9. Шлюз, преобразующий протоколы между рабочими станциями и мэйнфреймом фирмы IBM, к которому эти станции обращаются

Шлюз (gateway) представляет собой сетевое устройство, обеспечивающее взаимодействие между различными устройствами, системами или протоколами, и которое может работать на любом уровне сетевого обмена в зависимости от заданных ему функций. Чаще всего шлюзы используются для преобразования протоколов. Подобное преобразование может потребоваться при передаче данных из одной локальной сети в другую или из локальной сети в глобальную. Некоторые шлюзы позволяют сетевым компьютерам обращаться к мэйнфрейму, находящемуся в той же локальной сети или подключаться к глобальной сети для передачи информации на большие расстояния. Например, как показано на рис. 1.9, компьютеры в локальной сети могут взаимодействовать с мэйнфреймом IBM через шлюз SNA, подключенный к той же сети. Другие шлюзы предназначены для обработки межсетевых пакетов, генерируемых специальным программным обеспечением, например, сообщений электронной почты. Поскольку обычно шлюзы выполняют очень ограниченное количество специализированных функций, то они используются реже, чем маршрутизаторы и мосты.

Примечание

Подобно маршрутизаторам шлюзы могут быть автономными устройствами или службами операционной системы. Например, компьютер под управлением IBM AIX можно сконфигурировать как шлюз SNA, или же сервер Windows 2000 с установленным протоколом TCP/IP может работать как шлюз к серверу NetWare, использующему протокол IPX/SPX. Практическое задание 1-10 рассказывает о том, как настроить систему Windows 2000 Server в качестве шлюза NetWare.

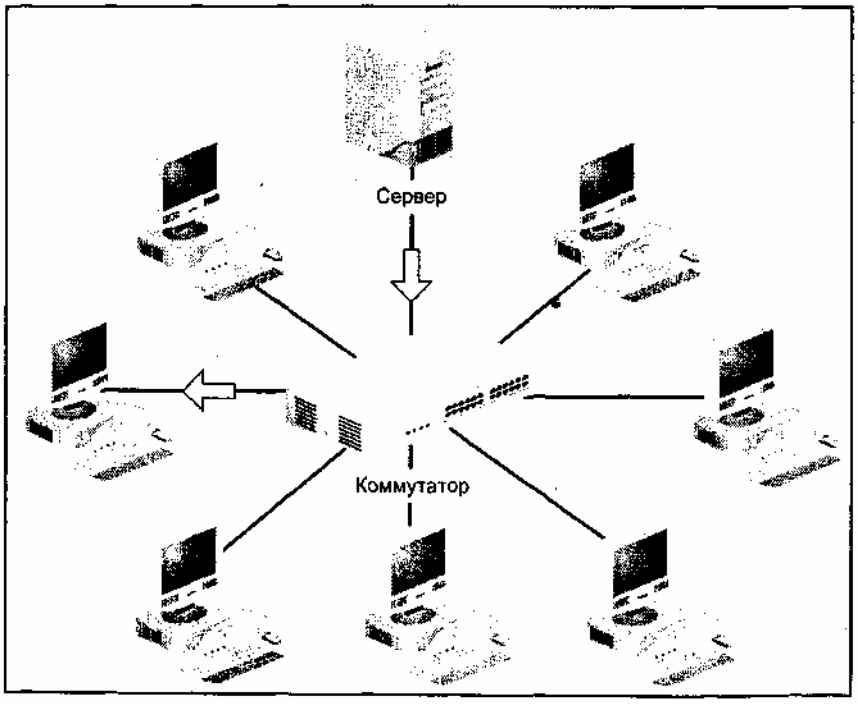


Рис. 1.10. Коммутатор в действии

Первоначально *коммутаторы* (switch) предназначались для выполнения функций мостов (2-й уровень модели OSI), обеспечивающих более высокую производительность, чем обычные мосты. Это достигалось за счет того, что коммутаторы могут передавать данные непосредственно в заданный сетевой порт или сегмент. В настоящее время коммутаторы некоторых производителей имеют возможности, близкие к возможностям маршрутизаторов (3-й уровень модели OSI), поскольку они анализируют адреса протокола IP и на основе этого анализа посылают сетевые пакеты по указанному маршруту. Другие коммутаторы могут определять назначение передаваемой информации в зависимости от того, какая прикладная программа ее генерирует. На рис. 1.10 проиллюстрирована работа коммутатора. Мосты, маршрутизаторы, шлюзы и коммутаторы более подробно будут описаны в последующих главах этой книги.

Передача данных между локальными и глобальными сетями

При реализации некоторых типов взаимодействия между сетями выполняется процедура, называемая *трансляцией* (translation). При трансляции фрейм или пакет преобразуется из одного формата в другой (например, все фреймы или пакеты могут "выравниваться" по длине, независимо от протокола). Другим средством трансляции является специально разработанное устройство, называемое *транслирующим мостом.* Такой мост анализирует адресную и управляющую информацию во всех фреймах и преобразует ее в соответствии с требованиями подключенных к нему локальных или глобальных сетей.

Инкапсуляция — еще один способ передачи данных между сетями разного типа или передачи нескольких протоколов с помощью одного протокола через различные сети. При инкапсуляции фрейм или пакет данных сети одного типа помещается в заголовок фрейма или пакета, применяемого в сети другого типа. При таком подходе новый заголовок выполняет функции почтового конверта для посланного письма, обеспечивая его соответствующей адресной и управляющей информацией, необходимой для того, чтобы послание достигло пункта назначения. В зависимости от их назначения, инкапсуляцию фреймов или пакетов выполняют сами компьютеры или сетевые устройства. Например, инкапсуляция используется для того, чтобы передать фрейм или пакет от одной локальной сети Microsoft или Novell – через Интернет – другой локальной сети аналогичного типа.

Новейшая технология трансляции между сетями называется *эмуляцией локальной сети* (LAN Emulation, LANE) и применяется в некоторых высокоскоростных локальных и глобальных сетях. При эмуляции локальной сети фреймы или пакеты сети одного типа форматируются так, чтобы они выглядели как

модули данных, передаваемые в сети другого типа. Для этого изменяется управляющая информация в заголовке, и включаются дополнительные разряды. Одним из важнейших достоинств данной технологии является: то, что эмулирующее программное обеспечение находится в некотором сетевом устройстве доступа, которое "прозрачно" для отдельного клиента независимо от того, какие программы или операционные системы тот использует.

Введение в проектирование сетей

Процесс проектирования локальных и глобальных сетей начинается с шагов, которые описываются в разных главах этой книги. Сначала нужно понять работу сетей с точки зрения протоколов, методов доступа и топологий. Например, проектирование сети Ethernet зачастую отличается от методов, проектирования, применяемых для создания сетей с маркерным кольцом. Аналогичным образом, проектирование глобальных сетей на основе телекоммуникационных каналов проводится иначе, нежели для спутниковых глобальных сетей.

Другим шагом в процессе проектирования сети является знакомство с физическими устройствами, применяемыми в локальных и глобальных сетях., Сюда входят и коммуникационная среда (например, оптоволоконный ка-1 бель), и сетевые устройства, такие как маршрутизаторы и коммутаторы. При правильном проектировании необходимо учитывать детали: нужно, к примеру, знать, какая передающая среда используется в магистралях, а какая — для подключения настольных компьютеров. Изучение характеристик различных коммуникационных сред и устройств позволит вам спроектировать сеть самым эффективным образом.

Третий шаг — понимание основных принципов проектирования сетей: знакомство с методами применения структурированных кабельных систем, технологией создания сетей для мультимедийных клиент-серверных приложений, преимуществами тех или иных характеристик устройств, применяемых в локальных и глобальных сетях. Например, во многих случаях производительность сети повышается, если вместо моста или простейшего концентратора использовать методы коммутации. Кроме этого, с помощью маршрутизатора можно создать брандмауэр, защищающий сеть, или обеспечить повышение скорости передачи мультимедийных данных.

Четвертым шагом в процессе проектирования сети является определение факторов, влияющих на архитектуру сети выбранного предприятия. В частности, для этого следует получить ответы на следующие вопросы.

- Какие компьютеры имеются и где они расположены?
- Какое программное обеспечение существует и какие сетевые ресурсы нужны для работы этих приложений?
- Какие бизнес-правила применяются на предприятии и как для их реализации используется сеть?
- Как распределяются периоды максимальной и минимальной загрузки сети предприятия?
- Какими средствами должна обладать сеть для облегчения процесса поиска и устранения неисправностей?
- Какие средства безопасности требуются для сети?
- Каковы перспективы роста предприятия и в какой мере (в чем) они могут повлиять на использование сетевых ресурсов?

Резюме

- Локальные, региональные и глобальные сети — три основных типа компьютерных сетей. Главным их отличием друг от друга является область обслуживания, а затем – протоколы и топологии, используемые для построения сети. Термины "локальная сеть" и "глобальная сеть" в первую очередь относятся, соответственно, к небольшим самостоятельным сетям и к крупномасштабным сетям, их соединяющим. Соотношение между локальными и

глобальными сетями напоминает подключение небольшой учрежденческой телефонной станции к крупной телекоммуникационной системе. С другой стороны, сеть можно рассматривать как совокупность корпоративных ресурсов, в число которых входят компьютеры, серверы, мэйнфреймы, принтеры и другое оборудование, при этом все ресурсы связаны посредством разнообразных локальных, региональных и глобальных сетей.

- История развития сетей весьма достойна изучения, поскольку с ее помощью можно понять сложные социальные, политические и технические факторы, определившие создание сетей и их быстрое распространение. Корни локальных и глобальных сетей следует искать в самых первых телеграфных и телефонных системах. В настоящее время сетевые технологии по-прежнему тесно связаны с успехами в области телекоммуникаций и в значительной мере определяются потребностями бизнеса, а также запросами в сфере личного общения и развлечений.

- Интеграция локальных и глобальных сетей становится все теснее и теснее благодаря развитию разнообразных сетевых устройств, таких как мосты, маршрутизаторы, шлюзы и коммутаторы. На этот процесс также влияют программные решения, позволяющие осуществлять взаимодействие между локальными сетями через глобальную сеть.

- Процесс проектирования сети включает в себя множество шагов. Чтобы разработать эффективную сеть, необходимо хорошо знать протоколы, топологий, сетевое оборудование, принципы проектирования сетей и способы определения сетевых потребностей всего предприятия. Обо всем этом будет рассказано в следующих главах книги.

Основные термины

Advanced Research Projects Agency Network (ARPANET) ¤ Сеть Управления! перспективных исследовательских программ. Эта сеть, первоначально спонсируемая Управлением перспективных исследовательских программ Министерства обороны США, являлась развитой исследовательской сетью, предшествующей Интернету.

American Standard Code for Information Interchange (ASCII) ¤ Американский стандартный код обмена информацией. Метод кодирования символов 8-разрядными словами; включает 96 заглавных и строчных букв, цифры и 32 непечатаемых символа.

Ethernet. Коммуникационная технология, использующая для передачи данных по сети метод доступа CSMA/CD. Сети Ethernet обычно имеют шинную; или комбинированную топологию.

Extended Binary Coded Decimal Interchange Code (EBCDIC) ¤ Расширенный двоично-десятичный код обмена информацией. Способ кодирования символьных сигналов, используемый в первую очередь на мэйнфреймах IBM и представляющий собой систему 8-разрядных кодов для представления; 256 символов, включая буквы, цифры и специальные знаки.

Request for Comments (RFC) ¤ Запрос на комментарии. Информационный документ, распространяемый с целью продвижения сетевых, компьютерных и интернет-коммуникаций. Эти запросы обрабатываются и заносятся в каталог Проблемной группой проектирования Интернета (IETF).

Systems Network Architecture (SNA) ¤ **Системная сетевая архитектура.** Многоуровневый коммуникационный протокол, используемый компанией IBfyf для передачи данных между мэйнфреймами и периферийными устройствами такими как терминалы и принтеры.

Виртуальная частная сеть ¤ Virtual private network (VPN). Частная сеть, работающая как туннель внутри сети большего масштаба (например, внутри Интернета или корпоративной сети) и, таким образом, доступная только для определенных клиентских компьютеров.

Глобальная сеть ¤ Wide area network (WAN). Совокупность сетей,, охватывающих большие площади (на расстояниях свыше нескольких десятков километр ров друг от друга) и зачастую находящихся в различных странах и на разных континентах.

Инкапсуляция ¤ Encapsulation. Процесс преобразования фрейма при передаче между сетями, при

котором фрейм данных сети одного типа помещается в заголовок фрейма, используемого в сети другого типа. Новый заголовок подобен конверту, в котором отправляется письмо.

Интернет ¤ Internet. Всемирная сеть взаимосвязанных локальных и региональных сетей, работающих по протоколу TCP/IP; позволяет людям обмениваться сообщениями электронной почты и получать доступ к самой различной информации.

Клиент-серверные вычисления ¤ Client/server computing. Архитектура компьютерных аппаратных и программных средств, в которой различные модули приложения могут выполняться на отдельных компьютерах или разными компонентами одного компьютера. Обычно клиентские компоненты приложений обеспечивают пользовательский ввод/вывод, а серверные программы выполняют поиск в базах данных, управляют выводом на печать и т. д.

Коммутатор ¤ Switch. Устройство для связи сетевых сегментов, пересылающее и фильтрующее фреймы между ними. Изначально коммутаторы работали, в первую очередь, на Уровне 2 модели OSI и для пересылок использовали физические адреса, или адреса устройств; однако современные коммутаторы могут также функционировать на Уровне 3 модели OS1 и более высоких уровнях.

Компьютерная сеть ¤ Computer network. Совокупность компьютеров, устройств печати, сетевых устройств и программных средств, между которыми осуществляется передача информации по кабелям или при помощи радио и УКВ-волн.

Корпоративная сеть, сеть предприятия ¤ Enterprise network. Объединение локальных, региональных или глобальных сетей, позволяющее пользователям компьютеров использовать многочисленные вычислительные и сетевые ресурсы для выполнения различных задач.

Локальная сеть ¤ Local area network (LAN). Совокупность взаимосвязанных компьютеров, устройств печати и другого сетевого оборудования, в которой аппаратные и программные средства используются совместно. Область обслуживания обычно ограничена пределами отдельного офиса, этажа или здания.

Магистраль ¤ Backbone. Скоростная коммуникационная среда, соединяющая сети на одном или разных этажах здания или на удаленных расстояниях.

Маршрутизатор ¤ Router. Сетевое устройство, соединяющее сети с одним или разными методами доступа и передающими средами (например, сети Ethernet и сеть с маркерным кольцом). Маршрутизатор пересылает пакеты и фреймы в соответствующие сети, для чего используется определенный метод принятия решений, основанный на данных таблицы маршрутизации, способах обнаружения наиболее эффективных маршрутов, а также параметрах, предварительно заданных сетевым администратором.

Межсетевой обмен, объединение сетей ¤ Internetworking. Процесс соединения сетей как одного типа, так и сетей различных типов для обеспечения взаимного обмена информацией.

Мост ¤ Bridge. Сетевое передающее устройство, соединяющее различные локальные сети или сегменты одной локальной сети, которые используют один и тот же метод доступа. Примером могут служить две локальные сети Ethernet, соединенные между собой. Мосты функционируют на Канальном уровне.

Пакет ¤ Packet. Модуль данных, упакованных в виде, пригодном для передачи по сети, и содержащих управляющую и иную информацию. Соответствует Сетевому уровню модели OSI (Уровню 3).

Протокол ¤ Protocol. Установленный регламент, определяющий способ форматирования сетевых данных в пакете или фрейме, механизм их передачи и методы интерпретации данных, полученных на принимающем узле.

Региональная сеть ¤ Metropolitan area network (MAN). Сеть, связывающая несколько локальных сетей в пределах большого города или значительной городской территории.

Сеть общего пользования ¤ Public network. Сеть, предлагающая свои услуги всем членам некоторого сообщества (например, сетевые службы, предоставляемые телекоммуникационной компанией или компанией кабельного телевидения).

Топология ¤ Topology. Физическая конфигурация кабеля и логические маршруты, по которым следуют сетевые пакеты, передаваемые по этому кабелю.

Транслирующий мост ¤ Translation bridge. Мост между сетями, использующими различные транспортные протоколы, который может направлять трафик по этим протоколам в соответствующие сети.

Трансляция ¤ Translation. Способ преобразования одного транспортного протокола в другой.

Фрейм ¤ Frame. Этот термин иногда используется как эквивалент понятия "пакет" и обозначает блок данных, передаваемый по сети и содержащий управляющую и адресную информацию, соответствующую Канальному уровню модели OSI (Уровню 2).

Хост, узел ¤ Host. Компьютер (мэйнфрейм, мини-ЭВМ, сервер или рабочая станция), имеющий операционную систему, позволяющую другим компьютерам одновременно обращаться к нему для получения доступа к файлам, данным и службам. Программы и обработка информации могут выполняться непосредственно на хосте или могут быть загружены для выполнения на клиентский компьютер, обращающийся к хосту. В другом значении "хост" – это любой компьютер, подключенный к сети.

Частная сеть ¤ Private network. Сеть, принадлежащая некоторой организации и управляемая силами этой организации (например, университетская сеть, которую поддерживает один из колледжей).

Шлюз ¤ Gateway. Сетевое устройство, обеспечивающее обмен информацией между сетевыми системами разного типа (например, между сложными протоколами или различными почтовыми системами).

Эмуляция локальной сети ¤ LAN Emulation (LANE). Метод адаптации технологии ATM к сетям Ethernet. Для его реализации создается широковещательная сеть, позволяющая заранее определенным группам Ethernet-узлов принимать передаваемую информацию.

Эмуляция терминала ¤ Terminal emulation. Использование программных решений для того, чтобы компьютер (например, персональный) функционировал как терминал.

Вопросы для повторения

1. Какие аспекты из перечисленных вы рассматривали бы при проектировании корпоративной сети?
   a) периоды максимального и минимального использования сети;
   b) типы компьютеров, используемых в сети;
   c) бизнес-процессы, существующие в организации;
   d) все перечисленное выше;
   e) ничего из перечисленного выше;
   f) только а) и б).
2. Какой из перечисленных типов сети охватывает наибольшие расстояния?
   a) LAN;
   b) WAN;
   c) MAN;
   d) NAN.
3. Какое устройство вы, скорее всего, использовали бы в качестве "дешевого" канала для передачи обычных данных и "дорогого" – для передачи мультимедиа?
   a) мост;
   b) шлюз;
   c) маршрутизатор;
   d) соединительный интерфейс.
4. Кодировка символов _____ была разработана как альтернатива коду Extended Binary Coded Decimal Interchange Code (EBCDIC, расширенный двоично-десятичный код обмена информацией).

5. Что было разработано раньше — TCP или IP, и что означают эти аббревиатуры?
6. Какой из перечисленных методов сетевых коммуникаций был разработан раньше других?
   a) SONET;
   b) ATM;
   c) X.25;
   d) SMDS.
7. Что дало основной импульс развитию Интернета в 1998 году?
   a) университетские исследования;
   b) разработка нового универсального протокола Интернета;
   c) бизнес и коммерция;
   d) Белый дом (правительство США).
8. Что такое "запрос на комментарии" (Request for Comment, RFC)?
9. Фрейм содержит информацию о получателе передаваемых цифровых данных, но не об их источнике. Верно это или нет?
10. В начале 1970-х годов впервые глобальные сети, такие как ARPANET,предназначались для:
    a) исследователей;
    b) военных;
    c) электронной коммерции;
    d) всех перечисленных пользователей и задач;
    e) только а) и б).
11. Процедура переноса информационных полей одного протокола в заголовок другого Протокола называется ___.
12. В зависимости от своей конструкции, коммутатор может функционировать как _____ или как _____.
13. Первоначальное развитие какой технологии стимулировало разукрупнение компаний AT&T Bell?
    a) модемы;
    b) 24-канальные ИКМ-системы типа T (T-carriers);
    c) персональные компьютеры;
    d) интегральные схемы.
14. Первые устройства, подключенные к сети ARPANET и обеспечивающие взаимодействие между хостами, назывались _____ .
15. Модуль данных, содержащих информацию, относящуюся к Уровню 3,называется .
16. Если бы 20 лет назад вы были подключены к мэйнфрейму IBM, то для передачи данных, скорее всего, использовали бы:
    a) SNA;
    b) VLSI;
    c) ARPALink;
    d) ICP;
    e) все перечисленные средства;
    f) только а) и в);
    g) только в) и с).
17. Первые локальные сети персональных компьютеров использовали программное обеспечение, которое впоследствии получило название _____ .
18. Физическая конфигурация сети называется:
    a) географией;
    b) эмуляцией;
    c) протоколом;
    d) топологией;
    e) ничто из перечисленного не подходит.
19. Эмуляция локальной сети является разновидностью процесса и применяется в сетях.
20. _____или_____можно использовать для подключения локальной сети к глобальной.

Практические задания

Во многих практических заданиях, предлагаемых в этой книге, используется одна из систем: Microsoft Windows 2000 (версии Professional и Server), Windows XP Professional или Red Hat Linux 7.2. Работа ведется в стандартном пользовательском интерфейсе Windows 2000, новом интерфейсе Windows XP или в среде X Window GNOME для Red Hat Linux 7.2.

Задание 1-1

В этом задании вы познакомитесь с архитектурой корпоративной сети. Задание напоминает игру, в которой за установленное время нужно найти максимальное количество предметов. Предварительно договоритесь с администратором сети о доступе к помещениям, где располагается компьютерное оборудование университетской сети.

Для знакомства с архитектурой корпоративной сети выполните следующее:

1. Разбейтесь на небольшие группы или действуйте индивидуально для поиска максимально возможного количества устройств, подключенных к сети.
2. Установите лимит времени на поиск: например, один час или остаток учебного дня.
3. Каждый участник должен искать перечисленные ниже объекты и регистрировать местоположение каждого обнаруженного им объекта:

- рабочая станция;
- файловый сервер или сервер печати;
- хост-компьютер;
- сетевой лазерный принтер;
- мэйнфрейм;
- маршрутизатор, мост, шлюз, коммутатор или любой модуль, выполняющий функции этих устройств;
- подключение к глобальной сети;
- соединение между локальными сетями;
- факсимильный аппарат или приложения, выполняющие эти функции;
- плоттер;
- почтовый сервер;
- терминатор;
- оптоволоконный кабель;
- оборудование для подключения к Интернету;
- интранет;
- сервер базы данных;
- ленточный накопитель или библиотека магнитных лент;
- привод CD-ROM или библиотека накопителей CD-ROM;
- подключение беспроводной связи;
- модем;
- другие устройства, подключенные к сети.

4. Определите, кто из участников первым обнаружил устройства, перечисленные в списке, и проверьте их местоположение.

Задание 1-2

В этом задании вы познакомитесь с точкой подключения локальной сети к глобальной, для чего выполните следующие действия:

1. Свяжитесь с администратором имеющейся сети.
2. Узнайте у него, можно ли увидеть оборудование, используемое для подключения локальной сети к глобальной (например, к региональной телефонной компании).
3. Узнайте тип глобальной сети, с которой соединяется локальная сеть.

4. Узнайте, какое оборудование применяется в точке подключения.
5. Определите скорость локальной сети и сравните ее со скоростью передачи данных в глобальной сети.
6. Запишите всю информацию в лабораторный журнал или в текстовый файл.

Примечание

В качестве альтернативного варианта вы можете попросить сетевого администратора провести групповую экскурсию по местам расположения оборудования, соединяющего локальную и глобальную сети. Также можно попросить его провести презентацию в классе и рассказать о коммуникационных устройствах.

Задание 1-3

Иногда для подключения одной сети к другой используется коммутируемое соединение или виртуальная частная сеть (VPN). В этом задании вы познакомитесь с логическими подключениями различного типа, создаваемыми в системах Windows 2000 Server и Windows XP Professional. Для просмотра различных сетевых подключений выполните следующие действия:

1. Чтобы увидеть логические подключения в системе Windows 2000, нажмите кнопку **Start** (Пуск) и в меню **Settings** (Настройка) выберите пункт **Network and Dial-up Connections** (Сеть и удаленный доступ к сети).
2. Какие подключения вы видите в правой части окна **Network and Dial-up Connections** (Сеть и удаленный доступ к сети)?
3. Дважды щелкните по значку **Make New Connection** (Создание нового подключения).
4. При запуске программы Network Connection Wizard (Мастер сетевого подключения) нажмите кнопку **Next** (Далее).
5. Соединения каких типов можно создать?
6. Нажмите кнопку **Cancel** (Отмена).
7. Закройте окно **Network and Dial-up Connections** (Сеть и удаленный доступ к сети).
8. Чтобы увидеть логические подключения в системе Windows XP Professional, нажмите **Start** (Пуск), откройте панель управления (Control Panel) и щелкните по ссылке **Network and Internet Connections** (Сеть и подключения к Интернету).
9. Какие сетевые опции перечислены в разделе **Pick a Task** (Выберите задание)
10. Щелкните по ссылке **Network Connections** (Сетевые подключения).
11. Какие подключения уже существуют?
12. Закройте окно **Network Connections** (Сетевые подключения).

Задание 1-4

Многие системы, включая системы Windows, имеют возможность создания сетевых и коммутируемых подключений, т. е. они могут подключаться как к локальным, так и глобальным сетям. В этом задании вы познакомитесь с сетевыми возможностями системы Red Hat Linux 7.2, обеспечивающей работу с интерфейсом X Window GNOME.

Для знакомства с сетевыми возможностями системы выполните следующие действия:

1. Зарегистрируйтесь в сети, используя основную административную учетную запись root.
2. В среде GNOME откройте окно командной строки, для чего нужно щелкнуть по значку **Terminal emulation program** (в виде компьютерного монитора) на панели (аналогичной панели задач систем Windows), расположенной в нижней части экрана.
3. В командной строке введите ipconfig и нажмите клавишу <Enter>.

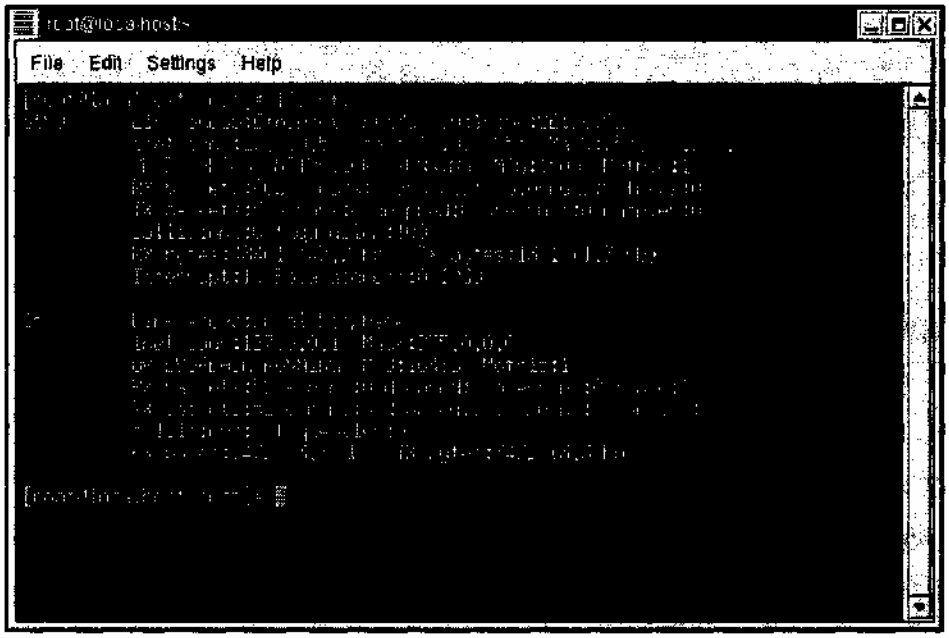


Рис. 1.11. Сетевая конфигурация операционной системы Red Hat Linux

4. Взгляните на левую часть экрана. Если имеется строка для устройства etho, то система подключена к сети Ethernet, например, с помощью сетевого адаптера. Если отображается устройство ppp, система настроена на доступ к Интернету, для чего может использоваться коммутируемое модемное подключение. На рис. 1.11 показано, что система имеет выход на сеть Ethernet (etho), однако коммутируемые подключения (ppp) отсутствуют: устройство 1o соответствует локальному обратному (loopback) подключению, которое всегда создается вместе с Ethernet-подключением.

Задание 1-5

В этом задании вы узнаете о том, как найти информацию о запросах на комментарии (RFC).
Чтобы найти определенный документ RFC, выполните следующие действия:

1. Запустите веб-браузер.
2. Откройте веб-страницу **www.rfc-editor.org/cgi-bin/rfcsearch.pl.**
3. Введите в поле поиска RFCI. В списке категорий поиска выберите значение **All Fields** и нажмите кнопку **Search** (Поиск).
4. В полученном списке щелкните по ссылке REF0001.
5. Как называется данный RFC? Кто и когда разработал его?
6. Вернитесь назад, в поле поиска введите rfc1.txt и нажмите клавишу <Enter>.
7. Щелкните по ссылке REF0001, которая будет единственной в списке найденных RFC.
8. Прочитайте найденный документ RFC.

9. Не закрывайте окно браузера – оно потребуется для выполнения следующего задания.

Задание 1-6

В этом задании вы познакомитесь с дополнительной информацией по истории сетевых технологий, для чего будет использоваться хронология Hobbes' Internet Timeline.

Для знакомства с хронологией выполните следующие действия:

1. Откройте окно веб-браузера.
2. Откройте веб-страницу **www.zakon.org/Robert/internet/timeline** (Hobbes Internet Timeline Copyright (c) 1993-2003 by Robert H Zakon).
3. Пользуясь хронологией, ответьте на следующие вопросы:
   a) какой компьютер использовали в 1969 году в University of California at Santa Barbara (UCSB) для подключения к сети ARPANET?
   b) как назывался первый удаленно управляемый компьютер, подключенный к Интернету?

c) от чего пострадали 6000 хостов в 1988 году?

d) что сделала английская королева Елизавета II в 1976 году в области сетевых технологий?

e) какая организация была создана в 1997 году для контроля за регистрацией IP-адресов?

f) кто создал сеть USENET в 1979 году и какие учебные заведения она связывала?

g) что появилось в 1994 году в Палате представителей и Сенате США?

4. Не закрывайте окно браузера — оно потребуется для выполнения следующего задания.

Задание 1-7

Сведения из истории компьютеров и сетей содержатся еще в одной хронологии – Computer Timeline of History.

Для знакомства с хронологией Computer Timeline of History выполните следующие действия:

1. Откройте окно веб-браузера.
2. Обратитесь к веб-странице **www.computerhistory.org/timeline.**
3. Щелкните по ссылке '85. Какую скорость имела первоначально сеть NSFNET? Какие каналы связи появились у сети NSFNET после модернизации в 1992 году и какова была скорость этих каналов?
4. Щелкните по ссылке '79. Кто придумал первую программу-червь (worm). Откуда произошел термин "червь"?
5. Щелкните по ссылке '90. Какой язык, важный для всемирной паутины World Wide Web, был разработан и кем?
6. Щелкните по ссылке '64. Для чего использовалась система SABRE? Какие сетевые компоненты использовались для нее?
7. Закройте окно веб-браузера.

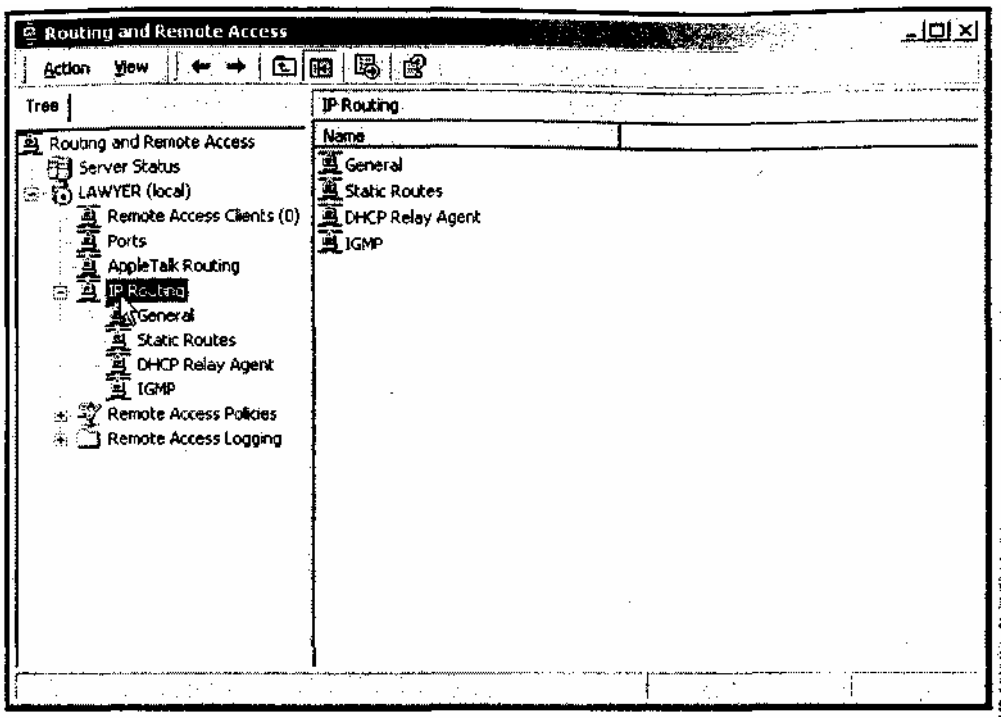
Задание 1-8

Система Windows 2000 Server может быть сконфигурирована как маршрутизатор. В этом задании вы узнаете, как настраиваются службы маршрутизации в этой системе. Для выполнения задания необходимо иметь учетную запись с административными правами. Кроме того, на используемом сервере уже должны быть сконфигурированы службы Routing and Remote Access и DHCP.

Для знакомства с методами конфигурирования системы Windows 2000 Server в качестве маршрутизатора выполните следующие действия:

1. Зарегистрируйтесь в системе.
2. Нажмите кнопку **Start** (Пуск), в меню **Programs** (Программы) выберите подменю **Administrative Tools** (Администрирование), а в нем — опцию **Routing and Remote Access** (Маршрутизация и удаленный доступ).

3. В дереве объектов дважды щелкните по узлу **IP Routing** (Маршрутизация IP) — вы увидите имеющиеся опции, показанные на рис. 1.12. Следует помнить, что сервер может работать как универсальный маршрутизатор, а может выполнять определенную роль, например, являться агентом ретранслятором DHCP для некоторого сервера, автоматически раздающего IP-адреса (о протоколах IP и DHCP будет рассказано в следующих



главах).

Рис. 1.12. Оснастка **Routing and Remote Access**
в операционной системе Windows 2000 Server

4. Закройте окно **Routing and Remote Access** (Маршрутизация и удаленный доступ).

Задание 1-9

Компьютер под управлением системы Red Hat Linux может выполнять функцию простого маршрутизатора между двумя сетевыми сегментами при, условии, что в нем установлены два сетевых адаптера. В этом задании вы научитесь с помощью командной строки конфигурировать маршрутизацию, в системе Red Hat Linux 7.2.

Для знакомства с утилитами командной строки выполните следующие действия:

1. Откройте терминальное окно, щелкнув в среде GNOME по значку **Terminal emulation program,** расположенному на панели.
2. В командной строке введите route и нажмите клавишу <Enter>. Эта команда позволит увидеть текущую конфигурацию таблиц маршрутизации, и с ее помощью можно задавать маршруты между сегментами сети.
3. Чтобы увидеть описание команды route, введите в командной строке man route.
4. Для выхода из режима просмотра документации введите q, затем введите exit и нажмите клавишу <Enter> для выхода из терминального окна.

Задание 1-10

Система Windows 2000 Server, работающая с одним протоколом, может использоваться как шлюз к серверу NetWare, который настроен на работу с другим протоколом. При этом пользователи могут регистрироваться на сервере Windows 2000 и получать доступ к файлам и принтерам сервера NetWare, не устанавливая тот протокол, с которым работает данный сервер NetWare. В этом задании вы узнаете, как в системе Windows 2000 Server установить службы Gateway Services for NetWare (если они еще не инсталлированы).

Для установки служб Gateway Services for NetWare выполните следующие действия:

1. Нажмите кнопку **Start** (Пуск) и в меню **Settings** (Настройка) выберите пункт **Network and Dial-up Connections** (Сеть и удаленный доступ к сети).
2. Укажите на значок **Local Area Connection** (Подключение к локальной сети), щелкните правой кнопкой мыши и в контекстном меню выберите опцию **Properties** (Свойства).

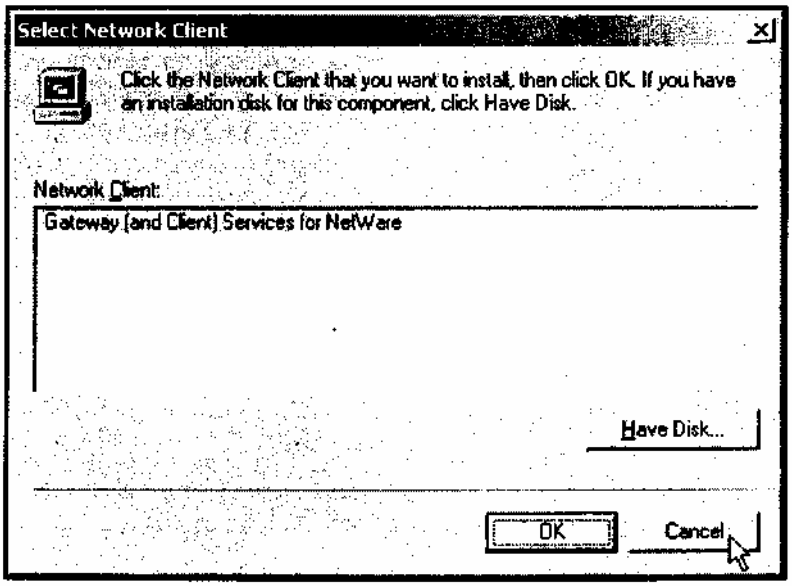


Рис. 1.13. Опция для установки служб Gateway (and Client) Services for NetWare в операционной системе Windows 2000 Server

3. Нажмите кнопку **Install** (Установить) и в открывшемся окне дважды щелкните по опции **Client** (Клиент).
4. В следующем диалоговом окне, показанном на рис. 1.13, вы можете запросить установку служб Gateway (and Client) Services for NetWare.
5. Нажмите кнопку **Cancel** (Отмена), затем нажмите одноименную кнопку еще раз.
6. Закройте окно свойств подключения к локальной сети.
7. Закройте окно **Network and Dial-up Connections** (Сеть и удаленный доступ к сети).

Учебные задачи

Вы работаете в качестве сетевого консультанта в компании Network Design Consultants. В вашей компании имеется 15 консультантов, которые помогают любым организациям решать вопросы планирования, проектирования, развертывания и сопровождения сетей. В зависимости от портфеля заказов компания работает как с национальными, так и с международными проектами.

В настоящий момент вы делегированы для работы с отделом информационных технологий новой металлообрабатывающей компании Metal Works, имеющей отделения в городах Торонто (Канада) и Олленстаун (Пенсильвания).

Выполните следующие задачи:

1. Руководители IT-отдела просят вас подготовить презентацию, рассказывающую о сетевых технологиях членам администрации компании Metal Works, чтобы те поняли, почему эти технологии важны в бизнес-планах компании. Продумайте презентацию, раскрывающую следующие вопросы:

- описание различных типов сетей;
- обзор достижений сетевых технологий за последние 10 лет;
- краткий рассказ о том, как реализация сетей повлияла на развитие бизнеса в стране;
- общее описание тех преимуществ, которые компания Metal Works получит при внедрении сетевых технологий.

2. Во время презентации один из менеджеров компании спрашивает у вас о том, какое событие в истории развития сетей оказалось наиболее значимым. Что вы ответите?
3. Менеджер по работе с пользователями IT-отдела не знаком с некоторыми основными типами сетевых устройств, которые можно использовать при развертывании корпоративной сети. Опишите кратко некоторые устройства, которые, вероятнее всего, могут применяться.

4. Этот менеджер также интересуется основными этапами в процессе проектирования сети. Сделайте обзор этих этапов.

Дополнительные учебные задачи для групповой работы

1. Компания Western Antiques представляет собой сеть антикварных магазинов, расположенных в пяти городах Западного побережья США. Она собирается использовать Интернет в качестве еще одного "рынка сбыта своей продукции и наняла вашу фирму с целью проведения исследований в области интернет-коммерции. Образуйте группу из двух-трех консультантов и подготовьте статистику по данному вопросу. Кроме того, обсудите вопрос – каким образом наличие коммерческого интернет-сайта может принести пользу для этой сферы бизнеса. В качестве одного из источников информации используйте Интернет.

2. Компания Gladstone Group проводит исследования в области локальных сетей. Она просит вашу компанию выполнить анализ способов использования подобных сетей в бизнесе, а также в правительственных и образовательных учреждениях. Создайте рабочую группу и подготовьте для вашего клиента подробный перечень областей применения локальных сетей.

Резюме

- Локальные, региональные и глобальные сети — три основных типа компьютерных сетей. Главным их отличием друг от друга является область обслуживания, а затем – протоколы и топологии, используемые для построения сети. Термины "локальная сеть" и "глобальная сеть" в первую очередь относятся, соответственно, к небольшим самостоятельным сетям и к крупномасштабным сетям, их соединяющим. Соотношение между локальными и глобальными сетями напоминает подключение небольшой учрежденческой телефонной станции к крупной телекоммуникационной системе. С другой стороны, сеть можно рассматривать как совокупность корпоративных ресурсов, в число которых входят компьютеры, серверы, мэйнфреймы, принтеры и другое оборудование, при этом все ресурсы связаны посредством разнообразных локальных, региональных и глобальных сетей.

- История развития сетей весьма достойна изучения, поскольку с ее помощью можно понять сложные социальные, политические и технические факторы, определившие создание сетей и их быстрое распространение. Корни локальных и глобальных сетей следует искать в самых первых телеграфных и телефонных системах. В настоящее время сетевые технологии по-прежнему тесно связаны с успехами в области телекоммуникаций и в значительной мере определяются потребностями бизнеса, а также запросами в сфере личного общения и развлечений.

- Интеграция локальных и глобальных сетей становится все теснее и теснее благодаря развитию разнообразных сетевых устройств, таких как мосты, маршрутизаторы, шлюзы и коммутаторы. На этот процесс также влияют программные решения, позволяющие осуществлять взаимодействие между локальными сетями через глобальную сеть.

- Процесс проектирования сети включает в себя множество шагов. Чтобы разработать эффективную сеть, необходимо хорошо знать протоколы, топологий, сетевое оборудование, принципы проектирования сетей и способы определения сетевых потребностей всего предприятия. Обо всем этом будет рассказано в следующих главах книги.

Глава 2

Взаимодействие локальных и глобальных сетей

По прочтении этой главы и после выполнения практических заданий вы сможете:

- объяснить эталонную модель OSI, устанавливающую стандарты взаимодействия локальных и глобальных сетей;
- понять процесс передачи информации между стеками OSI для компьютеров, объединенных в сеть;
- применять модель OSI в реальных сетевых конфигурациях;
- описать типы сетей с точки зрения топологии локальных сетей;
- описать основные методы передачи данных в локальных сетях, включая Ethernet, Token Ring и FDDI;
- понимать основные топологии глобальных сетевых коммуникаций и методы передачи данных, включая каналы телекоммуникации и кабельного телевидения, спутниковые технологии.

Взаимодействие локальных и глобальных сетей является быстроразвивающейся областью техники, что объясняется жесткой конкуренцией между компаниями, работающими в трех следующих секторах промышленности: телекоммуникации, кабельное телевидение и спутниковые средства связи. Быстрый рост этих отраслей увеличил возможности совместного использования информации, доступной через сети и Интернет. Например, пользователь, живущий в небольшом городе, может подключаться к Интернету по телефонной линии, с помощью спутниковой "тарелки" или входа кабельного телевидения. Много дополнительных возможностей появляется при соединении локальных сетей, находящихся в разных странах или частях света.

Телекоммуникационные компании могут обеспечить связь локальных сетей через глобальную сеть, используя для этого междугородные высокоскоростные телефонные линии. Глобальные сети строятся на основе радио, радиорелейных (СВЧ) и спутниковых каналов. Жесткая конкуренция между поставщиками услуг глобальных сетей приводит к быстрому появлению новых возможностей передачи данных.

Данная глава знакомит читателей с идеологией объединения локальных и глобальных сетей, для чего подробно рассматривается эталонная модель взаимодействия открытых систем – OSI (Open Systems Interconnection). Без этой модели, устанавливающей разработанные более 20 лет назад стандарты для локальных и глобальный сетей, современные сетевые коммуникации были бы в состоянии хаоса и возможностей межсетевого общения было бы гораздо меньше. Также читатели познакомятся с основными топологиями сетей и методами передачи данных в локальных сетях. Кроме этого, будут рассмотрены способы организации глобальных сетей и используемые в них способы передачи информации.

Эталонная модель взаимодействия открытых систем OSI

Без соответствующих стандартов сетевые коммуникации представляли бы собой неупорядоченный набор частных протоколов и устройств, созданных различными производителями с использованием разных концепций и моделей. Так было на первых этапах развития компьютеров, когда для оборудования не существовало единых стандартов. Например, принтер от одного компьютера нельзя было без изменения электрической схемы подключить к другому компьютеру, поскольку конструкции коммуникационных портов отличались.

К счастью, объединение локальных и глобальных сетей с первых шагов выполнялось в соответствии с некоторой идеологией, называемой *эталонной моделью взаимодействия открытых систем* (Open Systems Interconnection, OSI). Модель OSI является детищем двух регламентирующих организаций: *Международной организации по стандартизации* (International Organization for Standardization, ISO) и *Национального института стандартизации США* (American National Standards Institute, ANSI). В сфере разработки экономических, интеллектуальных, научных и технологических стандартов

организация ISO представляет свыше 140 стран. Институт ANSI работает совместно с деловыми и правительственными кругами США и международными группами и создает стандарты на коммерческие (серийные) изделия, включая сетевое оборудование и компьютеры.

Модель OSI, разработанная в 1974 году, регламентирует взаимодействие локальных и глобальных сетей и представляет собой попытку стандартизации сетевых программных и аппаратных средств (чтобы узнать о том, как в модели OSI рассматривается необходимость стандартизации, выполните практическое задание 2-1). На протяжении многих лет модель OSI способствовала развитию сетевых коммуникаций, позволяющих решать следующие вопросы:

- ❖ обеспечение передачи информации между различными типами локальных и глобальных сетей;
- ❖ стандартизация сетевого оборудования, что позволяет устройствам одного производителя взаимодействовать с устройствами других производителей;
- ❖ сохранение капиталовложений пользователей, обеспеченное возможностью взаимодействия старого сетевого оборудования с новыми устройствами; при этом устраняется необходимость замены оборудования при установке новых устройств;
- ❖ разработка программного и аппаратного обеспечения, использующего общие интерфейсы для передачи данных как внутри сети, так и между различными сетями;
- ❖ возможность появления всемирных сетевых коммуникаций, в первую очередь – Интернета.

Появление модели OSI предшествовало созданию большинства современных сетевых устройств, однако она явилась основой для разработки идей межсетевого обмена и постоянно развивается, впитывая в себя новые сетевые технологии. Концепции эталонной модели OSI соблюдаются не всегда, поскольку исследования и технологии иногда идут в других направлениях, однако она все равно является основой, от которой можно отталкиваться (в последующих главах вы узнаете о том, насколько те или иные протоколы и сетевые устройства соответствуют этой модели). OSI является чисто теоретической моделью, а не описанием конкретных аппаратных и программных решений. Скорее это набор руководящих документов для изготовителей оборудования, который они должны использовать при проектировании аппаратных и программных средств. При разработке протоколов и сетевых устройств нормативы являются тем же, что и грамматика для разговорного языка. Нормативы OSI описывают следующие моменты:

- ➢ как сетевые устройства общаются друг с другом и как взаимодействуют устройства, использующие разные протоколы;
- ➢ каким образом сетевое устройство узнает, когда можно и когда нельзя передавать данные;
- ➢ способы организации и физического соединения сетевых устройств;
- ➢ методы обеспечения правильности передачи данных по сети;
- ➢ способы поддержания непрерывного потока данных в сетевых устройствах;
- ➢ способы представления данных в виде электрических сигналов при передаче по сетевой среде.

Как показано на рис. 2.1, модель OSI состоит из семи отдельных уровней, расположенных один поверх другого:

- Физический;
- Канальный;
- Сетевой;
- Транспортный;
- Сеансовый;
- Представительский;
- Прикладной.

Каждый уровень выполняет определенные коммуникационные задачи и с помощью соответствующих протоколов взаимодействует с соседними уровнями иерархии. Передача информации между двумя сетевыми устройствами осуществляется с использованием этой иерархии уровней (стека) в каждом из устройств. Например, если рабочая станция обменивается данными с сервером, передача информации начинается в рабочей станции на Прикладном уровне. Затем формируется определенная информация на более нижних уровнях до тех пор, пока данные не достигнут Физического уровня и не будут по сети переданы серверу. Сервер принимает данные на Физическом уровне своего стека и передает их для интерпретации более высоким уровням, пока

данные не достигнут Прикладного уровня. Каждый уровень называется либо по имени, либо по положению в стеке (1-й уровень, 2-й уровень и т. д.). Например, нижний уровень стека называется Физическим уровнем или Уровнем 1.

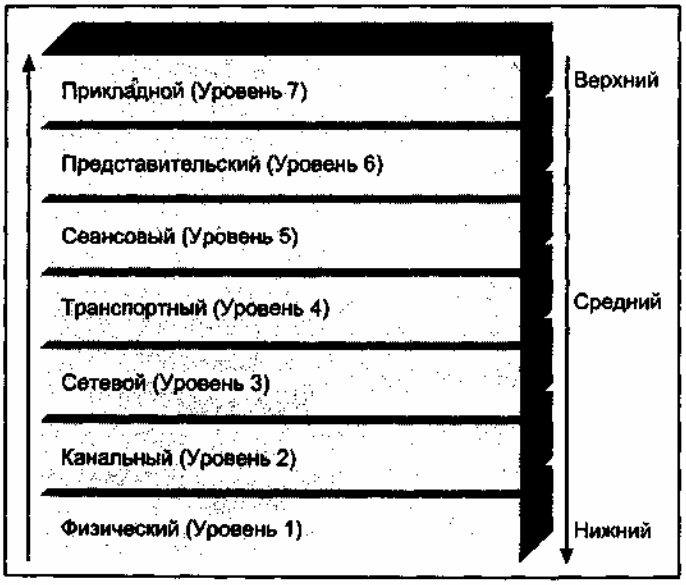


Рис. 2.1. Уровни модели OSI

Нижние уровни стека выполняют функции, относящиеся к передаче физического сигнала (например, они создают фреймы и передают сигналы, содержащие пакеты данных). Средние уровни координируют сетевые коммуникации между узлами (например, обеспечивают бесперебойное и безошибочное осуществление сеанса связи). Верхние • уровни выполняют задачи, непосредственно влияющие на прикладные программы и представление данных, включая форматирование и шифрование информации, а также управление передачей файлов. В совокупности набор уровней называется стеком. В последующих разделах каждый из семи уровней рассматривается подробно (также см. табл. 2.1).

Физический уровень (1)

Самый нижний из уровней модели OSI называется *Физическим уровнем* (physical layer). Этот уровень описывает:

- все физические среды передачи данных (кабель, оптоволокно, волны радио и других диапазонов);
- сетевые разъемы;
- топологию сети;
- методы передачи и кодирования сигнала;
- устройства передачи данных;
- сетевые интерфейсы;
- методы распознавания ошибок при передаче сигналов.

Устройства, используемые на Физическом уровне, отвечают за генерирование, передачу и распознавание электрических сигналов, предназначенных для передачи и приема данных. Сетевые сигналы могут быть представлены в аналоговом или цифровом виде. *Аналоговый* сигнал может изменяться непрерывно и выглядеть как волна с положительными и отрицательными перепадами напряжения. Примером такого сигнала может являться обычный радио- или телефонный сигнал, поскольку он может иметь широкий диапазон для передачи звука. Аналоговый телевизор или компьютерный монитор может одновременно воспроизводить миллионы цветов в любом диапазоне. Аналоговые сигналы используются в глобальных сетях, где для передачи данных применяются аналоговые модемы. Например, с помощью такого модема пользователь может подключиться к Интернету через поставщика услуг Интернета (интернет-провайдера). Аналоговый сигнал изображен на рис. 2.2.

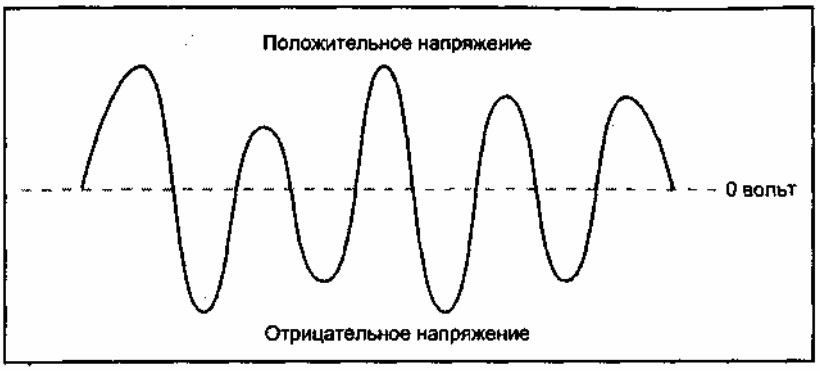


Рис. 2.2. Аналоговый сигнал

В *цифровом* сигнале для представления единиц и нулей используются фиксированные уровни напряжения. Такие сигналы чаще всего используются в локальных и скоростных глобальных сетях. Например, наличие напряжения +5 вольт может трактоваться как единица, а нулевое напряжение – как ноль (что проиллюстрировано на рис. 2.3). Другой путь для представления единиц и нулей – использование некоторого положительного напряжения (скажем, +5 вольт) для передачи единиц и отрицательного напряжения (например, -5 вольт) для передачи нулей. В оптоволоконных каналах двоичные единицы и нули обозначаются наличием или отсутствием света. Все названные варианты показаны на рис. 2.3.

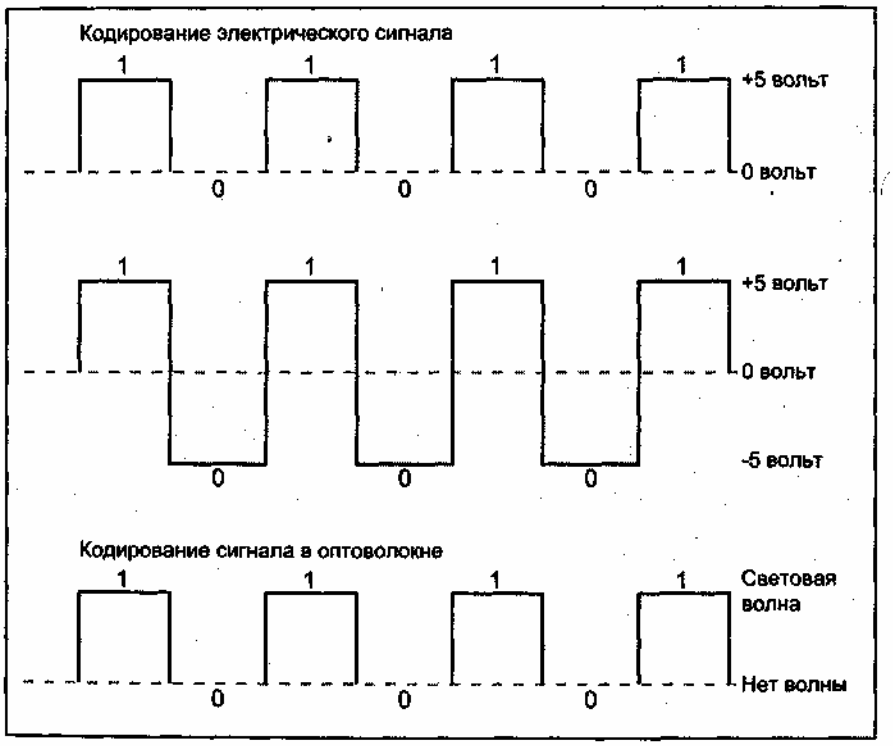


Рис. 2.3. Примеры цифровых сигналов

Примечание

Кодируемый сигнал преобразуется в двоичный формат (система счисления с основанием 2), имеющий определенное значение для компьютера или сетевого устройства. Существуют два основных метода кодирования цифровых сигналов: *с использованием текущих состояний* (current-state encoding) и *с использованием переходов из одного состояния в другое* (state transition). В первом случае двоичное значение кодируется с помощью некоторого состояния сигнала: например, двоичная единица обозначается напряжением +5 вольт, а двоичный ноль - нулевым напряжением. Во втором случае просто проверяется изменение состояния сигнала - переход от низкого уровня к высокому и наоборот. В сетях чаще всего используется метод, называемый *манчестерским кодированием* (Manchester encoding), при котором двоичная единица представлена переходом от низкого уровня сигнала к высокому, а двоичный ноль соответствует переходу сигнала от высокого к низкому.

Физический уровень управляет скоростью передачи данных, анализом потока ошибок и уровнями напряжения, используемыми для передачи сигнала. На его работу влияют физические проблемы в сети, например, разрывы передающего кабеля или электромагнитные наводки. Наводки могут создаваться близко расположенными электромоторами, линиями высокого напряжения, осветительными и другими электрическими приборами.

Электромагнитное излучение и *радиопомехи* - вот два источника ошибок физического уровня. Электромагнитное излучение вызывают силовые магнитные поля, генерируемые электрическими устройствами, такими как вентиляторы, двигатели лифтов, переносные обогреватели и кондиционеры. Радиопомехи создаются электрическими приборами, генерирующими радиоволны той же частоты, что используются для передачи сетевого сигнала. Такими приборами могут быть компоненты кабельного телевидения, радио- и телевизионные станции, расположенные близко передатчики, балластные устройства ламп дневного света, недорогое компьютерное или телевизионное оборудование и устройства для радиосвязи. Влияние сетевых помех рассматривается в практическом задании 2-2 в конце этой главы.

Совет

Понимание концепций Физического уровня особенно важно при работе с сетями, поскольку ошибки именно на этом уровне зачастую мешают правильной работе сети. Например, сеть может быть подключена к двум различным источникам напряжения, находящимся даже в одной комнате, но имеющим разные шины заземления. Поскольку у обоих источников отсутствует истинная "земля", нулевые напряжения у обоих источников отличаются как от истинного нуля, так и между собой. Если случайно одновременно схватиться за кабели, связанные с оборудованием, подключенным к данным источникам питания, можно получить электрический удар, т. к. через тело пойдет ток, вызванный разностью потенциалов между этими кабелями.

Канальный уровень (2)

Задача *Канального уровня* (data link layer) в локальной сети – компоновать передаваемые биты данных в виде фреймов, или кадры (frame). Каждый фрейм определенным образом форматирован – так, чтобы для надежной передачи данных от узла к узлу информационные пакеты были упорядочены. Этот уровень кодирует данные в виде фреймов, после чего отформатированные фреймы поступают на Физический уровень, где передающий узел может отправить их в коммуникационную среду (например, в кабель). Принимающий узел получает фрейм от Физического уровня, декодирует электрический сигнал, представляющий разряды данных, преобразует отдельные разряды во фрейм и проверяет наличие ошибок во фрейме.

Канальный уровень представляет информационные разряды в виде «фрейма» канального уровня, который содержит поля с адресной и управляющей информацией. Таким образом, фрейм содержит:

- признак начала фрейма (start of frame, SOF);
- адрес устройства или передающего узла, отправляющего фрейм (адрес источника);
- адрес устройства или принимающего узла, получающего переданный фрейм (адрес назначения);
- административную или управляющую информацию (для контроля коммуникационного процесса);
- данные;
- информацию для обнаружения ошибок (контрольные данные);
- трейлер (концевик) или признак конца фрейма (end of frame, EOF).

Для установления связи между двумя узлами сначала передается небольшой набор сигналов, используемых для синхронизации потока данных. После того, как соединение установлено, Физические уровни обоих узлов сказываются связанными через среду передачи данных (например, через кабель), а их Канальные уровни связаны логически благодаря используемым протоколам. Как только логический канал установлен, принимающий Канальный; уровень может декодировать сигнал и преобразовывать его в отдельные фреймы.

На Канальном уровне выполняется проверка входящих сигналов, а также обнаруживаются повторно, неправильно или частично переданные данные во входящем потоке. При обнаружении ошибок уровень

запрашивает у передающего узла повторную передачу данных – фрейм за фреймом. Для обнаружения ошибок на Канальном уровне используется *контроль циклическим избыточным кодом* (cyclic redundancy check, CRC). Этот метод распознавания; ошибок позволяет вычислить некоторое контрольное значение для содержимого всех информационных полей, имеющихся во фрейме (SOF, адреса, управляющие разряды, данные, контрольную сумму и EOF). На Канальном, уровне передающего узла полученное значение вставляется в конец фрейма; и затем проверяется на этом же уровне принимающего узла. По мере того, как фреймы поступают на следующий уровень, Канальный уровень обеспечивает очередность фреймов – т. е. они должны передаваться в том же порядке, в котором и принимаются.

Канальный уровень содержит два важных подуровня: более высокий - *управление логическим соединением* (logical link control, LLC) и более низкий - *протокол управления доступом к передающей среде* (media access control, MAC). Подуровень LLC обеспечивает надежность коммуникаций путем установки канала передачи данных между двумя узлами и поддержки устойчивости этого канала. Подуровень MAC распознает *физический адрес* (или *адрес устройства)* иногда называемый *MAC-адресом,* содержащийся в каждом фрейме. Например, на некоторой рабочей станции подуровень MAC проверяет каждый фрейм, получаемый этой станцией, и передает фрейм более высокому уровню лишь в том случае, если адрес совпадает. В противном случае фрейм отбрасывается. Кроме того, подуровень MAC управляет совместной работой множества устройств внутри одной сети. В практическом задании 2-3 рассказывается о том, как определить адрес рабочей станции.

Примечание

Большинство сетевых устройств имеют уникальный адрес, "зашитый" в микросхему сетевого интерфейса. Этот адрес представлен некоторым шестнадцатеричным числом (например, 0004AC8428DE). Первая половина адреса предназначена для обозначения конкретного производителя оборудования, а вторая, обычно формируемая самим производителем, является уникальной для интерфейса или устройства. Некоторые производители во второй половине адреса используют также код, идентифицирующий тип устройства – компьютер, мост, маршрутизатор или шлюз. Некоторые сетевые устройства (например, серверы с двумя сетевыми адаптерами) имеют несколько интерфейсов и, следовательно, несколько физических подключений к сети. Каждый сетевой интерфейс такого устройства имеет уникальный адрес, и это устройство идентифицируется в сети с помощью нескольких уникальных адресов, принадлежащим конкретным сетевым интерфейсам.

Совет

Важно, чтобы в сети не было устройств или интерфейсов с дублирующимися физическими адресами. Производители сетевого оборудования гарантируют уникальность физических адресов, отслеживая все использованные адреса, в результате чего повторное появление адреса исключено. Если бы два или несколько устройств или интерфейсов имели один и тот же адрес, в сети возникли бы коллизии, связанные с определением получателя фреймов.

Физический адрес является полезной информацией при обнаружении и устранении сетевых проблем. Например, по адресу можно найти создающий избыточный трафик неисправный сетевой интерфейс в компьютере или устройстве, после чего этот интерфейс можно заметить и обеспечить нормальное функционирование сети. Анализ адресов позволяет обнаружить в сети деятельность злоумышленников и найти их местоположение раньше, чем они нарушат безопасность сети.

Два типа сервисов используются для взаимодействия подуровня LLC и следующего, более высокого уровня стека - Сетевого уровня. Первый тип операций (Type 1) представлен *службой без установки соединения* (connectionless service), которая не требует наличия логического соединения между передающим и принимающим узлами. В этом случае не выполняется проверка очередности фреймов (чтобы они принимались в том же порядке, в котором передаются), отсутствует подтверждение приема фрейма и исправление ошибок.

Операции второго типа (Type 2) представлены *службой с установлением соединения* (connection-oriented service), для которой перед началом фактической передачи данных устанавливается логическая связь между передающим и принимающим узлами. Каждый фрейм содержит порядковый номер, который проверяется принимающим узлом, и это гарантирует то, что фреймы обрабатываются в том же порядке, в

котором они были посланы. Установленный канал связи обеспечивает скорость передачи информации (чтобы передающий узел не посылал данные чаще, чем их мог обработать принимающий узел). Принимающий узел дает подтверждение передающему узлу в получении посланной информации. При возникновении ошибок данные передаются повторно.

Сетевой уровень (3)

Третьим уровнем стека является *Сетевой уровень* (network layer). Этот уровень управляет прохождением пакетов по сети. Все сети содержат физические маршруты передачи информации (кабельные тракты) и логические маршруты (программные тракты). Сетевой уровень анализирует адресную информацию протокола передачи пакетов и посылает их по наиболее подходящему маршруту – физическому или логическому, обеспечивая максимальную эффективность сети. Также этот уровень обеспечивает пересылку пакетов между сетями через маршрутизаторы.

Контролируя прохождение пакетов, Сетевой уровень выступает в роли "управляющего трафиком": он маршрутизирует (направляет) пакеты по наиболее эффективному из нескольких возможных трактов передачи данных. Для определения наилучшего маршрута Сетевой уровень постоянно собирает информацию (метрики) о расположении различных сетей и узлов, этот процесс называется *обнаружением маршрута* (discovery).

Примечание

Не все протоколы содержат информацию, которая может использоваться сетевым уровнем, и это означает, что такие протоколы нельзя маршрутизировать. Примерами немаршрутизируемых протоколов являются протокол LAT фирмы Digital Equipment Corporation и протокол NetBEUI фирмы Microsoft. Чаще всего оба этих протокола не используются в средних и крупных сетях, требующих маршрутизации.

Примечание

Некоторые целевые адреса назначаются группам устройств. Пакет с групповым адресом маршрутизируется и передается нескольким компьютерам или сетевым устройствам.

Сетевой уровень может направлять данные по разным маршрутам, создавая виртуальные каналы (circuit). *Виртуальные каналы* (virtual circuit) представляют собой логические коммуникационные линии для передачи и приема данных. Виртуальные каналы, представленные только на сетевом уровне, образуются между сетевыми узлами, обменивающимися информацией. Поскольку Сетевой уровень управляет данными, поступающими по нескольким виртуальным каналам, то эти данные могут поступать в неправильной очередности. Для устранения этих издержек сетевой уровень проверяет и при необходимости корректирует порядок передачи пакетов перед отправкой их следующему уровню стека. Также на Сетевом уровне фреймы получают адреса, и выполняется форматирование фреймов в соответствии с сетевым протоколом принимающей стороны. Кроме того, обеспечивается передача фреймов с такой скоростью, чтобы принимающий уровень успевал обрабатывать их.

Совет

Знание принципов работы Сетевого уровня помогает обеспечить максимальную эффективность сети при ее разработке или эксплуатации. Например, в организации могут использоваться серверы, работающие с немаршрутизируемым протоколом, в результате чего из-за избыточного трафика в большой сети будут создаваться "заторы". Когда, в конце концов, серверы будут настроены на работу с маршрутизируемым протоколом, заторы исчезнут. Такое решение будет эффективным и недорогим.

Транспортный уровень (4)

Транспортный уровень (transport layer) – подобно Канальному и Сетевому уровням – выполняет функции, обеспечивающие надежную пересылку данных от передающего узла к принимающему. Например, Транспортный уровень гарантирует, что данные передаются и принимаются в одном и том же порядке. Кроме этого, по завершении пересылки принимающий узел может послать подтверждение (иногда называемое квитанцией).

Когда в сети используются виртуальные каналы, Транспортный уровень отслеживает уникальные идентификаторы, назначенные каждому каналу. Эти значения называются портами, идентификаторами соединения или сокетами; они назначаются Сеансовым уровнем. Также Транспортный уровень обеспечивает проверку пакетов. При этом на самом верхнем уровне контроля гарантируется безошибочная передача пакетов от узла к узлу в заданный промежуток времени.

Протоколы, используемые для взаимодействия на Транспортном уровне, реализуют несколько механизмов обеспечения надежности. Простейшим является протокол Класса 0. Он не выполняет никаких проверок на наличие ошибок и не управляет потоком данных, передавая эти функции Сетевому уровню. Протокол Класса 1 отслеживает ошибки передачи пакетов и при наличии ошибки запрашивает у Транспортного уровня передающего узла повторную передачу пакета. Протокол Класса 2 проверяет наличие ошибок, передачи и обеспечивает управление потоком данных между Транспортным и Сеансовым уровнями. Функция *управления потоком* (flow control) гарантирует скорость передачи данных, чтобы одно устройство не посылало информацию быстрее, чем ее сможет принять сеть или обработать принимающее устройство. Протокол Класса 3 обеспечивает функции Классов 1 и 2, а также возможность восстановления потерянных в некоторых случаях пакетов. И, наконец, протокол Класса 4 выполняет те же функции, которые обеспечивает Класс 3, осуществляя кроме этого более сложные операции по исправлению ошибок и восстановлению пакетов.

Еще одной функцией Транспортного уровня является деление посылаемых сообщений на более мелкие фрагменты в тех случаях, когда в сетях используются разные протоколы с отличающимися размерами пакетов. Данные, разбитые на мелкие блоки Транспортным уровнем передающей сети, собираются в правильном порядке Транспортным уровнем принимающей стороны и интерпретируются Сетевым уровнем.

Примечание

Именно Транспортный уровень обеспечивает получение каждого пакета или фрейма без потерь. Пользователи сотовых телефонов знают, что из-за наводок или помех могут пропадать куски фраз. Аналогичным образом в сети могли бы пропадать элементы данных при их слишком быстрой или слишком медленной передаче. Задача Транспортного уровня - обеспечить такую скорость передачи информации, чтобы не было ее потерь. Транспортный уровень также может регулировать размер "окон" данных, передаваемых между сигналами подтверждения приема, в результате чего объем переданных данных за единицу времени может увеличиться. Например, если компьютер посылает один пакет, а затем ждет в течение некоторого времени подтверждения от принимающей стороны, Транспортный уровень может увеличить "окно" так, чтобы между подтверждениями посылались четыре пакета, а не один, что в четыре раза ускорит передачу информации.

Сеансовый уровень (5)

Сеансовый уровень (session layer) отвечает за установление и поддержку коммуникационного канала между двумя узлами, он обеспечивает очередность работы узлов: например, определяет, какой из узлов первым начинает передачу данных. Помимо этого, Сеансовый уровень определяет продолжительность работы узла на передачу, а также способ восстановления информации после ошибок передачи. Если сеанс связи был ошибочно прерван на более низком уровне, Сеансовый уровень пытается восстановить передачу данных.

Совет

Работая в некоторых операционных системах, можно отключить рабочую станцию от сети, подключить ее заново и продолжить работу без повторной регистрации в сети. Это возможно благодаря тому, что Сеансовый уровень выполняет повторное подключение рабочей станции даже после временной приостановки работы Физического уровня.

Подобно тому, как почтовый индекс связан с некоторым географическим районом, Сеансовый уровень ассоциирует с каждым узлом уникальный адрес. По окончании сеанса связи этот уровень отключает узлы.

Примером связи на Сеансовом уровне может быть подключение рабочей станции к некоторому серверу Интернета. Станция и сервер имеют уникальные адреса протокола Интернета (IP)

(например, 122.72.15.122 и 145.19.20.22). Сеансовый уровень использует эти адреса для установки соединения между узлами. После того как подключение осуществлено, и рабочая станция зарегистрировалась на сервере, на данном уровне устанавливается сеанс передачи данных.

Сеансовый уровень позволяет так выполнять передачу данных по сети, что ее производительность можно увеличить в два раза. Например, устройства, работающие на Сеансовом уровне, могут передавать и принимать данные, однако не одновременно. Для Сеансового уровня этот способ передачи называется двусторонним альтернативным (two-way alternative, TWA) режимом для управления диалогом. Но кроме этого, Сеансовый уровень позволяет соединить эти устройства для одновременного приема-передачи, что вдвое увеличивает скорость передачи данных при сеансовом диалоге между двумя узлами. Этот режим называется двусторонним одновременным (two-way simultaneous, TWS).

Совет

При развертывании сети приобретайте сетевые интерфейсы и устройства, обеспечивающие полнодуплексный (двунаправленный) режим работы, поскольку в этом случае можно значительно повысить эффективность сети.

Представительский уровень (6)

Представительский уровень (presentation layer) управляет форматированием данных, поскольку прикладные программы нередко используют различные способы представления информации. В некотором смысле Представительский уровень выполняет функции программы проверки синтаксиса. Он гарантирует, что числа и символьные строки передаются именно в том формате, который понятен Представительскому уровню принимающего узла. Например, данные, посылаемые от мэйнфрейма компании IBM, могут кодироваться в символьном формате EBCDIC, который необходимо преобразовать в символы ASCII, если данные должны читаться рабочими станциями под управлением систем Windows XP или Red Hat Linux.

Также Представительский уровень отвечает за шифрование данных. *Шифрование* (encryption) – это такой процесс засекречивания информации, который не позволяет неавторизованным пользователям прочесть данные в случае их перехвата. Например, в локальной сети может шифроваться пароль учетной записи компьютера, или же номер кредитной карточки может шифроваться с помощью технологии *Secure Sockets Layer (SSL)* (Протокол защищенных сокетов) при передаче по глобальной сети. Безопасность представительского уровня более подробно рассматривается в практическом задании 2-4.

Примечание

Технологии шифрования являются гарантией успешной торговли через Интернет. При их отсутствии мало бы кто решился делать покупки через Интернет используя кредитные карточки.

Еще одной функцией Представительского уровня является сжатие данных
После их форматирования между символьными строками и числами может оставаться свободное место. При сжатии информации эти промежутки удаляются, в результате чего требуется значительно меньше времени на передачу более компактных данных. После пересылки Представительский уровень принимающего узла выполняет декомпрессию данных.

Прикладной уровень (7)

Самым высоким в модели OSI является *Прикладной уровень* (application layer). Этот уровень непосредственно управляет доступом к приложениям я сетевым службам. Примером таких служб являются передача файлов, управление файлами, удаленный доступ к файлам и принтерам, управление сообщениями электронной почты и эмуляция терминалов. Именно этот уровень программисты используют для связи рабочих станций с сетевыми службами (например, для предоставления некоторой программе услуг электронной почты или доступа к базе данных через сеть).

На Прикладном уровне работает *редиректор* (redirector) систем Microsoft Windows. Редиректор – это служба, позволяющая видеть компьютер в сети и обращаться к нему. Если в сети Microsoft

разрешается общий доступ к некоторой папке, то при помощи редиректора другие компьютеры могут видеть эту папку и использовать ее. Работа редиректора в системах Windows 2000 или XP демонстрируется в практическом задании 2-5.

Примечание

Многие широко используемые компьютерные программы реализованы благодаря наличию Прикладного уровня. Всякий раз, когда вы запускаете веб-браузер (например, Microsoft Internet Explorer или Netscape Communicator) или же посылаете сообщение по электронной почте, вы работаете с Прикладным уровнем.

В табл. 2.1 представлены функции каждого из семи уровней модели OSI.

Таблица 2.1. *Функции уровней эталонной модели OSI*

Уровень	**Функции**
Физический (Уровень 1)	Реализует физическую среду передачи сигнала (например, кабельную систему) Преобразует данные в передаваемый сигнал, соответствующий физической среде Посылает сигнал по физической среде Распознает физическую структуру сети Обнаруживает ошибки передачи Определяет уровни напряжения, используемые для передачи цифровых сигналов и синхронизации передаваемых пакетов Определяет тип сигнала - цифровой или аналоговый
Канальный (Уровень 2)	Образует фреймы данных соответствующего формата с учетом типа сети Генерирует контрольные суммы Обнаруживает ошибки, проверяя контрольные суммы Повторно посылает данные при наличии ошибок Инициализирует канал связи и обеспечивает его бесперебойную работу, что гарантирует физическую надежность коммуникаций между узлами Анализирует адреса устройств Подтверждает прием фреймов
Сетевой (Уровень 3)	Определяет сетевой маршрут для передачи пакетов Позволяет уменьшить вероятность перегруженности сети Реализует виртуальные каналы (маршруты) Маршрутизирует пакеты в другие сети, при необходимости переупорядочивая передаваемые пакеты Выполняет преобразования между протоколами
Транспортный (Уровень 4)	Обеспечивает надежность передачи пакетов между узлами Обеспечивает правильный порядок передачи и приема пакетов данных Подтверждает прием пакета Отслеживает ошибки передачи пакетов и повторно посылает плохие пакеты Разбивает большие фрагменты данных и собирает их на приемном узле в сетях, использующих разные протоколы
Сеансовый (Уровень 5)	Инициирует канал связи Проверяет состояние установленного канала связи В каждый момент времени определяет очередность работы узлов, (например, какой узел первым начинает передачу данных) Разрывает канал по окончании сеанса связи

Уровень	Функции
	Преобразует адреса узлов
Представительский (Уровень 6)	Преобразует данные *в* формат, понятный для принимающего узла (например, перекодирует символы EBCDIC в ASCII) Выполняет шифрование данных Выполняет сжатие данных
Прикладной (Уровень 7)	Обеспечивает совместный доступ к удаленным дискам Обеспечивает совместный доступ к удаленным принтерам Обрабатывает сообщения электронной почты Обеспечивает работу служб передачи файлов Обеспечивает работу служб управления файлами Обеспечивает работу служб эмуляции терминалов

Взаимодействие между стеками протоколов

Для того чтобы два компьютера могли взаимодействовать между собой в локальной или глобальной сети, они оба должны использовать одну и ту же модель коммуникаций (например, модель OSI). Эта модель определяет стандарты взаимодействия как внутри локальной сети, так и при передаче данных между локальными сетями, между локальной и глобальной сетями, а также между

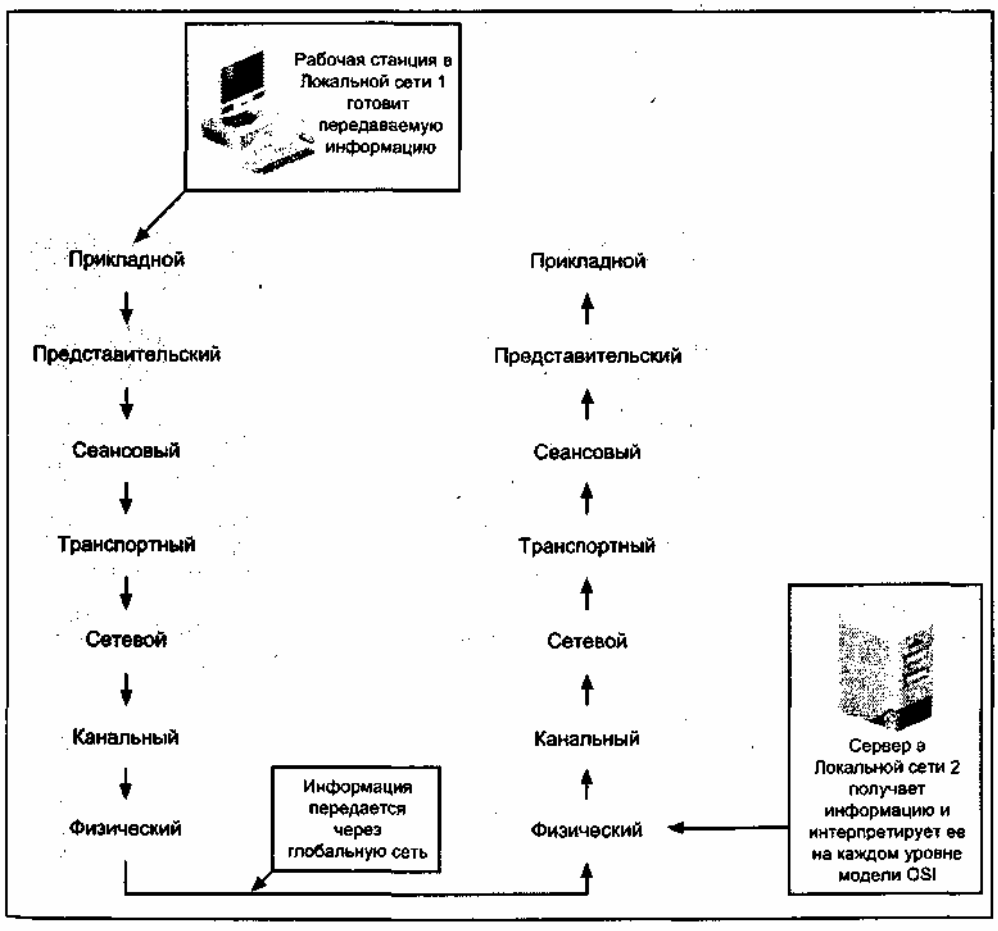


Рис. 2.4. Передача информации с использованием эталонной модели OSI

глобальными сетями.

Сформированная информация начинает свой путь на верхушке стека передающего узла на Прикладном уровне. Затем данные передаются Представительскому уровню и продолжают движение по стеку до Физического уровня, где они посылаются в сеть в виде законченного информационно сигнала (рис. 2.4).

1 Принимающий узел получает данные на Физическом уровне (на самом нижнем уровне стека), а затем для проверки фреймов передает отдельные порции информации Канальному уровню, который определяет, адресован ли конкретный фрейм сетевому интерфейсу данного узла. Канальный уровень действует

как почтальон, просматривающий всю почту и выбирающий письма, посланные на конкретный адрес. Письма с этим адресом забираются и передаются конкретному адресату, проживающему по данному адресу. Остальные письма отправляются дальше до тех пор, пока не найду своего адресата.

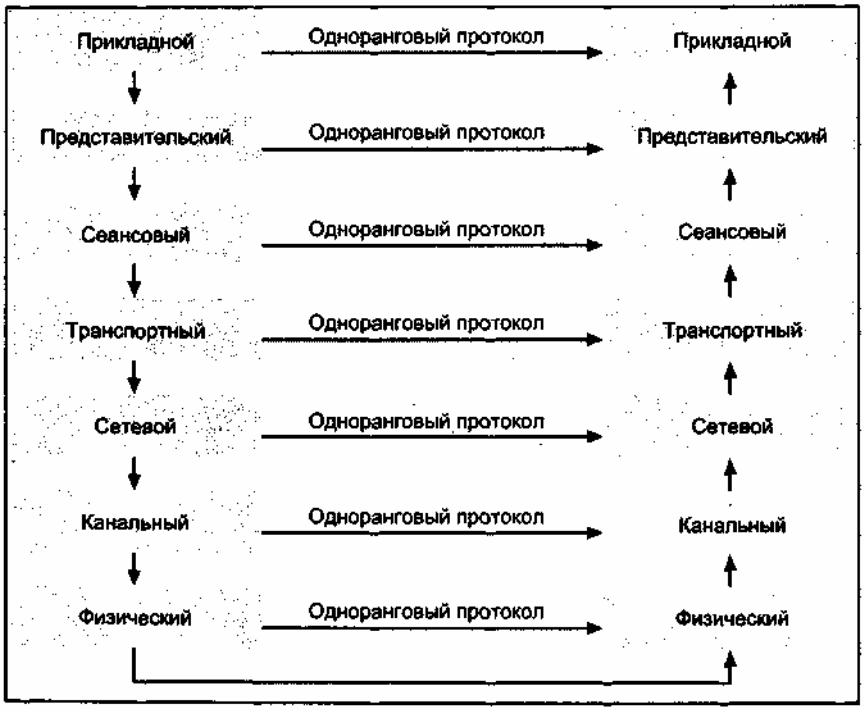


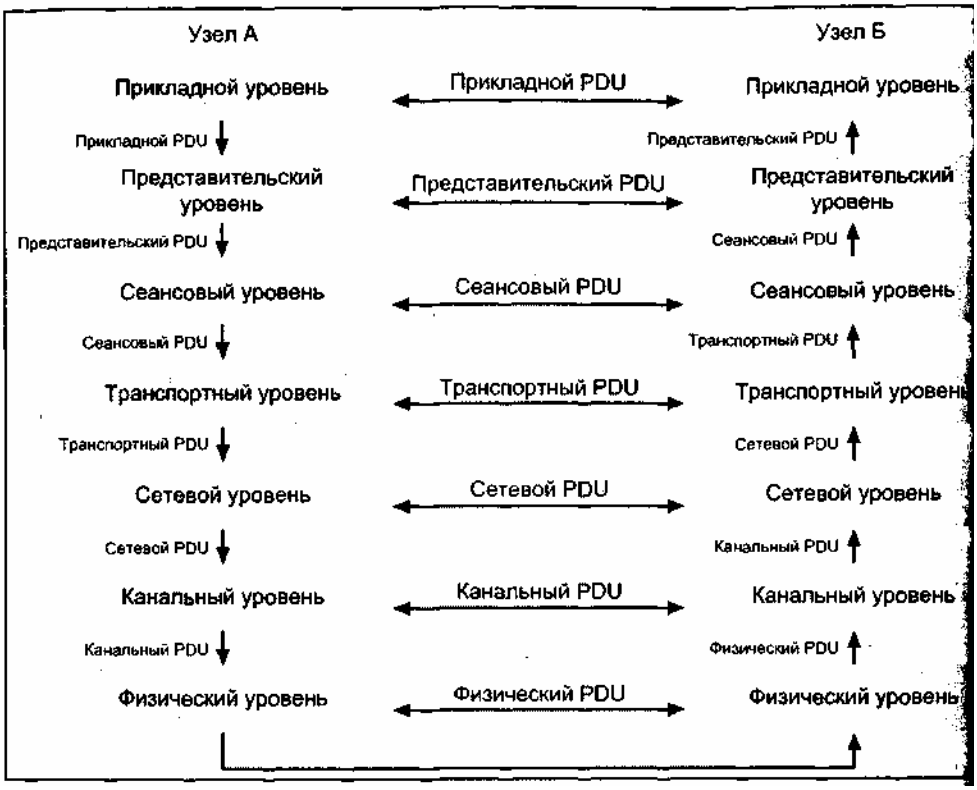
Рис. 2.5. Одноранговые протоколы, обеспечивающие взаимодействие между одинаковыми уровнями

Когда Канальный уровень обнаруживает фрейм, адресованный данной рабочей станции, он передает его сетевому уровню, который отсортировывает предназначенную ему информацию и посылает оставшиеся данные выше по стеку. Однако перед тем как фрейм будет передан от Канального уровня к Сетевому, Канальный уровень проверит контрольную сумму (CRC) и определит целостность фрейма.

Каждый уровень стека действует как самостоятельный модуль, выполняющий одну основную функцию, и каждый уровень имеет собственный, формат команд передачи данных, определяемый соответствующим протоколом. Протоколы, используемые для связи функций, относящихся к одному и тому же уровню, называются протоколами взаимодействия равноправных систем (peer protocol) или одноранговыми протоколами (рис. 2.5). *Одноранговые протоколы* позволяют некоторому уровню О81,на передающем узле взаимодействовать с таким же уровнем принимающего узла. Например, когда Канальный уровень передающего узла генерирует контрольные суммы, он использует одноранговый протокол, который будет понятен Канальному уровню принимающего узла.

Между уровнями информация передается при помощи команд, называемых *примитивами* (primitive) (рис. 2.6). Передаваемая информация называется *протокольной единицей обмена* или *модулем данных протокола* (protocol data unit, PDU). Когда данные поступают от одного уровня к другому (более высокому или более низкому), к модулю PDU добавляется новая управляющая информация. После того как на некотором уровне сформирован модуль PDU, он пересылается аналогичному уровню взаимодействующего узла с помощью одноранговых протоколов (рис. 2.7). Вместе с тем когда модуль PDU готов к передаче следующему уровню, предыдущий уровень добавляет к этому модулю команды пересылки.

Рис. 2.6. Взаимодействие между уровнями с применением примитивов



Взаимодействие между уровнями с использованием модулей PDU

После того как модуль PDU принимается следующим уровнем, управляющая информация и команды пересылки отбрасываются. Полученный называется *модулем данных службы* (service data unit, SDU). В процессе пересылки модуля SDU от одного уровня к следующему каждый уровень добавляет к модулю свою управляющую информацию.

Совет

На каждом уровне OSI для получения модуля PDU к нужному модулю SDU добавляются управляющая информация и команды пересылки. Если, например, модуль PDU формируется на некотором уровне компьютера А, то затем он пересылается этому же уровню компьютера Б. Если же на компьютере А проходит взаимодействие между уровнями стека, то модуль PDU передается следующему уровню стека, расположенному ниже. Управляющая информация и команды пересылки удаляются из модуля PDU, остается только модуль SDU, после чего добавляется новая управляющая информация.

Применение модели OSI

В качестве примера коммуникаций с использованием многоуровневой модели рассмотрим процесс обращения рабочей станции к общему диску, расположенному на сервере в другой сети. Редиректор

рабочей станции на Прикладном уровне находит общий сетевой диск. Представительский уровень обеспечивает форматирование данных в кодах ASCII (этот формат использует как рабочая станция, так и сервер). Сеансовый уровень устанавливает связь между двумя компьютерами и обеспечивает его устойчивость в течение всего времени, пока рабочая станция обращается к содержимому общего диска. Транспортный уровень устраняет все ошибки передачи или приема, гарантируя сохранение последовательности пересылки и интерпретации данных. Сетевой уровень обеспечивает передачу пакетов по кратчайшему маршруту для уменьшения задержек. Канальный уровень форматирует фреймы и следит за тем, чтобы они передавались нужной рабочей станции (используя физические адреса). И, наконец, Физический уровень осуществляет передачу данных, преобразуя информацию в электрические сигналы, посылаемые в сетевой коммуникационный кабель. Фреймы и пакеты по мере их формирования адаптируются для осуществления связи локальных сетей через глобальную сеть, для чего используется инкапсуляция или эмуляция ЛВС, о чем рассказывалось в *главе 1*.

Модель OSI также применяется к сетевым взаимодействиям между аппаратными и программными средствами. Чтобы отвечать принятым стандартам, эти средства должны работать на определенных уровнях модели OSI. Подробно сетевое оборудование будет обсуждаться в *главе 4,* однако в табл. 2.2 кратко описано соответствие сетевых аппаратных и программных средств Уровням модели OSI.

Таблица 2.2. *Сетевые аппаратные и программные средства, связанные с различными уровнями модели OSI*

Уровень OSI	**Сетевые аппаратные и программные средства**
Прикладной	Прикладные программные интерфейсы, браузеры Интернета, программы передачи сообщений и электронной почты, программы удаленного доступа к компьютерам и шлюзы
Представительский	Программы преобразования и шифрования данных, программы форматирования графики (например, для преобразования в GIF- и JPG-файлы), а также шлюзы
Сеансовый	Программные драйверы сетевого оборудования, программное обеспечение для поиска имен компьютеров, средства для полу- и полнодуплексного режима работы, средства удаленного вызова процедур (RPC) для запуска программ на удаленном компьютере, а также шлюзы
Транспортный	Программные драйверы сетевого оборудования, программы и средства управления потоком данных, а также шлюзы
Сетевой	Шлюзы, маршрутизаторы, протоколы маршрутизации, мосты с исходными маршрутами и коммутаторы Уровня 3
Канальный	Сетевые адаптеры, интеллектуальные концентраторы и мосты, коммутаторы Уровня 2 и шлюзы
Физический	Кабельная система, кабельные разъемы, мультиплексоры, трансмиттеры и ресиверы, пассивные и активные концентраторы, репитеры и шлюзы

Примечание

Нередко шлюзы выполняют в сети ограниченные или строго определенные функции. В результате этого встречается все меньше и меньше реализации "чистых" шлюзов (за исключением программных шлюзов электронной почты поскольку другие устройства, такие как мосты, маршрутизаторы и коммутаторы предлагают дополнительные функции. Исторически сложилось, что определение шлюза довольно широкое, и шлюзы могут работать на любом уровне модели OSI.

Успешно функционирующие локальные сети следуют рекомендациям, установленным моделью OSI. Две основных характеристики локальной сети – тип (топология) сети и методы передачи данных – являются обязательными критериями, подтверждающими, что сети соответствуют стандартам.

Типы сетей

Любая сеть состоит из совокупности кабелей, сетевого оборудования, файловых серверов, рабочих станций и программного обеспечения. Комбинируя эти элементы, можно создать сеть, соответствующую задачам и возможностям конкретной организации. Первоначальная установка некоторых типов сетей не требует больших расходов, однако расходы появляются при эксплуатации или модернизации. Другие сети, наоборот, требуют значительных капиталовложений на этапе развертывания, но они просты в обслуживании их легко расширять.
Одним из важнейших различий между разными типами сетей является их топология. Топология – это физическая конфигурация сети в совокупности с ее логическими характеристиками. Физическая конфигурация подобна плану разводки кабелей в офисе, здании или кампусе. Иногда ее называют *кабельным участком* (cable plant). Логические характеристики сети описывают способ передачи сигнала по кабелю от одной точки к другой.

Конфигурация сети может быть или децентрализованной (когда кабель "обегает" каждую станцию в сети), или централизованной (когда каждая станция физически подключается к некоторому центральному устройству, распределяющему фреймы и пакеты между станциями). Примером централизованной конфигурации является звезда с рабочими станциями, располагающимися на концах ее лучей. Децентрализованная конфигурация похожа на цепочку альпинистов, где каждый альпинист имеет свое положение в связке, а все вместе соединены одной веревкой. Логические характеристики топологии сети определяют маршрут, проходимый пакетом при передаче по сети.

Существуют три основных топологии: шина, кольцо и звезда. При выборе топологии необходимо, чтобы тип сети соответствовал ее предназначению внутри организации. Например, некоторые организации более интенсивно используют свои сети по сравнению с другими. Количество и тип прикладных программ внутри организации влияют на количество и частоту передачи фреймов и пакетов, что в совокупности образует *сетевой трафик*. Если пользователи сети в первую очередь работают с текстовыми редакторами, то сетевой трафик будет относительно небольшим и большая часть работы будет выполняться на рабочих станциях, а не в сети.

Клиент-серверные приложения в зависимости от своей архитектуры создают сетевой трафик средней и высокой интенсивности. В сетях, в которых происходят частые обращения к базам данных, таким как Microsoft SQL Server или Oracle, трафик средний или высокий. Научные программы и серверы публикаций создают трафик высокой интенсивности, поскольку они работают с очень большими файлами. Также большой трафик вызывает работа программ обработки графики (например, серверы потокового мультимедиа или телеконференций).

Влияние на сеть количества хостов и серверов определяется типом используемых прикладных программ. К примеру, сервер базы данных, к которому часто обращаются для получения отчетов и финансовых сведений, будет создавать значительно больший сетевой трафик, чем файловый сервер, с которого изредка получают деловую корреспонденцию или бланки писем.
При выборе топологии сети нужно учитывать, будет ли она связана с другими сетями. Сетевая топология для малого предприятия, в котором используются несколько компьютеров, отличается от топологии сети промышленного предприятия, связанного через глобальную сеть с сетями других предприятий. Малое предприятие вряд ли взаимодействует с другими сетями, за исключением разве что подключения к Интернету. Корпоративная сеть может состоять из нескольких взаимно связанных сетей, в число которых, например, могут входить сеть для управления производственным оборудованием, сеть настольных систем, исследовательская сеть и внешняя глобальная сеть для связи с удаленными площадками. Одни топологии имеют лучшие возможности для объединения сетей, чем другие.

Сеть с большим трафиком нуждается в высокоскоростных каналах передач данных. От скорости сети зависит производительность работы пользователей. Наличие быстродействующих каналов особенно важно при передач изображений, графики и других объемных файлов на большие расстояний или через глобальные сети.

Безопасность, представляющая собой механизм защиты данных от неавторизованного доступа, также влияет на архитектуру сети. В безопасной сет для ограничения доступа к информации и ресурсам используются специальные сетевые устройства, пароли, управляющие программы и другие технологии. Можно также применять шифрование данных и паролей, копи фреймы и пакеты кодируются, и только авторизованные компьютеры могут декодировать их. В сетях с высокой степенью защиты используется оптоволоконный кабель, который минимизирует риск перехвата данных. Другой способ повысить защищенность сети – поместить оборудование и сервер в помещения с ограниченным доступом (например, в серверные комнаты; монтажные шкафы).

Топология сети непосредственно влияет на возможность ее расширения. После установки сети наверняка потребуется подключение новых пользователей, в том же офисе или в других помещениях или зданиях. Также весьма вероятно, что для удаленного доступа к данным потребуется подключи локальную сеть к какой-нибудь глобальной сети.

Шинная топология

Шинная топология (bus topology) представляет собой кабель, последователь соединяющий компьютеры и серверы в виде цепочки. Как и обычная цен сеть с шинной топологией имеет начальную и конечную точки, и к каждому концу сегмента шинного кабеля подключается *терминатор* (terminator). Передаваемый пакет принимается всеми узлами сегмента и на прохождения всего сегмента требуется некоторое количество времени, называемое задержкой. Для того чтобы пакеты доходили в течение ожидаемого времени, длина сегмента сети с шинной топологией должна соответствовать спецификациям Института инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE) *(см. главу 3).* Этот институт представляет собой объединение ученых, инженеров, технических специалистов и преподавателей, играющих ведущую роль в разработке стандартов на сетевые кабельные системы и средства передачи данных. На рис. 2.8 изображена простейшая сеть с шинной топологией.

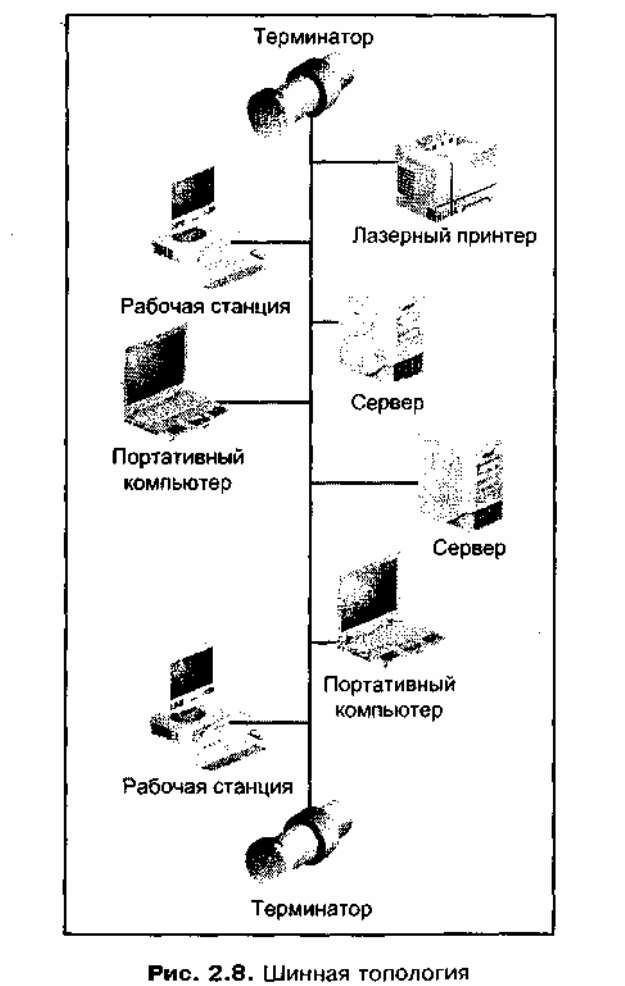


Рис. 2.8. Шинная топология

Наличие терминатора обязательно для шинной топологии, поскольку терминатор указывает на физическое окончание сегмента. На практике терминатор представляет собой электрическое

сопротивление, гасящее сигнал когда тот достигает конца сети. Без терминатора сегмент не соответствовал бы спецификациям IEEE и сигналы могли бы отражаться обратно и воз вращаться в тот кабель, по которому они были переданы. Отраженный сигнал сбивает синхронизацию сети и может столкнуться с новыми сигналами передаваемыми по сети.

Совет

Если терминатор отсутствует или работает неправильно, передача данных по соответствующему сегменту сети нарушается и сетевое оборудование обычно отключает этот сегмент.

Традиционная шинная топология, показанная на рис. 2.8, хорошо работает небольших сетях, и стоимость ее реализации относительно невелика. При развертывании сети расходы минимальны, поскольку кабеля требуется меньше, чем для других топологий. Также легко можно добавить новые рабочие станции и немного удлинить шину в пределах комнаты или офис. Недостатком этой топологии является высокая стоимость ее эксплуатации. Например, трудно обнаружить отдельный неисправный узел или сегмент кабеля и связанные с ним разъемы, а один отказавший узел или сегмент с разъемами может вывести из строя всю сеть (хотя современное сетевое оборудование уменьшает вероятность такой ситуации). Другим недостатком является то, что трафик по шине может оказаться слишком большим, из-за чего для управления им потребуются дополнительные коммутаторы, маршрутизаторы и другое оборудование.

Примечание

Традиционная шинная топология используется все реже и реже, поскольку некоторые производители сетевого и компьютерного оборудования больше не поддерживают применяемые в ней методы передачи сигналов.

Кольцевая топология

Кольцевая топология (ring topology) представляет собой непрерывную магистраль для передачи данных, не имеющую логической начальной или конечной точек и, следовательно, терминаторов. Рабочие станции и серверы подключаются к кабелю в точках, расположенных по кольцу (рис. 2.9). Когда данные поступают в кольцо, они передаются по нему от узла к узлу, пока не достигнут точки назначения, после чего перемещаются дальше к узлу отправителю.

Первоначально кольцевая топология позволяла данным перемещаться только в одном направлении, при этом данные обегали кольцо и передача заканчивалась в передающем (исходном) узле. В новых высокоскоростных технологиях кольцевых сетей используются два кольца для дополнительной передачи данных в обратном направлении. В результате этого, если разрывается кольцо передачи в одном направлении, данные все же могут достигнуть пункта назначения, перемещаясь в обратном направлении по другому кольцу (о чем будет рассказано позже в разделе, описывающем технологию FDDI).

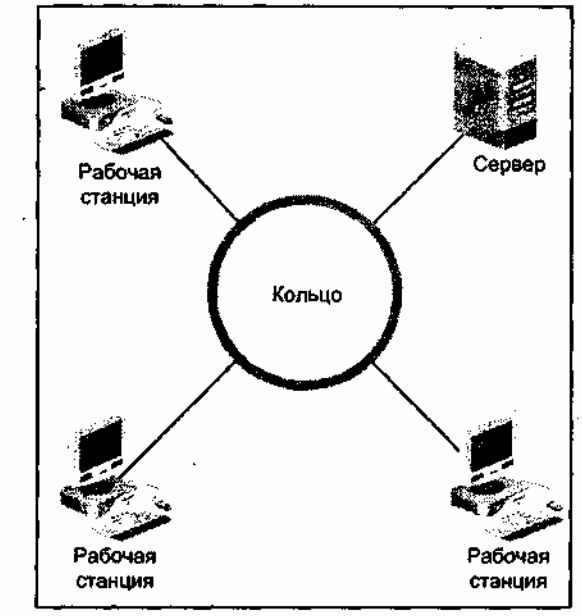


Рис. 2.9. Кольцевая топология

Кольцевой топологией легче управлять, чем шинной, поскольку оборудование, используемое для построения кольца, упрощает локализацию дефектного узла или неисправного кабеля. Данная топология хорошо подходит для передачи сигналов в локальных сетях, поскольку она справляется с большим сетевым трафиком лучше, чем шинная топология. В целом можно сказать, что по сравнению с шинной топологией, кольцевая обеспечивает более надежную передачу данных.

Однако кольцевая топология намного дороже шинной. Обычно для ее развертывания требуется больше кабеля и сетевого оборудования. Кроме того, Кольцо не так широко распространено как шинная топология, из-за чего ограничен выбор оборудования и меньше возможностей для осуществления высокоскоростных коммуникаций.

Звездообразная топология

Звездообразная топология (star topology), или просто "звезда", является старейшим способом передачи сигналов, имеющим свое начало в коммутационных телефонных станциях. Несмотря на возраст, достоинства при использовании в сетях делают звездообразную топологию удачным выбором для современных сетей. Физически звездообразная топология состоит из множества узлов, подключенных к центральному концентратору. Каким образом рабочие станции и сервер подключены к концентратору, показано на рис. 2.10. *Концентратор* (hub) – это центральное устройство, объединяющее в сеть отдельные кабельные сегменты или отдельные локальные сети. Некоторые концентраторы также называются элементами доступа (access unit) Отдельные сегменты передающего кабеля расходятся от концентратора как звезда (выполните практическое задание 2-6 и создайте диаграмму звездообразной топологии).

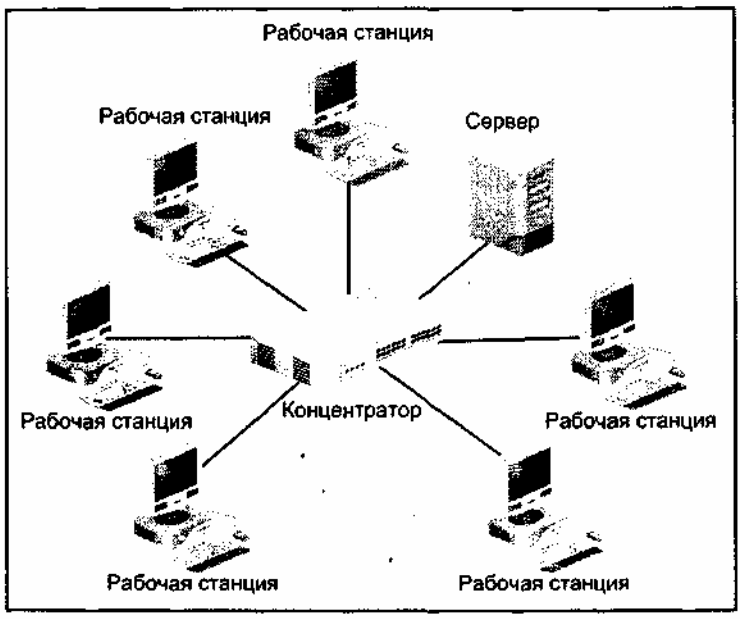


Рис. 2.10. Звездообразная топология

В настоящее время начальные затраты на реализацию звездообразной топологии ниже, чем для традиционной шинной топологии и сравнимы с рая ходами на создание кольца. Это объясняется понижением цен на сетевое оборудование и кабель, вызванным широким распространением этой архитектуры. Как и кольцо, звездообразная топология проще в управлении, чем традиционная шинная сеть (отказавшие узлы обнаруживаются очень быстро). Если узел или кабель неисправны, сетевое оборудование легко может изолировать их от сети и работоспособность других узлов не нарушится. Звезду легче расширить, подключив дополнительные узлы или сети. Также она наилучшим образом может быть модернизируема для работы на больших скоростях. Звезда – это наиболее распространенная топология и поэтому для нее существует широкий выбор оборудования.

Недостатком звезды является то, что концентратор является единственной точкой отказа: при выходе его из строя все подключенные узлы теряют возможность передачи данных (если отсутствуют дополнительные меры обеспечения избыточности). Другим недостатком является то, что для звезды требуется больше кабеля, чем для шины; однако кабели и разъемы для звездообразной топологии в настоящее время дешевле, чем для шинной.

Реализация шинной топологии в виде физической звезды

В современных сетях логическая организация сети с применением шинной топологии совмещается с физической реализацией в виде звезды. При такой архитектуре каждый луч звезды функционирует как отдельный сегмент логической шины, имеющий только один или два подключенных компьютера. Такой сегмент шины по-прежнему имеет два конца, однако преимуществом является отсутствие терминаторов. В данном случае один конец сегмента заканчивается на концентраторе, а другой – на сетевом устройстве.

Другим достоинством комбинированной архитектуры является то, что для расширения сети в разных направлениях можно соединить несколько концентраторов при условии выполнения спецификаций IEEE на длину кабелей, количество концентраторов и подключенных устройств. Соединение между концентраторами представляет собой магистраль, которая чаще всего обеспечивает высокоскоростную передачу данных между ними. *Магистраль* (backbone) – это быстродействующая среда передачи информации, соединяющая сети и центральные сетевые устройства в масштабах этажа, всего здания или нескольких удаленных площадок.

Для упрощения процесса обнаружения неисправностей концентраторы имеют специальные встроенные средства. Также имеются возможности расширения для реализации высокоскоростных сетей. Поскольку описываемая архитектура широко распространена, то для шинных сетей, реализованных в виде физической звезды, имеется большой выбор оборудования.

Методы передачи данных в локальных сетях

Существуют два основных способа передачи данных в локальных сетях: Ethernet и маркерное кольцо (token ring). Они стандартизованы в IEEE комитетами 802 и Project 802. Ethernet описан как стандарт локальных сетей в спецификациях IEEE 802.3, а маркерное кольцо – в спецификациях IEEE 802.5. Оба способа используются широко, однако число инсталляций с применением Ethernet больше, поскольку этот метод имеет самые широкие возможность для расширения и реализации высокоскоростных технологий. Также в данном разделе описан третий метод передачи данных в локальных сетях – Fiber Distributed Data Interface, FDDI (Распределенный интерфейс передачи данных по волоконно-оптическим каналам), представляющий собой модификацию маркерного кольца для высокоскоростных коммуникаций.

Ethernet

Стандарт Ethernet использует преимущества шинной и звездообразной то) пологий. На момент написания книги скорости передачи по сетям Ethernet составляли: 10 Мбит/с, 100 Мбит/с, 1 Гбит/с и 10 Гбит/с. В стандарте Ethernet используется метод управления доступом под названием *Carrier Sense Multiple Access with Collision Detection,* CSMA CD (Множественный доступ контролем несущей и обнаружением конфликтов). CSMA CD – это алгоритм передачи и декодирования форматированных фреймов данных. С помощью данного алгоритма посылающий узел сети Ethernet инкапсулируя фрейм и готовит его для передачи. Все узлы, стремящиеся отправить фрейм в кабель, соревнуются между собой. Ни один узел не имеет преимуществ перед другими узлами. Узлы прослушивают наличие пакетов в кабеле. Если обнаруживается передаваемый пакет, то узлы, не стоящие в очередь на передачу, переходят в режим "ожидания".

Протокол Ethernet в каждый момент времени позволяет только одному узлу работать на передачу. Для передачи генерируется сигнал несущей частот *Контроль несущей* – это процесс проверки коммуникационного кабеля на наличие определенного напряжения, указывающего на наличие сигнал передающего данные. Если в течение заданного интервала времени в среде передачи отсутствует информационный сигнал, любой узел может начать передачу данных.

Иногда несколько узлов начинают передачу одновременно, что приводит к *конфликту.* Передающий узел обнаруживает конфликт, проверяя уровень сигнала. В случае конфликта сигнал по крайней мере в два раза превышает нормальный. Для разрешения конфликтов пакетов передающий узел использует программный алгоритм обнаружения конфликтов. Этот алгоритм разрешает станциям, отправляющим пакеты, продолжать передачу в течение установленного промежутка времени. При этом передается сигнал помехи, состоящий из двоичных единиц, и по этому сигналу все слушающие сеть узлы определяют наличие конфликта. Затем на каждом узле программно генерируется случайное число, которое используется как время ожидания для начала следующей передачи. Такой подход является гарантией того, что два узла не начнут одновременно повторную передачу данных.

При передаче фреймов заданному узлу используются физические адреса. Каждая станция и сервер имеет уникальный адрес Уровня 2, связанный с сетевым адаптером (network interface card, NIC). Этот адаптер соединяет станцию или сервер с сетевым коммуникационным кабелем. Адрес "зашивается" в микросхему ПЗУ, расположенную на адаптере.

Компьютерная логика, выполняющая описанные выше функции, реализована в виде программ и соответствующих файлов, называемых сетевыми драйверами. Каждый сетевой адаптер требует наличия специальных сетевых драйверов, соответствующих методу доступа к сети, формату инкапсулируемых данных и способу адресации. Драйвер устанавливается на компьютере.

Данные, передаваемые в стандарте Ethernet, помещаются во фреймы (рис. 2.11). Каждый фрейм состоит из строго определенных фрагментов (полей). Первый фрагмент – заголовок (preamble), имеет длину 56 бит. Заголовок синхронизирует передачу фрейма и состоит из перемещающейся последовательности нулей и единиц. Следующее поле – 8-битный разграничитель фреймов (называемый SFD или SOF). Признак начала фрейма имеет значение 10101011 и указывает на то, что далее во фрейме следует адресная информация. За этим признаком помещаются два адресных поля, содержащих адреса назначения и источника. Согласно рекомендациям IEEE 802.3, адресные поля могут иметь длину 16 или 48 бит (обычно 48). Имеются два адреса: адрес источника (source address, SA), представляющий собой адрес передающего узла, и адрес назначения (destination address, DA), являющийся адресом принимающего узла. Далее 16-битное поле указывает длину поля данных (идущего следом).

Заголовок	SFD	Адрес назначения	Адрес источника	Длина	Данные и поле-заполнитель	FCS
56	8	16 или 48	16 или 48	16	368–12000	32

Рис. 2.11. Побитовое представление формата фрейма 802.3

Раздел данных во фрейме идет вслед за полем длины. Длина инкапсулированных данных должна быть кратна 8 (одному байту). Если реальные данные имеют длину менее 368 бит или не кратны 8, добавляется поле-заполнитель. Длина поля данных с заполнителем может быть от 368 до 12 000 бит (или от 46 до 1500 байт). Последний фрагмент фрейма – поле контрольно последовательности (суммы) фрейма (frame check sequence, FCS), имеющее длину 32 бита. Для обнаружения ошибок это поле содержит значение дм контроля с помощью циклического избыточного кода (CRC). Это значение вычисляется на основе значений других полей фрейма в момент инкапсуляции данных. При приеме фрейма он пересчитывается заново. Если результат повторного вычисления не совпадает с исходным, генерируется ошибка и принимающий узел запрашивает повторную передачу данного фрейм. Если результаты вычислений совпадают, алгоритм получения контрольно суммы указывает на то, что повторная передача не требуется. Алгоритм CRC определяется стандартом IEEE.

Ethernet II – метод форматирования фреймов Ethernet, используемый в Интернете и других современных сетях, немного отличающихся от традиционного стандарта IEEE 802.3 (однако в настоящее время признанный часть стандарта IEEE 802.3 и описанный в RFC 894), для повышения эффективности сетевых коммуникаций. В фрейме Ethernet II заголовок имеет длим 64 бита и содержит как информацию для синхронизации фреймов, так и признак начала фрейма (SOF). Адреса назначения и источника во фрейм Ethernet II имеют длину точно 48 бит, как показано на рис. 2.12.

Заголовок и SOF	Адрес назначения	Адрес источника	Тип	Данные	FCS
64	48	48	16	368–12000	32

Рис. 2.12. Побитовое представление формата фрейма Ethernet II (DIX)

Примечание

Фрейм Ethernet II иногда называют DIX-фреймом по названию трех компаний первоначально разработавших эту технологию: Digital (Digital Equipment Compapy, позднее приобретенной компанией Compaq), Intel и Xerox.

Во фрейме Ethernet II вместо поля длины используется 16-битное поле типа, предназначенное для сетевых коммуникаций более высокого уровня. Поле данных инкапсулируется без поля-заполнителя и его длина в диапазоне от 368 до 12 000 бит. Переменный размер поля используется для улучшенного обнаружения конфликтов пакетов и оптимизации загрузки сети, чтобы длинные пакеты не занимали сеть в течение слишком большого времени. Последнее поле фрейма Ethernet II – 32-битное поле контрольной суммы фрейма (FCS). С помощью этого поля по тому же алгоритму, как и в традиционном стандарте 802.3, выполняется контроль CRC.

Совет

Во избежание коммуникационных проблем не используйте фреймы Ethernet II и 802.3 для одних и тех же узлов в пределах одной сети.

Как указано в стандарте IEEE 802.3 для коммуникаций на подуровне LLC канального уровня, оба фрейма (802.3 и Ethernet II) могут содержать три необязательных поля между полем длины или типа и полем данных: поле целевой точки доступа к службе (destination service access point, DSAP), поле исходной точки доступа к службе (source service access point, SSAP) и поле управления. Эти поля позволяют Канальному уровню управлять фреймами и взаимодействовать с более высокими уровнями модели OSI. Поля DSAP и SSAP имеют длину 8 бит. Точки доступа к службе (SAP)

позволяют сетевому уровню определять, какой сетевой процесс узла назначения должен получать фрейм. Эти точки представляют такие коммуникационные процессы, как OSI, Novell, NetBIOS, TCP IP, BPDU, управление сетями IBM, XNS и другие (описываемые в этой книге). Например, шестнадцатеричное значение EO указывает на Novell SAP, а значение 06 – на SAP стека TCP IP. DSAP указывает точку доступа к службе на целевом узле, который должен принимать фрейм, а SSAP идентифицирует точку доступа к службе передающего узла, который отправляет фрейм. Поле управления определяет функцию (назначение) фрейма (например, указывает на то, что фрейм содержит данные или же код ошибки). Это поле может иметь длину 8 или 16 бит.

Кроме этого, стандарт IEEE 802.3 описывает для LLC реализацию протокола SubNetwork Access Protocol, SNAP (Стандартный протокол доступа к сети), также называемого Ethernet SNAP. SNAP используется в качестве способа быстрой адаптации протоколов, которые не полностью соответствуют стандартам 802.3 (например, протокола AppleTalk или протокола LAT компании DEC). Когда для подобных протоколов отсутствуют установленные точки SAP, поля DSAP и SSAP содержат шестнадцатеричное значение AA, которое представляет точку SAP для SNAP-фрейма. Кроме этого, поле управления в SNAP-фрейме содержит шестнадцатеричное значение 03. При создании SNAP-фрейма, поле разделителя протоколов помещается сразу же за полем управления и перед полем данных. Поставщик типа фрейма (например, Apple) идентифицируется первыми тремя байтами поля разделителя протоколов, а тип фрейма Ethernet идентифицируется двумя последними байтами.

Для сетей Ethernet выпускается большое количество оборудования, которое широко поддерживается производителями компьютеров. Одной из причин популярности Ethernet является то, что этот стандарт имеет много решений для реализации высокоскоростных сетей. Например, сети Ethernet с часто той 10 Мбит/с легко модернизировать в сеть Fast Ethernet с частоте 100 Мбит/с, зачастую используя для этого уже установленные сетевые адаптеры и кабельную систему. Кроме того, для сетей Ethernet выпускаете множество средств тестирования и управления. В табл. 2.3 кратко перечне лены многие из существующих или перспективных стандартов Ethernet имеющихся на момент написания книги.

Таблица 2.3. *Стандарты IEEE 802.3 для сетей Ethem*

Стандарт	Описание
802.3	Стандарты для коммуникаций 10 Мбит/с
802.3u	Стандарты для коммуникаций 100 Мбит/с
802.3x	Стандарты для управления информационным потоком
802.3z	Стандарты для коммуникаций 1 Гбит/с (по оптоволоконному кабелю)
802.3ab	Стандарты для коммуникаций 1 Гбит/с (по медному проводу)
802.3ac	Стандарты для реализации виртуальных локальных сетей (VLAN)
802. 3ad	Стандарты для группировки (объединения) каналов (использование нескольких каналов для увеличения скорости, например, удвоение или утроение скорости за счет использования двух или трех сгруппированных каналов)
802.3ae	Стандарты для коммуникаций 1 0 Гбит/с
802. 3af	Стандарты на источники питания оконечного оборудования передачи данных с использованием Media Dependent Interface (MDI)

Token Ring

Метод доступа *маркерное кольцо* (token ring) был разработан компанией IBM в 1970-х годах и остается одной из основных технологий локальных сетей, хотя уже и не столь популярной, как Ethernet. Скорость передачи данных старых версиях маркерных сетей равна 4 Мбит/с или 16 Мбит/с, а в новых скоростных сетях – 100 Мбит/с. Метод передачи данных в маркерном кольце использует топологию физической звезды в сочетании с логикой кольцевой топологии. Несмотря

на то, что каждый узел подключается к центральному концентратору, пакет перемещается от узла к узлу так, будто начальная и конечная точки отсутствуют. Каждый узел соединяется с другими при помощи *модуля множественного доступа* (Multistation Access Unit, MAU). MAU – это специализированный концентратор, обеспечивающий передачу пакета по замкнутой цепочке компьютеров. Поскольку пакеты движутся по кольцу, на рабочих станциях или в модуле MAU отсутствуют терминаторы.

Совет

При организации скоростного маркерного кольца (fast token ring) нужно быть, внимательным. Некоторые производители, первоначально предлагающие сетевые устройства для этой технологии, ушли с рынка подобного оборудования.

Специальный фрейм, называемый маркером (token), непрерывно передается по кольцу для определения момента, когда некоторый узел может отправить пакет. Этот фрейм имеет длину 24 бита и состоит из трех 8-битных полей признака начала (starting delimiter, SD), поля управления доступом (access control, AC) и признака конца (ending delimiter, ED). Признак начала – эта комбинация сигналов, отличных от любых других сигналов сети, что предотвращает ошибочную интерпретацию поля. Он выглядит как сигнал отсутствия данных. Эта уникальная комбинация восьми разрядов может распознаваться только как признак начала фрейма (SOF).

Поле управления доступом (8-битное) указывает на то, прикреплен ли к маркеру фрейм, содержащий данные. То есть это поле определяет, несет ли фрейм данные или он свободен для использования некоторым узлом. Признак конца также представляет собой уникальным образом закодированный сигнал отсутствия данных. Его восемь разрядов представляют сигнал, который невозможно спутать с признаком начала или интерпретировать как данные. Эта часть маркера определяет, должен ли узел еще передавать последующие фреймы (идентификатор последнего фрейма). Также она содержит информацию об ошибках, обнаруженных другими станциями.

В большинстве реализаций в кольце может быть только один маркер, хотя спецификации IEEE разрешают применение двух маркеров в сетях, работающих с частотой 16 Мбит/с и выше. Прежде чем некоторый узел начнет передачу, он должен перехватить маркер. Пока активный узел не закончит работу, ни один другой узел не может захватить маркер и передавать данные. Станция, захватившая маркер, создает фрейм, имеющий признак начала и поле управления доступом в начале этого фрейма. Признак конца помещается в конце данного фрейма. Полученный фрейм посылается по кольцу и передается до тех пор, пока не достигнет целевого узла. Целевой узел изменяет значения двух разрядов, указывая на то, что фрейм достиг пункта назначения, и что данные были прочитаны. Затем целевой узел помещает фрейм обратно в сеть, где тот передается по кольцу до тех пор, пока передающая станция не получит этот фрейм и не проверит факт его получения. После этого передающая станция формирует следующий фрейм с маркером и инкапсулированными данными или же создает маркер без данных, возвращая маркер в кольцо для того, чтобы другая станция могла его использовать.

На рис. 2.13 показан фрейм маркерного кольца с полями маркера, добавленными к полям данных. Первые 16 разрядов занимают поля признака начала и управления доступом. Затем следует поле управления фреймом. Эти поле идентифицирует фрейм как фрейм данных или как фрейм, предназначенный для управления сетью (например, как фрейм, содержащий коды сетевых ошибок). Следующие два поля имеют длину 16 или 48 бит и используются для адресации. Первое поле содержит адрес узла назначения, I второе – адрес исходного узла. Далее идет поле данных маршрутизации (routing information field, RIF), имеющее длину 144 бита или меньшую. Это поле содержит исходные данные маршрутизации, которые могут использоваться на Сетевом уровне модели OSI.

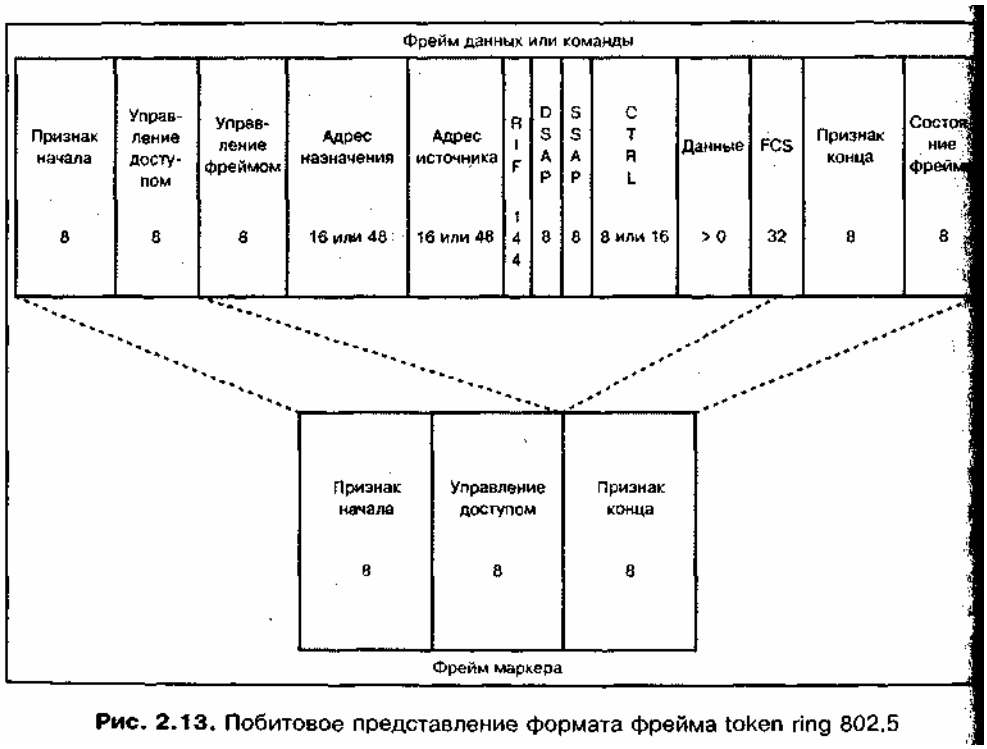


Рис. 2.13. Побитовое представление формата фрейма token ring 802.5

Следующие три поля – поле целевой точки доступа к службе (DSAP), по исходной точки доступа к службе (SSAP) и поле управления (CTRL) имеют такие же функции и размер, как и во фреймах 802.3 и Ethernet II. Поле DSAP определяет точку SAP узла назначения, а поле SSAP указывает, от какой точки доступа данный фрейм был послан, например, Novell или TCP IP. 8- или 16-битное поле управления определяет, содержит фрейм данные или информацию для управления ошибками. Поле данных следует за полем управления. Оно содержит данные или коды ошибок, используемые для управления сетью. Поле данных не имеет предопределенного размера. 32-битное поле контрольной суммы (FCS) применяется для проверки целостности всего фрейма. Как и во фрейме Ethernet, в нем используется алгоритм контроля с избыточным кодированием (CRC), позволяющий гарантировать правильность передачи и получения сигнала. Контрольная сумма в полученном фрейме должна совпадать с посланным значением.

Последняя часть маркера – признак конца – следует за полем контрольной суммы фрейма. Это поле содержит информацию, сообщающую принимающему узлу о достижении конца фрейма. Также поле указывает на то, будет ли послан следующий фрейм из исходного узла или же данный фрейм последний. Кроме того, данное поле может содержать информацию о том, что другие станции обнаружили ошибки во фрейме. Если фрейм содержит ошибку, он удаляется из сети и затем посылается заново передающим узлом.

Последнее поле во фрейме маркерного кольца представляет собой 8-битное поле состояния фрейма. Два разряда этого поля особенно важны для передающего узла: разряд распознавания адреса указывает на то, что целевой узел "увидел" свой адрес, содержащийся во фрейме; разряд копирования фрейма определяет, скопировал ли целевой узел посланный фрейм или же при этом были ошибки.

В каждом маркерном кольце один узел выполняет функции монитора активности (active monitor) или диспетчера. Обычно эти задачи выполняет первая станция, обнаруженная после запуска сети. Диспетчер отвечает за синхронизацию пакетов в сети и за генерацию нового фрейма маркера в случае возникновения проблем. Через интервалы в несколько секунд диспетчер рассылает широковещательный фрейм подуровня MAC, свидетельствующий о работоспособности диспетчера. *Широковещательный* (broadcast) *фрейм* или *пакет* адресуется всем узлам сети. Другие узлы рабочих станций являются резервными диспетчерами. Периодически они генерируют широковещательные фреймы, называемые фреймами наличия резервных диспетчеров, подтверждающие работоспособность узлов и их способность заменить активный диспетчер в случае его отказа.

Примечание

Широковещательный фрейм формируется на Канальном уровне модели OSI, и его поле

назначения заполняется двоичными единицами. Широковещательный пакет формируется на Сетевом уровне модели OSI в сетях, использующих протокол IP. Его адрес назначения равен 255.255.255.255. Помимо широковещательных, существуют однонаправленные (unicast) пакеты, которые передаются только целевому узлу, для которого предназначен конкретный пакет. Кроме того, бывают многоабонентские (multicast) пакеты, которые отправитель рассылает нескольким целевым узлам, при этом каждый из этих узлов получает копию пакета. Эти типы пакетов будут описаны в последующих главах.

Если широковещательные посылки от активного или резервных диспетчеров отсутствуют, кольцо переходит в состояние *"испускания маяка"*(beaconing). Это состояние начинается с того момента, когда некоторый узел генерирует так называемый фрейм маяка (beacon), указывающий на обнаружение некоторой ошибки. Кольцо пытается автоматически устранить ошибку (например, назначая новый активный диспетчер в том случае, если исходный диспетчер вышел из строя). После перехода в состояние испускания маяка передача маркеров с данными прекращается до момента ликвидации проблемы.

Маркерные кольца являются весьма надежной топологией и поэтому они иногда используются в особо важных конфигурациях. Одним из преимуществ маркерного кольца по сравнению с сетями Ethernet является то, что по них редко, возникают *"широковещательный шторм"* (broadcast storm) или конфликты между рабочими станциями. Широковещательный шторм иногда случается в сетях Ethernet, когда большое количество компьютеров или устройств одновременно пытаются передавать данные или же когда компьютеры или устройства "зацикливаются" на передаче. Также в сетях Ethernet возникают сетевые конфликты, когда неисправный сетевой адаптер продолжает передачу широковещательных пакетов, несмотря на занятость сети. Такие проблемы редко встречаются в маркерных сетях, поскольку в каждый момент времени только один узел может передавать данные. Более подробно о сетях Ethernet и маркерных кольцах рассказывается в практическом задании 2-7.

FDDI

Стандарт *Fiber Distributed Data Interface, FDDI* (Распределенный интерфейс передачи данных по оптоволоконным каналам) был разработан в середине 1980-х годов для обеспечения высокоскоростной передачи данных по сетям Ethernet (в то время на частоте 10 Мбит/с) или по маркерным кольцам (с частотой 4 или 16 Мбит/с). Стандарт установлен комитетом ANSI X3T9.5 и обеспечивает метод доступа, позволяющий с большой скоростью передавать информацию по загруженным сетям.

При частоте передачи, равной 100 Мбит/с, стандарт FDDI обеспечивая большую производительность, чем сети Ethernet с частотой 10 Мбит/с и маркерные кольца с частотой 16 Мбит/с. Однако по мере развития скоростных технологий Fast Ethernet и Fast Token Ring этот стандарт применяется все реже и реже. В качестве передающей среды стандарт FDDI использует оптоволоконный кабель. Обычно FDDI применялся для обеспечения быстрого доступа к сетевым серверам (но, опять-таки, теперь для этих целей почти везде используют технологии Fast Ethernet).

Методы доступа FDDI и маркерного кольца похожи, поскольку в них для пересылки данных по сети используется передача маркера. Отличие FDDI от стандартного маркерного кольца заключается в применении синхронного метода доступа с передачей маркера. Маркер FDDI перемещается по сетевому кольцу от узла к узлу. Если некоторый узел не имеет данных для передачи, он принимает маркер и пересылает его следующему узлу. Если узел, владеющий маркером, должен передать данные, он может отослать любое нужное количество фреймов в течение фиксированного промежутка времени, называемого временем обращения целевого маркера (target token rotation time, TTRT). Поскольку стандарт FDDI использует синхронный метод передачи маркера, в сети в каждый момент времени могут находиться несколько фреймов от нескольких узлов, что обеспечивает высокую скорость передачи данных.

После того как узел передал фрейм, последний перемещается к следующему узлу сетевого кольца. Каждый из узлов определяет, предназначен ли фрейм текущему узлу и имеются ли в этом фрейме ошибки. Если узел является приемником данных, он помечает фрейм как прочитанный. Если какой-нибудь узел обнаруживает ошибку, он устанавливает разряд состояния фрейма, указывая на наличие ошибки. Когда фрейм возвращается к передающему узлу, тот определяет, получил ли целевой узел данный фрейм, а также имелись ли ошибки. В случае наличия ошибок фрейм

передается заново. При отсутствии ошибок передающий узел удаляет фрейм из кольца.

Стандарт FDDI допускает два способа передачи пакетов: синхронный и асинхронный. *Синхронная передача* данных используется для пересылки непрерывной по времени информации: голоса, видео или мультимедиа. *Асинхронная передача* применяется для обычного сетевого трафика, который не нужно пересылать непрерывными порциями. Для конкретной сети время TTRT равно полному времени, необходимому для синхронной передачи данных от некоторого узла плюс время прохождения фрейма максимальной длины по всему кольцу.

В сети FDDI отслеживаются два типа ошибок: длительные периоды простоя и длительные периоды отсутствия маркера. В первом случае предполагается, что маркер был потерян; во втором случае допускается, что некоторый узел непрерывно работает на передачу. При любом типе ошибки узел, обнаруживший ее, генерирует последовательность специальных фреймов, называемых исковыми фреймами (claim frame), или фреймами претензий. Исковой фрейм содержит предлагаемое время TTRT. Первый узел прекращает передачу, а следующий узел в кольце сравнивает свое время TTRT со значением, посланным предыдущим узлом. После сравнения он передает меньшее из значений TTRT следующему узлу, записывая это значение в свои исковые фреймы. К тому времени, как информация дойдет до последнего узла, будет выбрано самое маленькое значение TTRT. В этот момент кольцо инициализируется, для чего в него передается маркер и устанавливается новое время TTRT для каждого узла; такое состояние длится до тех пор. пока последний узел не получит новую информацию.I

В сети FDDI используются два кольца, так что в случае выхода одного кольца из строя данные могут дойти до целевого узла по другому кольцу К сети FDDI подключаются узлы двух классов. Узлы Класса А соединены с обоими сетевыми кольцами. Этот класс образует сетевое оборудование, например, концентраторы. Узлы Класса А могут переконфигурировать кольцо так, чтобы в случае отказа сети можно было использовать одно кольцо. Узла Класса В подключаются к сети FDDI через устройства Класса А. К этом) классу относятся серверы и рабочие станции.

Глобальные сетевые коммуникации

Глобальные сети, как и локальные, строятся с использованием определенных топологий и методов передачи данных. Во многих глобальных сетях используются модифицированные кольцевые или звездообразные топологии, однако их трудно описать подробно, поскольку из соображений конкурентоспособности основные поставщики глобальных сетей держат в секрет особенности конкретных топологий. Методы передачи данных в глобальных сетях весьма сложны, поскольку постоянно появляются все новые и новые технологии. В последующих разделах описываются основные методы глобальных коммуникаций, например, различные методы коммутации пакетов. В *главе* имеется подробное описание методов коммутации, реализованным в самых разнообразных коммуникационных технологиях глобальных сетей начиная от базовых сетей X.25 и заканчивая сложными сетями SONET.

Сетевые службы глобальных сетей обычно предоставляются телекоммуникационными компаниями, компаниями кабельного телевидения и провайдерами спутниковых каналов. В настоящее время самыми крупными провайдерами с наибольшим выбором услуг являются региональные телефонные компании, такие как Verizon (бывшие Bell Atlantic и GTE), Qwest (бывшая U S West and Quest), BellSouth, SBC Ameritech, SBC Southwestern Bell, SBC Pacific Bell, SBC Nevada Bell, а также телекоммуникационные компании дальней связи – AT&T, MCI и Sprint. Региональные телефонные компании в США называют *telco,* или *regional bell operating company* (RBOC). Компания сетей кабельного телевидения, также называемые *cab eco, или multiple systems operator* (MSO), являются новыми поставщиками канатов глобальных сетей, примером такой компании служит AT&T Broadband (см. практическое задание 2-8).

С компаниями сетей кабельного телевидения конкурируют компании спутникового телевидения, такие как DirecTV, предлагающие возможности глобальных коммуникаций с использованием сетей DirectPC и DirectWAY. Сеть DirectPC также сотрудничает с некоторыми энергетическими компаниями, например, KN Energy, которые предлагают комплексный сервис для многих традиционных бытовых служб, включая поставки газа, электричества, электрооборудования, а также услуги телевидения и Интернета. Помимо DirectPC и DirectWAY, существует множество беспроводных глобальных сетей, в которых радио- и ультракороткие волны используются для подключения

отдельных пользователей к глобальным сетям и для соединения локальных сетей в тех случаях, когда кабельные соединения невозможны.

Сети на основе телекоммуникационных каналов

Проще всего для реализации глобальных коммуникаций привлекать телефонные компании. Самые простые глобальные сети реализуются на базе обычных голосовых аналоговых линий, образующих *обычную телефонную сеть* (plain old telephone service, POTS), также называемую *коммутируемой телефонной сетью общего пользования* (public switched telephone network, PSTN). Существует свыше 600 миллионов телефонных линий, подключенных к частным домам, офисам, учебным и правительственным организациям. Для реализации коммуникаций по обычным телефонным сетям используются стандартные аналоговые модемы со скоростью передачи 56 Кбит/с и цифровые методы скоростного доступа, такие как ISDN (Integrated Services Digital Network – цифровая сеть связи с комплексными услугами) и DSL (Digital Subscriber Line – цифровая абонентская линия), обе эти технологии описываются в следующих главах книги.

Топологию, используемую региональными телефонными станциями (RBOC), нередко называют облаком, поскольку точный маршрут от точки к точке трудно проследить, и отдельные компании не распространяют эту информацию. Однако известна базовая топология между региональными телефонными станциями и поставщиками услуг дальней связи. Коммуникационные линии, предоставляемые региональной телефонной станцией, образуют каналы локальной области доступа и связи (local access and transport area, LATA). Линии, связывающие региональные телефонные станции и компании дальней связи, такие как AT&T, являются каналами владельца линий информационного обмена (interexchange carrier, IXC). С точки зрения топологии существует точка, в которой каналы LATA подключаются к каналам IXC, и эта точка называется точкой присутствия (point of presence, f OP). Точка присутствия хорошо защищена и может даже размещаться под землей для защиты от постороннего вмешательства, неблагоприятных погодных воздействий и природных катаклизмов. На рис. 2.14 показана общая топология, связывающая каналы LATA и IXC.

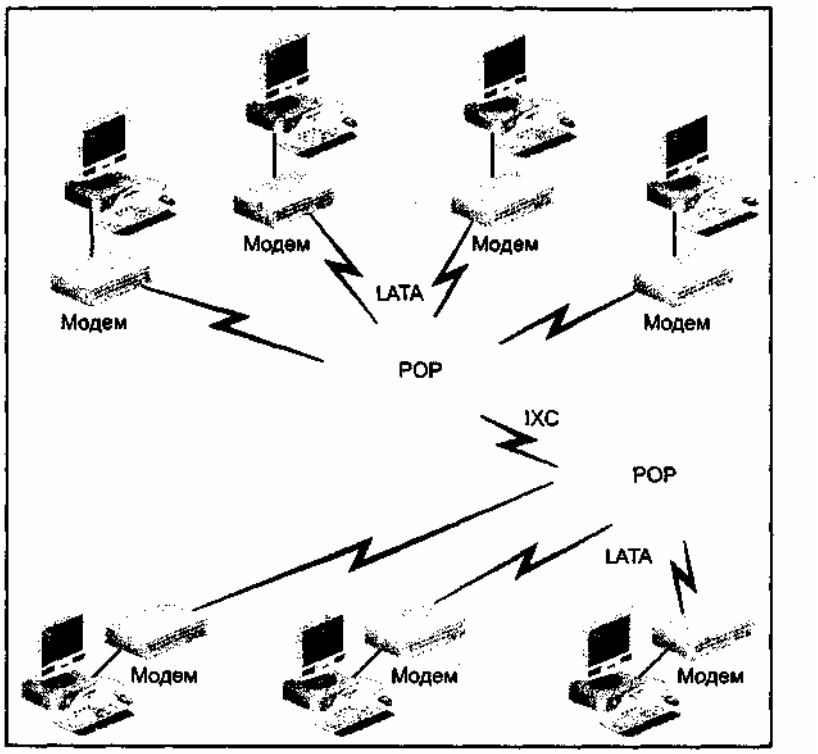


Рис. 2.14. Топология обычной телефонной сети (POTS)

Для промышленных высокоскоростных цифровых коммуникаций по обычным телефонным сетям используются выделенные телефонные подключения, такие как каналы типа T (T-carrier). *Канал типа T* (T-линия) – это выделенная телефонная линия, которая может использоваться для непрерывной передачи данных между двумя различными точками. Например, в некоторых университетах T-линии применяются для подключения к Интернету. В некоторых штатах T-линии связывают подразделения и колледжи правительственными офисами, расположенными в столице

штата. Эти линии обеспечивают надежную связь на очень больших расстояниях. Логически Т-линии образуют такую топологию, в которой виртуально отсутствуют устройства между двумя локальными сетями, как показано на рис. 2.15.

Простейшая Т-линия, называемая Т-1, обеспечивает передачу данных со скоростью 1,544 Мбит/с, и несколько линий могут группироваться для создания составных каналов высокоскоростной связи (как показано в табл. 2.4). Например, для создания службы следующего уровня (Т-2), группируются 4 линии типа Т-1. Линия Т-3 содержит 28 каналов, а линия Т-4 - 168 каналов. Поскольку Т-линии достаточно дороги, телефонные компании предлагают частные службы, для которых используется часть линии Т-1 и задействуются подканалы, имеющие скорость передачи 64 Кбит/с. Это возможно, т. к. каждая линия Т-1 состоит из 24-х подканалов с частотой 64 Кбит/с, называемых каналами цифрового сигнала (digital signal) уровня О (DS-0).

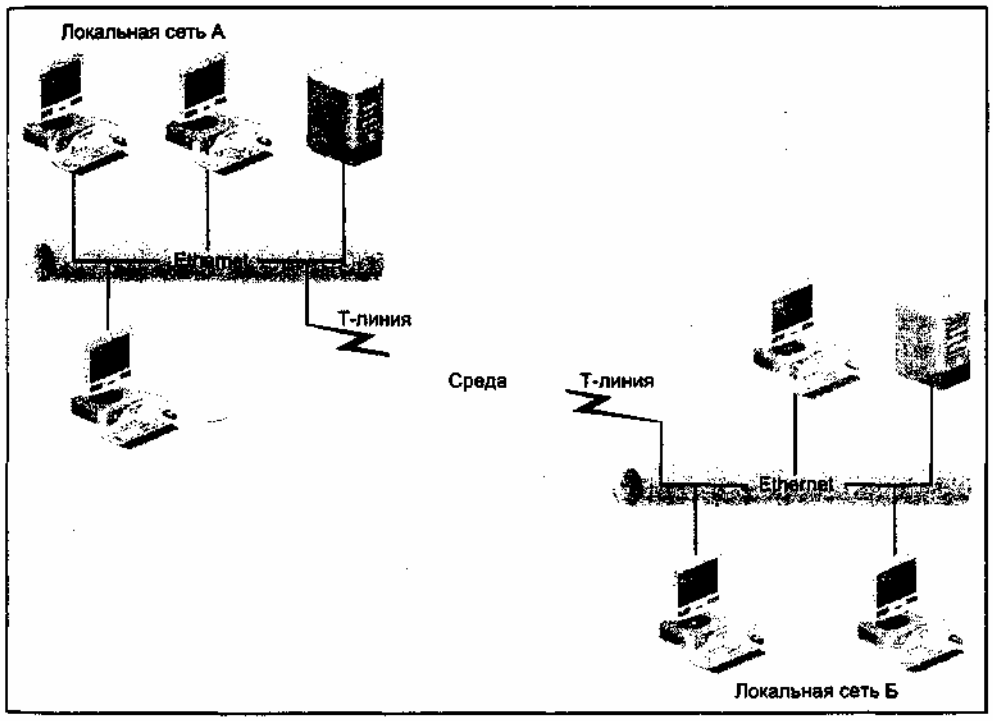


Рис. 2.15. Соединение локальных сетей по Т-линии

Таблица 2.4. *Службы каналов типа Т (Т-линий) и скорости передачи данных*

Т-линия	**Скорость передачи данных**	**Коммутируемые каналы Т-**	**Уровень сигнала**
Частная линия Т-	**64 Кбит/с**	**1 из 24-х подканалов линии**	**DS-0**
Т-1	**1,544 Мбит/с**	**1**	**DS-1**
Т-1 С	**3,1 52 Мбит/с**	**2**	**DS-1C**

Таблица 2.4 *(окончание*

Т-линия	Скорость передачи данных	Коммутируемые каналы Т-	Уровень сигнала
Т-2	6,31 2 Мбит/с	4	DS-2
Т-3	44,736 Мбит/с	28	DS-3
Т-3С	89,472 Мбит/с	56	DS-3C
Т-4	274, 176 Мбит/с	168	DS-4
Т-5	400,352 Мбит/с	336	DS-5

Примечание

Формально Т-линии называют службами TX/DSx; они соответствуют Физическому и Канальному уровням модели OSI. Термин "DS" (digital signal) описывает электрические характеристики сигнала передачи данных на Физическом уровне, а TX относится к типу передающей среды, относящейся к Канальному уровню.

Альтернативой Т-линиям являются синхронные коммуникационные каналы с частотой 56 Кбит/с, и коммутируемые асинхронные каналы со скоростью передачи 57,6 Кбит/с. Обе технологии обеспечивают передачу цифровых данных с использованием методов сжатия информации и методов коммутации каналов (описываемых в следующих главах), что в совокупности позволяет почти в четыре раза увеличить реальную пропускную способностей линий. Использование коммутируемых каналов с частотой 56 Кбит/с объясняется их меньшей стоимостью по сравнению с Т-линиями, и компании применяют эти каналы в качестве резервных при выходе из строя основном Т-линии.

Сети на основе каналов кабельного телевидения

В глобальных сетях на основе линий кабельного телевидения применяется распределенная архитектура, в состав которой входит несколько звездообразных центральных узлов. Главной точкой звезды является *головной узел* (headend), представляющий собой принимающий центр для сигналов различных источников, включая спутники, магистральные кабели и локальные телестанции. Головной узел – это совокупность антенн, кабельных разъемов, радиорелейных вышек и спутниковых тарелок (параболических антенн); он фильтрует все входящие сигналы и передает их на удаленные распределительные (коммутационные) центры по транковым каналам.1

Распределительные центры содержат передающее оборудование, которое усиливает и передает кабельные сигналы специальным смежным точкам коммутации, называемым магистральными кабелями или фидерами (feeder cable). Отдельные здания и офисы подключаются к фидерам с помощью ответвительных кабелей или отводов, подобно тому, как тонкие электрические провода подходят к домам от основных линий, расположенных на телеграфных столбах. Главная задача при построении кабельной службы – обеспечить правильное сочетание величины усиления сигнала и длины кабелей, чтобы уменьшить потери и искажения сигнала на принимающем конце. На рис. 2.16 изображена топология глобальной сети на основе каналов кабельного телевидения.

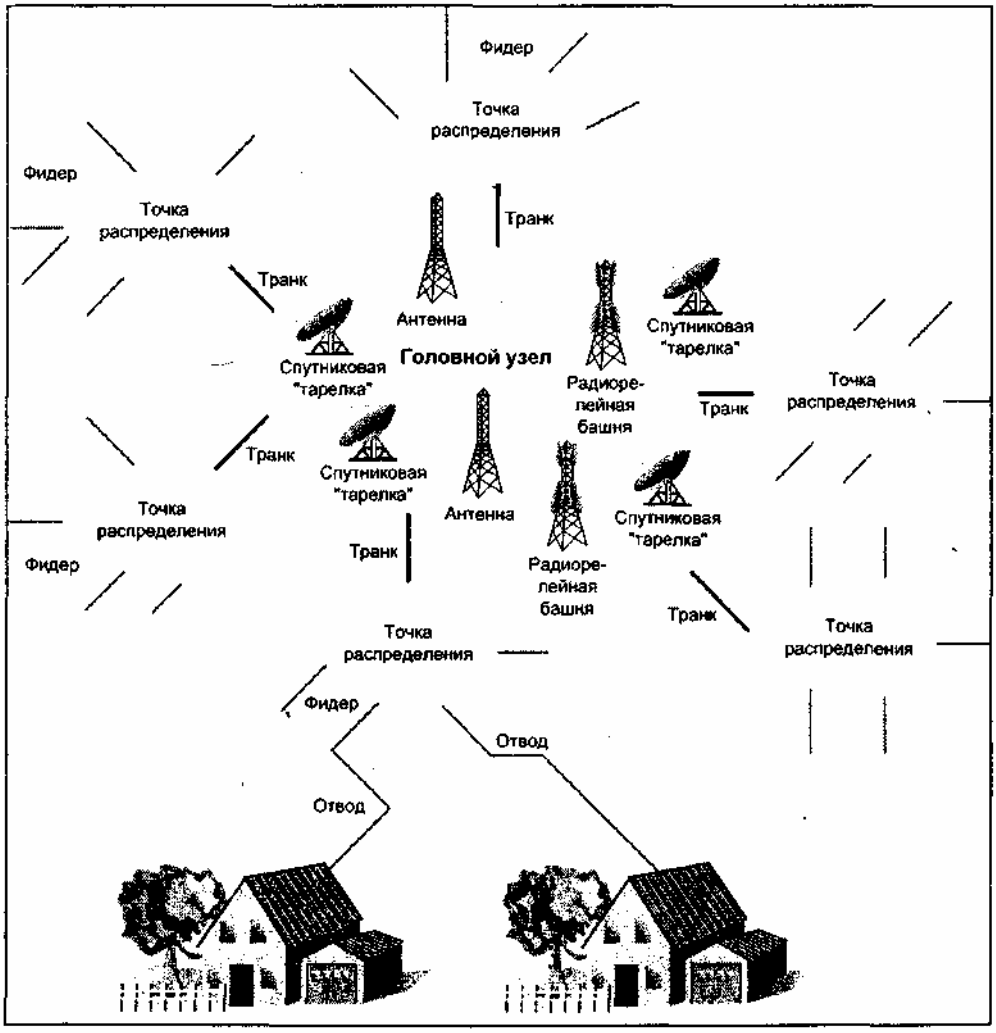


Рис. 2.16. Глобальная сеть, использующая каналы кабельного телевидения

Для преобразования кабельного сигнала в сигнал, используемый компьютером, применяются специально разработанные кабельные модемы. Для передачи данных кабельный модем использует восходящие и нисходящие частоты (каналы), которые уже реализованы кабельной службой. Восходящий канал применяется для передачи исходящего сигнала, при этом спектр (непрерывный диапазон частот) содержит данные, звук или телевизионный сигнал. Нисходящий канал используется для приема сигналов, он также смешивается с другими входящими сигналами данных, аудио- или телесигналами.

В зависимости от типа модема, скорости передачи восходящего и нисходящего сигнала могут совпадать или различаться. Например, модем может обеспечивать максимальную скорость восходящего сигнала, равную 30 Мбит/с, и максимальную скорость для нисходящего сигнала - 15 Мбит/с. Другой же модем может работать на скорости 10 Мбит/с как для восходящего, так и для нисходящего потоков данных. Однако, несмотря на то, что кабельные модемы рассчитаны на большие скорости сигналов, пользователь такого модема будет, скорее всего, иметь скорость доступа *(полосу пропускания,* bandwidth) в диапазоне от 256 Кбит/с до 3 Мбит/с (эти цифры относятся ко времени написания книги). Реальная скорость в особенности зависит от того, сколько соседей в данный момент используют свои кабельные модемы; это объясняется тем, что один кабель, подключающий группу абонентов к кабельному концентратору, может иметь максимальную полосу пропускания до 27 Мбит/с. Кроме того, провайдер кабельной службы может ограничить полосу пропускания (для приема и передачи данных) для того, чтобы кабельной сетью могло пользоваться большее количество людей.

Беспроводные сети

В беспроводных сетях для передачи сигналов используются радио-, СВЧ- спутниковые каналы.

Топология радиоканалов связи предусматривает подключение локальной сети к мосту или коммутатору беспроводной связи который в свою очередь может быть соединен с антенной. Антенна передав радиоволны на уделенную антенну, также подключенную в мосту или коммутатору, который принимает пакеты и передает их в другую локальную) сеть. Такой тип коммуникаций называется *пакетной радиосвязью* (packet radio) и реализуется на очень высоких радиочастотах. На рис. 2.17 показан топология глобальной сети на основе радиоволн, соединяющей две локальных сети.

СВЧ-каналы работают на еще больших частотах, чем радиоканалы. В этом случае в состав сети входит параболическая антенна (тарелка), подключенная к локальной сети и передающая сигнал на удаленную тарелку, которая преобразует сигнал в тот вид, который используется в сети. В случае применения спутниковых каналов связи одна площадка с помощью спутниковой антенны передает сигнал на спутник, находящийся в космосе. Затем сигнал ретранслируется со спутника на другую антенну, которая может находиться на другом континенте. Спутниковые каналы – это наиболее дорогой вид связи, используемый для построения беспроводных глобальных сетей, соединяющих локальные сети. Самый дешевый тип связи – обычные радиоволны.

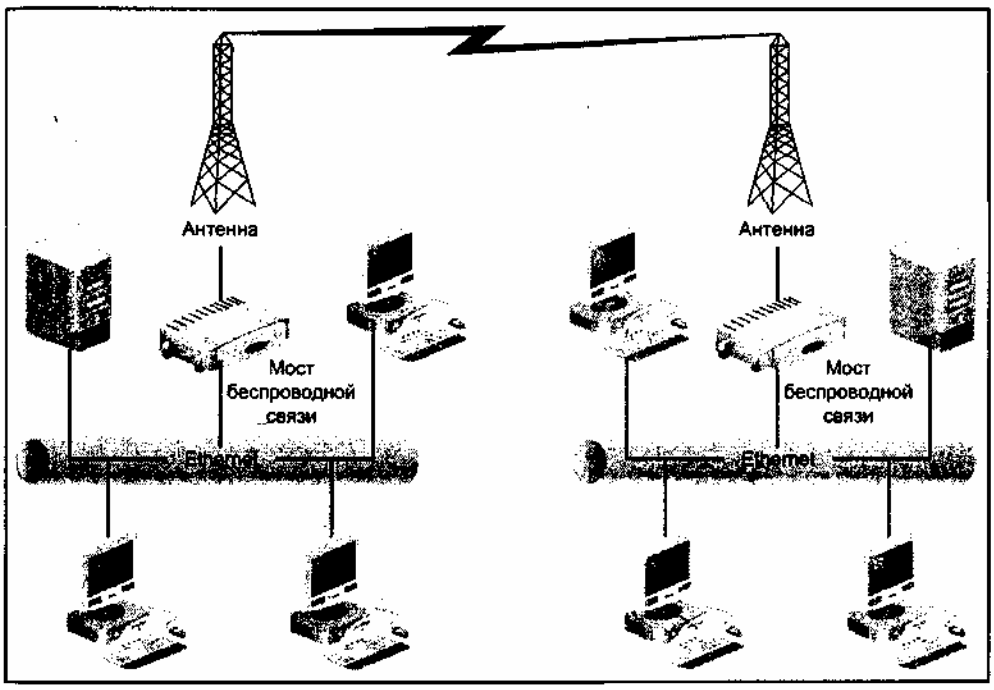


Рис. 2.17. Глобальная сеть, реализованная на основе радиоволн

Методы передачи данных в глобальных сетях

При передаче данных по глобальным сетям используются различные методы коммутации каналов, когда для осуществления коммуникаций создается один или несколько информационных маршрутов, называемых каналами. Каналы могут быть образованы как с помощью одного коммуникационного кабеля, так и с помощью нескольких кабелей, образующих маршруты передачи данных. Коммутация позволяет множеству узлов передавать и принимать данные одновременно, а также обеспечивает передачу информации по разным маршрутам для достижения максимальной эффективности в плане скорости и стоимости передачи. Ниже перечислены основные методы коммутации, используемые в глобальных сетях:

- множественный доступ с временным разделением (уплотнением) каналов;
- множественный доступ с частотным разделением каналов;
- статистический множественный доступ;
- коммутация каналов;
- коммутация сообщений;
- коммутация пакетов (или пакетная коммутация).

При *множественном доступе с уплотнением каналов* (time division multiple access, TDMA) время

доступа к каналам делится на отдельные интервалы. Каждый временной интервал предназначается для конкретного узла сети, как будто тот подключен к выделенной линии. Устройство коммутации в глобальной сети переключает эти временные интервалы для отдельных каналов. Это напоминает сетку круглосуточного телевизионного вещания, при котором интервал, начинающийся с 18:00, отводится для новостей, в 18:30 начинаются развлекательные новости, а в 19:00 – семейная комедия. Множественный доступ с уплотнением каналов не гарантирует наиболее эффективное использование сетевой среды, поскольку в каждый момент времени передача данных выполняется только по одному каналу. Также важна синхронизация времени работы узла, т. к. узел может начать передавать данные в момент, не совпадающий с выделенным ему временным интервалом. Кроме того, согласно спецификациям IEEE, каждому пакету выделено время, в течение которого он должен быть передан по всей сети для того, чтобы избежать конфликтов со следующим посланным пакетом.

При *множественном доступе с частотным разделением каналов* (frequency division multiple access, FDMA) каналы делятся не по времени использования, а по частоте. Каждый канал имеет собственную несущую частоту и полосу пропускания. По мере передачи данных коммутатор переключает эти частоты. Это похоже на то, как четыре слушателя в наушниках вместе слушают радио, настроенное на прием четырех каналов. Первый человек может слушать станцию классической музыки, второй - ток-шоу, третий - бейсбольный матч, а четвертый - новости. Каждый слушатель использует независимую частоту. Радиоприемник передает сигнал по каждому каналу так быстро, что никто не может сказать, что каналы быстро переключаются по мере приема сигнала каждой частоты.

Статистический множественный доступ (statistical multiple access) (или статистическое уплотнение) используется во многих технологиях глобальных, сетей. Этот метод более эффективен по сравнению с описанными выше методами TDMA и FDMA, поскольку полоса пропускания передающей среды (кабеля) распределяется динамически по требованию приложений. Коммутатор непрерывно анализирует каждый канал и определяет наличие запросов на передачу данных. Например, в некоторый момент канал должен передать большой графический файл, а затем он может быть свободным. Алгоритмы коммутации определяют полосу пропускания, необходимую для передачи файла. После того как он передан, коммутатор выделяет полосу другому каналу. Это можно сравнить с тем, как операционная система рабочей станции автоматически определяет объем памяти, выделяемой трем одновременно выполняющимся приложениям. Она может выделить 15 Кбайт/с для обработки текстового файла, 7 Мбайт/с - для сканирования изображения, и 1,2 Мбайт/с - для печати графического изображения.

Процесс *коммутации каналов* (circuit switching) предполагает создание выделенного физического канала между передающим и приемным узлами. Этот канал функционирует как прямая линия, по которой данные без помех можно передавать в одну и другую стороны, подобно тому, как осуществляется телефонный разговор между двумя абонентами. Канал передачи данных остается активным до тех пор, пока два узла не будут разъединены.

При *коммутации сообщений* (message switching) для передачи данных от передающего узла к принимающему используется метод промежуточного хранения. Данные передаются от одного узла к другому, где они временно запоминаются до тех пор, пока не будет доступным канал к точке назначения этих данных. Несколько узлов на протяжении маршрута могут сохранять и передавать данные дальше - пока те не дойдут до конечного пункта. Коммутация сообщений применяется, например, при отправке электронной почты по корпоративной сети, где несколько серверов выполняют функции почтовых отделений. Сообщение переходит от одного отделения к другому до тех пор, пока не достигнет адресата.

Коммутация пакетов (packet switching) представляет собой комбинацию методов коммутации каналов и сообщений. При ее использовании устанавливается выделенный канал между двумя взаимодействующими узлами, однако этот канал является логическим, а не физическим. Хотя для осуществления сеанса передачи данных могут использоваться несколько различных физических маршрутов, каждый узел знает только об одном выделенном канале. Преимуществом данной технологии является то, что в зависимости от типа и объема посылаемых данных может быть выбран наилучший маршрут, что предоставляет возможность для реализации скоростных коммуникаций. Коммутация пакетов осуществляется подобно тому, как оптический перископ обеспечивает передачу изображения от точки к точке по нелинейному пути. В последующих главах использование

перечисленных методов коммутации в глобальных сетях будет описано подробнее

Резюме

- Семиуровневая модель OSI является основой для передачи информации между локальными и глобальными сетями. При отсутствии модели OSI взаимодействие между этими сетями в настоящее время было бы недостижимо, а Интернет оставался бы теоретической моделью, но не фактом реальности.
- Каждый уровень модели OSI играет важную роль в сетевых коммуникациях. Нижние уровни обеспечивают физические соединения, формирование фреймов, кодирование и передачу сигналов. Средние уровни позволяют устанавливать и поддерживать сеансы передачи данных между двумя сетевыми узлами, а также обнаруживать ошибки. Верхние уровни обеспечивают поддержку приложений, шифруя и интерпретируя данные.
- Локальные сети, построенные на базе модели OSI, используют одну из трех основных топологий: шину, кольцо или звезду. Звездообразная топологая является самой старой и наиболее распространенной в современных сетях. Популярность этой топологии объясняется несколькими факторами, среди которых - стоимость, простота обслуживания и возможность расширения. Для осуществления коммуникаций в локальных сетях используются установленные методы передачи данных – Ethernet, или маркерное кольцо. Сети Ethernet в настоящее время наиболее распространены, поскольку для них выпускается достаточное количество сетевого оборудования, и этот метод доступа хорошо подходит для реализации высокоскоростных глобальных сетей.
- Топологии глобальных сетей трудно классифицировать из-за того, что многие провайдеры держат в секрете детали конкретных технологий. Однако, как и в локальных сетях, в глобальных широко используется звездообразная топология. Эта топология применялась в телекоммуникационных сетях еще задолго до появления локальных сетей и продолжают использоваться и поныне. Все чаще появляются глобальные сети на основе каналов кабельного телевидения и спутниковых каналов, и в таких сетях также применяются звездообразные топологии.
- Методы передачи данных в глобальных сетях весьма разнообразны и зависят от конкретных технологий, однако очень часто используются те или иные способы коммутации. Методы коммутации позволяют создавать множество коммуникационных маршрутов, обеспечивающих максимально быструю передачу наибольших объемов информации всем адресатам.

Глава 3

Методы передачи физического сигнала

По прочтении этой главы и после выполнения практических заданий вы сможете:

- описать функции основных организаций, разрабатывающих сетевые стандарты;
- описать различные типы сетевой передающей среды, включая коаксиальный кабель, витую пару и оптоволокно, а также определить, какой тип среды следует использовать в конкретной сетевой конфигурации;
- рассказать об основах беспроводных коммуникаций;
- обсудить высокоскоростные технологии на основе витой пары и оптоволоконного кабеля;
- сравнить технологии, обеспечивающие передачу пакетов и ячеек и применяемые для их реализации интерфейсы;
- рассказать о методах передачи данных в глобальных сетях, использующих двухточечные соединения, Т-линии, SONET, ISDN и беспроводные технологии.

Построение локальных и глобальных сетей возможно благодаря наличию передающей среды. Инфраструктура современных сетей строится на базе разнообразных кабельных систем, использующих медные и оптоволоконные кабели, а также на основе беспроводных соединений. По мере роста потребности в быстрой передаче данных значительно развивались возможности кабельных и беспроводных коммуникаций. Также совершенствовались методы передачи информации в этих средах. Например, всего несколько лет назад стало возможным подключение настольных систем по витой паре и оптоволокну со скоростью 100 Мбит/с. В настоящее время для настольных систем уже доступны скорости 1 Гбит/с и выше, что открывает путь для новых быстрых коммуникаций с передачей мультимедиа.

В начале этой главы описываются организации, разрабатывающие стандарты, влияющие на методы и среды передачи сетевых сигналов. Затем рассказывается о множестве коммуникационных кабельных систем, начиная с коаксиального кабеля, используемого в старых сетях, и заканчивая современными оптоволоконными кабелями, используемыми ныне. Будут рассмотрены высокоскоростные технологии, в том числе Fast Ethernet, Gigabit Ethernet и 10 Gigabit Ethernet. Вы узнаете о том, как для передачи данных используются пакеты и ячейки, а также о специальных методах передачи сигналом включая двухточечные соединения, Т-линии, SONET, ISDN и беспроводные коммуникации.

Организации по сетевым стандартам

Несколько национальных и международных организаций играют важную роль в разработке сетевых стандартов, обеспечивающих общий фундамент для осуществления коммуникаций и разработки сетевого оборудования Ниже перечислены основные такие организации (описанные подробно в следующих разделах):

- Национальный институт стандартизации США (ANSI);
- Институт инженеров по электротехнике и электронике (IEEE);
- Международный телекоммуникационный союз (ITU);
- Международная организация по стандартизации (ISO);
- Общество Интернета (ISOC) и входящая в нее Проблемная группа проектирования Интернета (IETF);
- Ассоциация электронной промышленности (EIA) и Ассоциация промышленности средств связи (TIA). Я

Национальный институт стандартизации США (ANSI)

Одной из организаций по стандартам, влияющей на многие технологические отрасли, является *Национальный институт стандартизации* (American National Standards Institute, ANSI). Основанный в 1918 году, институт ANSI сотрудничает с правительством США, правительственными комитетами и международными группами и согласует решения на стандартизацию продуктов, начиная от шлемов для велосипедистов и заканчивая коммуникационными кабелями. В качестве членов в ANSI входят свыше 1000 компаний и учреждений; институт ANSI участвовал в разработке более 14 000 промышленных стандартов. В области компьютерных технологии этот институт разрабатывал стандарты, определяющие, например, характеристики дисплеев, параметры цифровых коммуникаций и методы оптоволоконной связи. Институт ANSI выступает как представитель США в Международной организации по стандартизации (ISO), описываемой ниже.

Институт инженеров по электротехнике и электронике (IEEE)

Основной международной организацией, устанавливающей коммуникационные стандарты, является *Институт инженеров по электротехнике и электронике* (Institute of Electrical and Electronics Engineers, IEEE). IEEE – сообщество профессионалов, объединяющее научные, технические и образовательные учреждения в более чем 150 странах. Входящий в IEEE Комитет по локальным сетям Компьютерного общества (Computer Society 10cal Network Committee) разработал многие из используемых в настоящее время сетевых стандартов. Одними из важнейших являются стандарты 802, определяющие характеристики физических кабелей и методы передачи данных в локальных сетях. Разработка стандартов 802 началась в 1980 году с создания комитета IEEE 802 и Проекта 802.

В состав стандартов 802 входят следующие спецификации:

- 802.1: обзор стандартов 802;
- 802.2: стандарты на методы управления логическим соединением (10gical link control, LLC) и другие стандарты, определяющие базовый уровень сетевой связи;
- 802.3: стандарты на метод доступа Carrier Sense Multiple Access with Collision Detection, CSMA/CD (Множественный доступ с контролем несущей и обнаружением конфликтов);
- 802.4: стандарты на шину с передачей маркера;
- 802.5: стандарты на маркерное кольцо и на взаимодействие между локальными и региональными сетями;
- 802.6: стандарты для локальных и региональных сетей, включая высокоскоростную передачу данных и коммуникации без установления соединения;
- 802.7: стандарты на технологии с использованием широкополосного кабеля;
- 802.8: стандарты на технологии с использованием оптоволоконного кабеля;
- 802.9: стандарты на комплексные сетевые службы, например, для передачи речи и данных;
- 802.10: стандарты безопасности на взаимодействие локальных и региональных сетей;
- 802.11: стандарты на беспроводные методы передачи данных;
- 802.12: стандарты на метод приоритетного доступа по запросу;
- 802.14: стандарты на коммуникации с использованием широкополосного телевизионного кабеля;
- 802.15: стандарты на персональные сети, использующие беспроводные коммуникации;
- 802.16: стандарты на региональные сети, использующие широкополосные беспроводные коммуникации.

В практическом задании 3-1 рассматриваются стандарты, работа над которыми ведется в настоящее время в подкомитетах Проекта 802.

Международный телекоммуникационный союз (ITU)

Еще одна международная организация по стандартам, *Международный телекоммуникационный союз* (International Telecommunications Union, ITU), устанавливает стандарты на модемы, электронную почту и цифровые телефонные системы. ITU участвовал в разработке следующих стандартов:

- стандарты V для модемных коммуникаций, например, новые стандарты V.90 и V.92 для скорости 56 Кбит/с;
- стандарт глобальных сетей X.25 для сетей с коммутацией пакетов;
- стандарты X.400 на международную электронную почту и управление сообщениями;
- стандарты X.435 на передачу электронных данных (обмен электронными данными) с

использованием служб управления сообщениями;

- стандарты X.500 на создание однородных служб каталога (directory services) для доступа к сетевым объектам и управления ими (каталоги Novell Directory Services и Microsoft Active Directory частично соответствуют стандартам X.500);
- стандарты X.509 на использование цифровых сертификатов в качестве средства обеспечения безопасности при сетевом доступе и для Интернет-соединений, для чего сертификаты идентифицируют взаимодействующие стороны, например, пользователей или службы веб-сайтов.

Служба каталога представляет собой хранилище данных и сведений о сетевых ресурсах, таких как компьютеры, принтеры, учетные записи пользователей и групп. Во-первых, такой каталог является централизованным списком ресурсов, позволяющим быстро находить конкретные объекты. Во вторых, каталог обеспечивает механизм доступа к сетевым ресурсам управления ими. Службы каталога, такие как Novell Directory Services (NDS B и Microsoft Active Directory, используют протокол *Ligfitweght Directory Access Protocol,* LDAP (Облегченный протокол службы каталогов). Протокол LDAP был разработан в 1990-х годах в качестве реально работающего механизма, частично реализующего стандарт X.500. Стандарт X.500 описывал протокол клиентского доступа к данным (Data Access Protocol, DAP) и системный протокол каталога (Directory System Protocol, DSP); оба этих протокола являются основой LDAP.

Примечание

Обратите внимание на то, что протокол LDAP описан в RFC 1777. Одним из достоинств протокола LDAP является то, что он позволяет одновременно обращаться к информации, хранящейся в разных службах каталогов. Для администратора сети или системы это означает уменьшение управленческих затрат (например, можно создать учетную запись и пароль в каталоге Microsoft Active Directory, а затем с помощью LDAP-совместимой утилиты автоматически создать эту же запись с паролем в каталоге Novell Directory Services).

Международная организация по стандартизации (ISO)

Международная организация по стандартизации (International Organization for Standardization, ISO) является неправительственным образованием, расположенным в Женеве (Швейцария) и имеющим в своем составе свыше 140 стран-участниц. Организация ISO была образована в 1947 году для стимулирования международного взаимодействия и разработки стандартов в перечисленных ниже областях:

- наука;
- технологии;
- торговля;
- интеллектуальная собственность.

Организация ISO особенно заинтересована в выработке стандартов для компьютерной индустрии, которая оказывает значительное влияние на глобальные коммуникации. ISO работала над продвижением открытых систем, стремясь стимулировать инновации и конкуренцию между производителями компьютеров.

Примечание

Международная организация по стандартизации приняла аббревиатуру ISO не как сокращение, а как всеобщий термин, означающий "стандарт" во всех языках. Аббревиатура ISO порождена от греческого слова "isos", означающего "равный, одинаковый". По мнению учредителей, понятия "равный" и "стандартный" тесно взаимосвязаны, поэтому они отбросили в слове букву "s", чтобы это означало "стандартный" для всех стран-участниц.

Общество Интернета (ISOC) и Проблемная группа проектирования Интернета (IETF)

Общество Интернета (Internet Society, ISOC) является некоммерческой международной организацией, спонсирующей конференции и публикации, также координирующей принятие стандартов Интернета. *Проблемная группа проектирования Интернета* (Internet Engineering Task Force, IETF) когда-то была независимой организацией, а ныне существует как группа в составе

ISOC. Группа IETF ориентирована на технические проблемы Интернет, например, вопросы маршрутизации. Она была введена в состав ISOC Для того, чтобы упростить ее финансирование и стимулировать международное сотрудничество в сфере разработки стандартов Интернета.

ISOC является важным источником поддержки относительно новой организации – *Internet Corporation for Assigned Names and Numbers,* ICANN (Центр по назначению имен и уникальных параметров Интернета). Эта организация координирует назначение доменных имен. Она определяет создании новых имен доменов верхнего уровня (например, .biz) и помогает устанавливать правила, определяющие, например, требования по ведению реестра доменов.

Ассоциация электронной промышленности (EIA) и Ассоциация промышленности средств связи (TIA)

В 1985 году компьютерные и телекоммуникационные компании обратились к *Ассоциации электронной промышленности* (Electronic Industries Alliance, EIA с просьбой о создании стандартов на сетевые кабели. Были разработаны стандарты на электрические интерфейсы, например, на последовательный компьютерные порты. *Ассоциация промышленности средств связи* (Telecommunications Industry Association, TIA), образованная в 1988 году, явилась самостоятельной единицей в составе EIA, ориентированной на создание стандартов на телекоммуникации и кабельные системы. Например, стандарт EIA/TIA-568 описывает кабельные системы промышленных зданий и телекоммуникаций. Обсуждаемые в данной книге принципы *структурированная кабельных систем* (structured wiring) основаны на этом стандарте, обеспечивающем однородность методов проводки и соответствие методам передаче данных, таким как Ethernet и маркерное кольцо. Согласно стандарту EIA/TIA-568, *горизонтальная разводка* должна соединять рабочие станции Я серверы в рабочей области, а *магистральные кабели* должны объединять комнаты с сетевым оборудованием, этажи и здания. Стандарт указывавши какой тип коммуникационного кабеля должен использоваться в конкретных случаях, а также минимальную и максимальную длину отрезков кабеля. Например, как вы узнаете позднее, правила эксплуатации витой пары отличаются от требований к коаксиальным кабелям.

Примечание

Описываемый в книге стандарт EIA/TIA-568 широко применяется в станах Северной Америки. В европейских странах используется похожий стандарт – ISO/IEC 11801.

В дополнение к стандарту EIA/TIA-568 имеется стандарт EIA/TIA-569, определяющий требования к централизованным узлам кабельных соединений всего здания, обычно называемым монтажными шкафами. Стандарт EIA/TIA-569 содержит спецификации для различных конфигураций монтажных шкафов:

- *телекоммуникационная комната* – монтажное помещение или шкаф, где располагаются перекрестные связи горизонтальной и вертикальной разводки;
- *главный кросс-узел* – монтажный шкаф, в котором расположены главные кабели и кабели, идущие к основным сетевым и телекоммуникационным устройствам;
- *промежуточный кросс-узел* – монтажный шкаф, где расположены кабели, идущие от главного кросс-узла к другим уровням здания или кабельной системы.

Типы коммуникационной среды

Самые "низкоуровневые" операции по передаче информации выполняются на Физическом уровне модели OSI, или Уровне 1, который образуют коммуникационная среда и интерфейсы. Коммуникационная среда может представлять собой медный или оптоволоконный кабель, а также электромагнитные волны радио- и других диапазонов. Интерфейсы – это устройства, с которыми соединена коммуникационная среда.

Существуют четыре типа коммуникационной среды: коаксиальный кабель, витая пара, оптоволоконный кабель и беспроводные технологии. Коаксиальный кабель и витая пара выполнены на основе медного провода. Оптоволоконный кабель имеет стеклянную (чаще всего) или пластиковую проводящую среду. Беспроводные технологии используют радио- или СВЧ-волны. В следующих разделах в основном рассказывается о кабельных системах, а в *главе 9* будут рассматриваться

беспроводные коммуникации. Для каждой кабельной среды будут перечислены монтажные требования, а также достоинства и недостатки этой среды.

Свойства каждой коммуникационной среды определяют ее применение в конкретных типах сетей. Наиболее распространены кабельные системы на

основе витой пары. Коаксиальный кабель используется, главным образом, в старых локальных сетях и сетях, расположенных в зонах сильных источников помех. Оптоволоконный кабель обычно применяется для высокоскоростных соединений в локальных и глобальных сетях, а также для связи сетей находящихся на различных этажах и в разных зданиях, в тех случаях, когда необходима защита от источников сильных электромагнитных помех или повышенная безопасность. Беспроводные технологии используются, когда прокладка кабеля невозможна или слишком дорога, а также когда необходимо обеспечить мобильность сетевых хостов и устройств.

При выборе наилучшей передающей среды для локальной или глобальной сети важно учитывать возможности и ограничения каждого типа среды, при этом нужно иметь в виду следующие факторы:

- скорость передачи данных;
- возможность применения в конкретных сетевых топологиях;
- расстояния между сетевыми устройствами;
- стоимость кабеля и компонентов;
- дополнительное сетевое оборудование, которое может понадобиться; гибкость и простота установки;
- устойчивость к помехам от внешних источников;
- стоимость модернизации.

Коаксиальный кабель

Коаксиальный (coaxial) *кабель* (нередко называемый просто "коаксиал") бывает двух видов: толстый и тонкий. Толстый кабель использовался в первых сетях и нередко служил магистралью, связывающей разные сети. Это был первый тип передающей среды, определенный стандартами Ethernet, разработанными в начале 1980-х годов. В настоящее время толстый кабель применяется редко, поскольку имеются более выигрышные альтернативы, например, оптоволокно. Тонкий коаксиальный кабель имеет значительно меньший диаметр по сравнению с толстым кабелем и используется для подключения рабочих станций к локальным сетям (хотя он встречается все реже и реже). В практическом задании 3-2 вы познакомитесь с толстым тонким коаксиальными кабелями, а также и с другими типами коммуникационных кабелей.

Толстый коаксиальный кабель

Толстый коаксиальный кабель (также называемый "thicknet" – буквально "толстая сеть") в середине имеет медный или плакированный медно-алюминиевый проводник (рис. 3.1). Толстый кабель довольно большой в диаметре (0,4 дюйма или 10,16мм) по сравнению с тонким кабелем (0,2 дюйма). Проводник окружен изолятором и алюминиевым экраном, в который завернут изолятор. Алюминиевый экран покрывает защитная оболочка, сделанная из поливинилхлорида (ПВХ) или тефлона. Такой тип кабеля также называется кабелем RG-8.

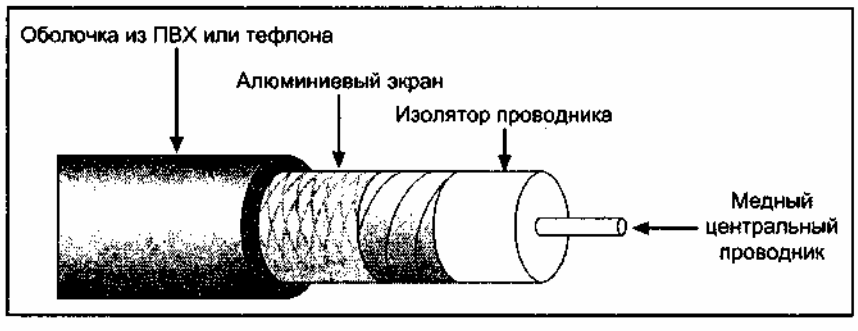


Рис. 3.1. Толстый коаксиальный кабель

Иногда сетевой кабель располагается в *вентиляционной зоне* (plenum area), например, в пространстве между фальшпотолком и перекрытием, имеющимся по всему зданию. Поскольку при горении ПВХ-

оболочка может выделять токсичный газ, в подобных случаях лучше (и зачастую требуется противопожарными правилами) применять специальный кабель (plenum cable) с тефлоновой оболочкой, не выделяющей при горении вредных веществ.

Защитная оболочка кабеля имеет отметки, расположенные через 2,5 м и указывающие места установки устройств подключения к сети (приемопередатчиков). Если расстояние между устройствами будет меньше 2,5 м, затухание сигнала может увеличиться, что вызовет появление сетевых ошибок. Приемопередатчик представляет собой трансивер – модуль подключения к среде передачи данных (media access unit, MAU), который напитывается от кабеля небольшим током (0,5 А) и оборудован 15-контактным разъемом *интерфейса подключаемых устройств* (attachment unit interface, AUI).

AUI-разъем соединяется кабелем с сетевым узлом, у которого имеется свое AUI-подключение к сетевому адаптеру (рис. 3.2). AUI – это стандартный интерфейс для соединителей и интерфейсных схем, электрические характеристики которого позволяют физически подключать устройство к коаксиальному кабелю, витой паре или оптоволоконному магистральному кабелю. Толстый AUI-кабель может иметь длину до 50 м, а тонкий или офисный AUI-кабель в длину не превышает 12,5 м.

Полное сопротивление, или *импеданс* (активное и реактивное сопротивление), толстого коаксиального кабеля равняется 50 Ом, и сегменты кабеля заканчиваются N-коннекторами с подключенным 50-омным резистором. Импеданс представляет собой полное сопротивление протекающему току и измеряется в Омах. Он влияет на то, с какой скоростью фрейм или пакет могут передаваться по проводнику в оптимальных условиях. Терминатор содержит резистор, поглощающий каждый сигнал, достигающий конца сети. Без терминатора сегмент сети будет нарушать спецификации IEEE, поскольку сигналы смогут отражаться и возвращаться обратно в кабель, по которому они передавались. Отраженный сигнал будет нарушать временные параметры сети и может накладываться на новые передаваемые сигналы.

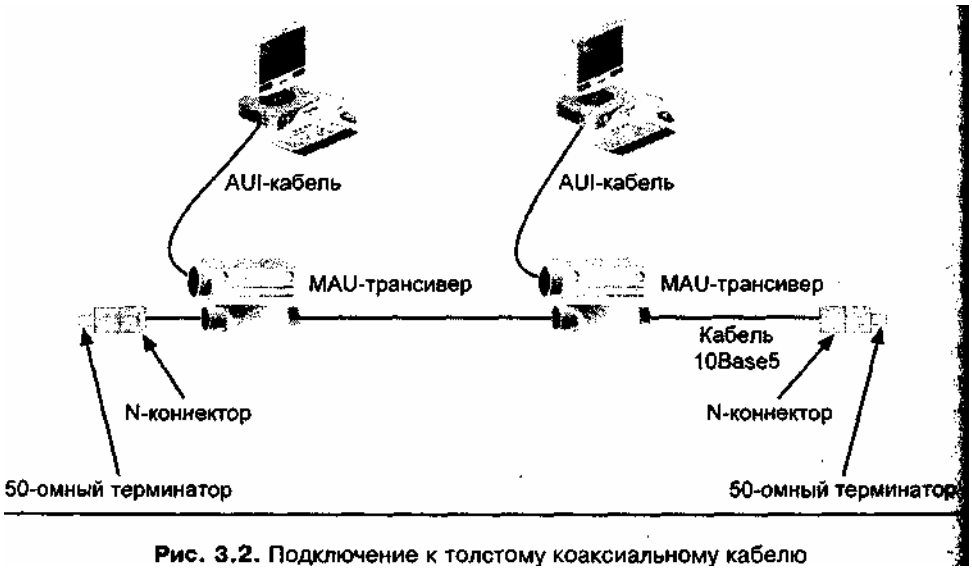


Рис. 3.2. Подключение к толстому коаксиальному кабелю

Толстый коаксиальный кабель плохо гнется, поэтому при его использовании необходимо следить за минимальным радиусом скруглений. Положительным качеством толстого кабеля является то, что по сравнению с тонким кабелем он лучше защищен от радио- или электромагнитных помех (помехи физического уровня), поскольку имеет больший диаметр проводника алюминиевого экрана.

Как показано в табл. 3.1, толстый коаксиальный кабель используется в шинных сетях, скорость передачи в которых обычно равна 10 Мбит/с. В соответствии со стандартами IEEE максимальная длина сегмента кабеля равна 500 м. Кратко эти спецификации называются 10Base5. Цифра 10 означает скорость передачи по кабелю, равную 10 Мбит/с. Base означает, что используется узкополосная, а не широкополосная передача данных. Цифра 5 соответствует максимальной длине сегмента кабеля, равной 5 * 100 м.

Таблица 3.1. *Параметры толстого коаксиального кабеля (WBaseS) при использовании в сетях Ethernet*

Параметр	**Спецификация Ethernet**
Волновое сопротивление (импеданс)	50 Ом

Максимальная длина	500 м
Максимальное количество кабельных отводов в сегменте	100 (включая терминаторы)
Минимальное расстояние между отводами	2,5 м
Максимальная длина AUI-кабеля	50 м для толстого AUI-кабеля и 12,5 м для тонкого (офисного) AUI-кабеля
Максимальная скорость	10 Мбит/с
Полоса рабочих частот	Узкополосная передача
Максимальное количество соединенных сегментов	5
Максимальное количество сегментов имеющих отводы	3
Максимальное количество повторителей (сколько раз сигнал может усиливаться с восстановлением синхронизации)	4
Максимальная общая длина с использованием повторителей	2500 м

При *узкополосной передаче* (baseband) вся емкость передающей среды используется одним сигналом данных. Следовательно, в каждый момент времени на передачу может работать только один узел. При *широкополосной передаче* (broadband) в одной передающей среде реализуются несколько коммуникационных каналов. Благодаря этому несколько узлов могут передавать сигналы одновременно. Способность, канала передавать данные с определенной скоростью, например, 10 Мбит/с или 100 Мбит/с, называется его *полосой пропускания* (bandwidth), или пропускной способностью.

Толстый коаксиальный кабель может использоваться для обоих способов передачи сигналов, но обычно он применяется в цифровых сетях для узкополосной передачи данных. Толстый кабель не так распространен, как другие типы кабелей, что объясняется его большим диаметром и сложностями при его укладке и установке терминаторов. Кроме этого, для его приобретения и монтажа требуются значительные расходы. Однако он очень долговечен, надежен и защищен от помех.

Тонкий коаксиальный кабель

Тонкий коаксиальный кабель напоминает обычный телевизионный кабель Однако, в отличие от телевизионного кабеля, электрические характеристики сетевого кабеля очень точно соблюдаются и должны соответствовать спецификациям, установленным IEEE. Требования для сетей Ethernet определяют импеданс тонкого кабеля, равный 50 Ом (как и для толстого коаксиального кабеля). Тонкий кабель имеет маркировку RG-58A/U. Сетевые администраторы называют его кабелем 10Base2 (а также "thinnet" или "cheapernet" буквально, "тонкая или дешевая сеть"), поскольку его максимальная скорость передачи равна 10 Мбит/с, он может иметь сегменты длиной до 185 (до 1990 года она равнялась 200 м) и используется для узкополосной (Base) передачи данных. Однако на перечисленные параметры влияют свойства сетевого оборудования, например, повторители (репитеры) могут усиливать и повторно синхронизировать сигнал для передачи на большие расстояния (об этом будет рассказано в *главе 4).*

В центре тонкого коаксиального кабеля находится медный или плакированный медью алюминиевый проводник, окруженный изолирующим материалом. Этот изолятор обернут в медную оплетку, поверх которой в высококачественных кабелях идет слой алюминиевой фольги. Сверху кабель защищает поливинилхлоридной или тефлоновой изолирующей оболочкой. Вся конструкция напоминает устройство толстого кабеля, показанного на рис. 3.1, однако тонкий кабель значительно меньше в диаметре и бывает окрашен различные цвета.

Тонкий коаксиальный кабель подключается к *байонетному разъему* (Bayonet Connector, BNC), который в свою очередь соединен с Т-образным коннектором (в практическом задании 3-3 рассматриваются различные виды кабельных разъемов, включая BNC-соединители). Центральная часть коннектора подключается к сетевому адаптеру компьютера или сетевого устройства. Если компьютер или

устройство расположено на конце кабеля то на свободном конце Т-коннектора устанавливается терминатор, как показано на рис. 3.3. В практическом задании 3-4 рассказывается, как устанавливать BNC-разъем на тонком кабеле.

BNC-разъем устроен по типу штыкового соединения (bayonet – штык). Вилочная часть разъема имеет два небольших выступа, которые входят в спиральные канавки, расположенные на гнездовой половине разъема. Для соединения нужно половинки разъема повернуть относительно друг друга на четверть оборота.

Иногда неопытные монтажники или пользователи по ошибке включают ответвительный кабель (небольшой отрезок тонкого кабеля) между Т-коннектором и сетевой платой устройства, соединенного с сетью, и получается что Т-коннектор не связан непосредственно с сетевой платой. Это делается в попытке увеличить расстояние между коннектором и платой или в случае когда неудобно подключать коннектор непосредственно к плате. Такое решение не соответствует спецификациям IEEE и может вызвать проблемы в сети, например, привести к отсутствию соединения.

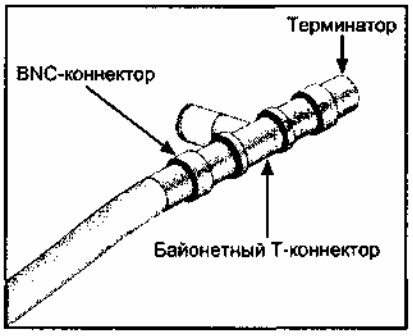


Рис. 3.3. Байонетный (BNC) Т-коннектор с терминатором на одном конце

Совет

Неправильное применение ответвительного кабеля может привести к серьезным последствиям. Одна рабочая станция, подключенная к Т-коннектору через ответвительный кабель, может нарушить работоспособность всех других станций, подключенных к данному сегменту основного кабеля.

Тонкий коаксиальный кабель устанавливать проще и дешевле, чем толстый кабель, хотя еще проще устанавливать и использовать витую пару. Это одна из причин того, что в настоящее время коаксиальные кабели применяются в ограниченном объеме. Преимуществом тонкого кабеля по сравнению с витой парой является его устойчивость к радио- и электромагнитным помехам. В табл. 3.2 перечислены характеристики тонкого коаксиального кабеля при работе в сетях Ethernet.

Таблица 3.2. *Параметры тонкого коаксиального кабеля (10Base2) при использовании в сетях Ethernet*

Параметр	**Спецификация Ethernet**
Волновое сопротивление (импеданс)	50 Ом
Максимальная длина	185м
Максимальное количество кабельных отводов в сегменте	30 (включая терминаторы)
Минимальное расстояние между отводами	0,5 м
Максимальная скорость	10 Мбит/с
Полоса рабочих частот	Узкополосная передача
Максимальное количество соединенных сегментов	5
Максимальное количество сегментов, имеющих отводы	3

Параметр	Спецификация Ethernet
Максимальное количество повторителей (сколько раз сигнал может усиливаться с восстановлением синхронизации)	4
Максимальная общая длина с использованием повторителей	925 м

Примечание

Коаксиальные кабели по-прежнему используются при наличии значительных радио- и электромагнитных помех, например, в машинных цехах и на заводах где имеются мощные двигатели или другое электрическое оборудование. Я

Совет

Если пользователи жалуются на замедление работы сети или потерю соединений, то для обнаружения проблем в тонком коаксиальном кабеле исследуйте места, где кабель может быть слишком изогнут, прижат столом или загнут возле разъема.

Витая пара

Кабель на основе витой пары (или просто "витая пара"), напоминающий обычный телефонный провод, был одобрен для использования в сетях стандартом IEEE в 1990 году и стал очень распространенной коммуникационной средой. Кабель на основе витой пары представляет собой гибкий коммуникационный кабель, содержащий пары изолированных медных проводов скрученных между собой для уменьшения радио- и электромагнитных помех, и покрытых внешней защитной оболочкой. Витая пара гнется лучше чем коаксиальный кабель, и поэтому лучше может огибать стены и углы. Чаще всего максимальная длина отрезка витой пары равняется 100 м. В настоящее время некоторые производители экспериментируют с витыми парами, предназначенными для скорости передачи 10 Гбит/с.

Совет

Хотя длина витой пары может достигать 100 м, обычно ее ограничивают 90 м чтобы учесть дополнительную длину в сетевом оборудовании и монтажных шкафах.

Витая пара подключается к сетевым устройствам с помощью штепсельных разъемов RJ-45 (рис. 3.4), напоминающих соединители RJ-11, используемые в телефонии. Эти разъемы дешевле Т-коннекторов. Их также легче устанавливать и они обеспечивают более гибкую прокладку кабеля, чем коаксиал. В практическом задании сравнивается гибкость кабелей, а в задании 3-5 вы научитесь монтировать кабель с разъемом. Витая пара бывает двух видов: экранированная и неэкранированная. Чаще используется неэкранированная витая пара, что объясняется ее меньшей стоимостью и высокой надежностью.

Рис. 3.4. Кабель на основе витой пары со штепсельным разъемом RJ-45

Экранированная витая пара

Кабель на основе экранированной витой пары (shielded twisted pair, STP) состоит из пар изолированных одножильных проводов, окруженных плетеным или гофрированным экраном. Плетеный экран используется для внутренней проводки, а гофрированный – для внешней или

подземной проводки. Экран уменьшает влияние на передаваемый сигнал со стороны радио- и электромагнитных волн. Скручивание проводов также уменьшает эти помехи, но не в такой степени, как экран.

Чтобы защита от помех была эффективнее, шаг скрутки для каждой пары должен отличаться от других. Кроме того, для достижения наилучших результатов необходимо экранировать разъемы и настенные розетки. Если основной экран прервется в каком-нибудь месте оболочки, то возможны значительные искажения сигнала. Также для экранированной витой пары большое значение имеет правильное заземление, обеспечивающее надежную опорную точку передаваемого сигнала.

Описываемый тип кабеля рекомендуется в тех случаях, когда рядом с сетью располагается мощное электрическое оборудование или другие источники помех. Первые типы экранированной витой пары – IBM type I, 1A, 2 и 2A – работали на относительно небольшой скорости, равной 4 Мбит/с. Кабель типа 2A в основном применяется для внутренней проводки. Новые типы кабелей могут применяться в высокоскоростных сетях. В верхней части рис. 3.5 изображена экранированная витая пара.

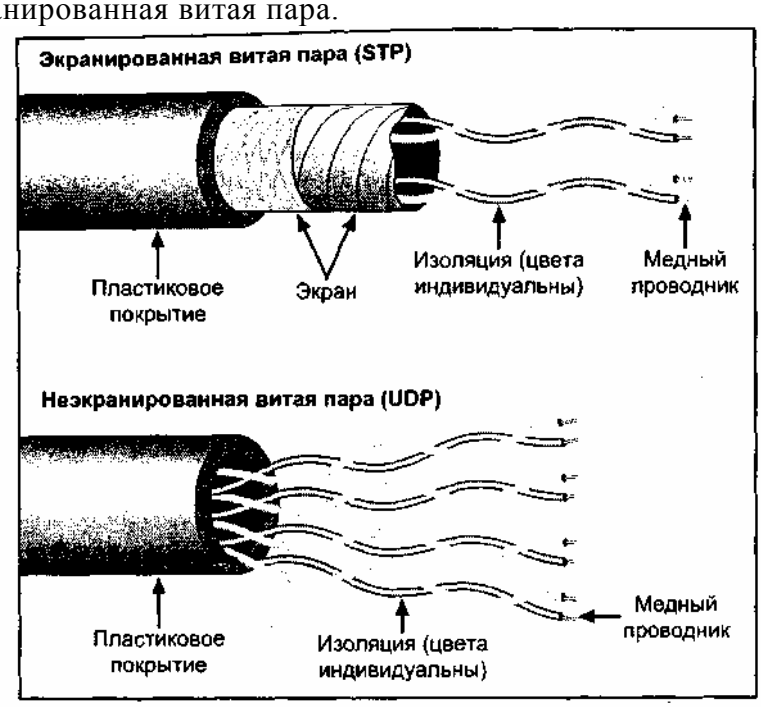


Рис. 3.5. Кабель на основе витой пары

Неэкранированная витая пара

Кабель на основе неэкранированной витой пары (unshielded twisted pair, UTM используется чаще других сетевых кабелей, поскольку он относительно нВ дорогой и прост в установке. Этот кабель состоит из пар проводов в защитной изоляции, причем экранирование между изолированными скрученным проводами и оболочкой кабеля отсутствует. Как и в экранированной витай паре, скрутка пар проводников помогает увеличить защищенность передаваемого сигнала от помех (см. нижнюю часть рис. 3.5). Для уменьшения радио- и электромагнитных помех в сетевое оборудование встраивается электрическое устройство, называемое фильтром передающей среды, однако несмотря на это, неэкранированная витая пара остается плохо защищенном

Часто неэкранированную витую пару называют кабелем 10BaseT. Это означает, что этот кабель имеет максимальную скорость передачи, равной 10 Мбит/с (хотя для некоторых методов передачи данных реальная скорее может составлять 16 Мбит/с), в нем используется узкополосная передача, Я он представляет собой витую пару (twisted pair). Такой вариант витой пары также называется кабелем Категории 3. Витая пара Категории 4 имеет максимальную скорость передачи, равную 20 Мбит/с, Категория 5 обеспечивает скорость 100 Мбит/с, а Категории 5е и 6 могут работать со скоростью 1000 Мбит/с.

В табл. 3.3 перечислены часто используемые категории витой пары, определенные ассоциациями EIA/TIA для работы в сетях Ethernet. В табл. 3.4 перечислены типы витых пар для сетей с маркерным кольцом. Обычно неэкранированная пара используется чаше экранированной, поскольку она имеет меньше точек отказа, у нее нет экрана, который может порваться, а разъемы и настенные

розетки не требуют экранирования. Кроме того, хотя правильное заземление оборудования важно и для неэкранированной витой пары, оно не так сильно отражается на качестве сигнала, как в случае экранированной пары.

Таблица 3.3. *Стандарты на витые пары, используемые в сетях Ethernet*

Витая пара, определенная в спецификациях EIA/TIA-568 для	Экранирование	Максимальная скорость передачи данных
IBM Type 1A	Экранированная	4 Мбит/с
IBM Type 2A	Экранированная	4 Мбит/с
Category 3	Неэкранированная	16 Мбит/с
Category 4	Неэкранированная	20 Мбит/с
Category 5	Неэкранированная	100 Мбит/с
Category 5e	Неэкранированная	1000 Мбит/с (для гарантированной работы в среде Gigabit Ethernet)
Category 6	Неэкранированная	1000 Мбит/с (для гарантированной работы в среде Gigabit Ethernet)

Таблица 3.4. *Витые пары, применяемые в сетях с маркерным кольцом*

Тип кабеля	**Описание**
Type 1 и 1A	Кабель на основе экранированной витой пары, состоящей из двух пар проводов калибра AWG-22, окруженных сетчатым экраном, используемый для прокладки в кабелепроводах, на стенах и в монтажных коробах
Type 2 и 2A	То же, что и для типа 1; однако для задач телефонии поверх экрана добавляются четыре пары из проводов калибра AWG-22– AWG-26
Type 3	Неэкранированные четыре пары из проводов калибра AWG-22–AWG-24; уступающие по характеристикам типам 1 и 2 из-за меньшей устойчивости к радио- и электромагнитным помехам
Type5	Оптоволоконный кабель с жилой 62,5/125 или 100/140 микрон, применяемый в первую очередь для кольцевых магистралей
Type 6 и 6A	Экранированные витые пары из проводов калибра AWG-26, используемые в качестве кросс-кабелей и для кабелей сетевых адаптеров сетей с маркерным кольцом
Type 8	Экранированные витые пары из проводов калибра AWG-26 с пластиковым защитным коробом для монтажа на полу в тех случаях» когда кабель нельзя пустить по стенам
Type 9	Экранированная витая пара из проводов калибра AWG-26 в оболочке

Примечание

Спецификация AWG (American Wire Gauge) определяет диаметр провода. Чем выше число AWG, тем меньше диаметр провода. Провода, используемые в экранированных и неэкранированных витых парах для

локальных сетей и телефонии, обычно представляют собой одножильный медный провод калибра AWG-22–AWG-26 (провод AWG-26 имеет меньший диаметр, чем провод AWG-22). Если витая пара имеет сравнительно большую длину, то меньшее затухание обеспечивает провод с большим диаметром, например, AWG-22.

В практическом задании 3-6 рассказывается о том, как сконфигурировали сетевой адаптер для работы с коаксиальным кабелем или витой парой в системах Windows 2000 и Windows XP. В задании 3-7 описывается процесс конфигурирования типа передающей среды для сетевого адаптера в системе Red Hat Linux 7.*x*.

Витые пары Категории 5e и Категории 6 часто применяются в новых кабельных системах, поскольку они обеспечивают высокую скорость передачи данных – до 1000 Мбит/с.

В табл. 3.5, 3.6 и 3.7 перечислены характеристики витых пар, используемых в сетях Ethernet (10 Мбит/с) и маркерных кольцах.

Таблица 3.5. *Параметры неэкранированной витой пары 10baseT при использовании в сетях Ethernet*

Параметр	Спецификация Ethernet
Максимальная длина сегмента	100 м
Максимальное количество узлов в сегменте	2 узла
Минимальное расстояние между узлами	3 м
Максимальное количество сегментов	1024
Максимальное количество сегментов с узлами	1024
Максимальное количество концентраторов, связанных в цепочку	4
Импеданс	1000 м

Таблица 3.6. *Параметры экранированной витой пары10ВавеТ при использовании в сетях Ethernet*

Параметр	**Спецификация Ethernet**
Максимальная длина сегмента	100 м
Максимальное количество узлов в сегменте	2 узла
Минимальное расстояние между узлами	3 м
Максимальное количество сегментов	1024
Максимальное количество сегментов с узлами	1024
Максимальное количество концентраторов, связанных в цепочку	4
Импеданс	150 Ом

Таблица 3.7. *Параметры маркерного кольца*

Параметр	**Спецификация Token Ring**
Количество узлов, подключенных к одному модулю множественного доступа (MAU)	От 8 до 1 6
Максимальная длина сегмента для кабеля Type 1 при использовании только одного модуля MAU	300 м
Максимальная длина сегмента для других типов кабеля	STP: 100 м UTP: 45,5 м Оптоволокно: 100 м
Максимальное количество модулей MAU во всем кольце	От 1 2 до 33 *(см. главу 4)*
Максимальное количество узлов во всем кольце	260

Максимальное количество узлов в кольце с кабелем Type3	72

Оптоволоконный кабель **1**

Оптоволоконный кабель (fiber optic cable) состоит из одной или нескольких стеклянных или пластиковых жил (световодов), покрытых слоем стекла, называемым плакированием (cladding). Плакированные световоды помещают в поливинилхлоридную оболочку, как показано на рис. 3.6. Для передачи сигнала по световодам обычно используются источники света инфракрасного диапазона.

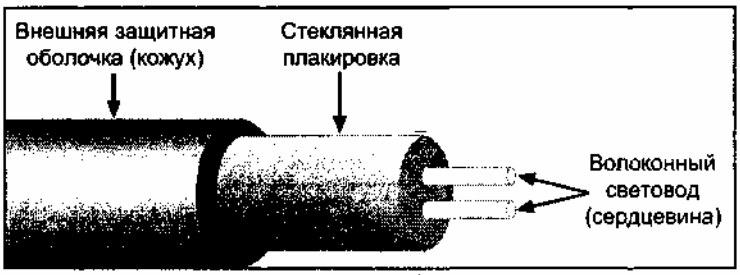


Рис. 3.6. Оптоволоконный кабель

Обычно используются оптоволоконные кабели трех размеров. Размер измеряется в микронах и имеет две составляющие: диаметр световода и диаметр оболочки. Например, кабель размера 50/125 мкм (микрон) имеет световод диаметром 50 мкм и оболочку диаметром 125 мкм. Два других распространенных размера– 62,5/125 мкм и 100/140 мкм. Все три типа кабеля могут работать в многомодовом режиме, что означает возможность одновременной передачи по кабелю нескольких световых волн. Чаще всего для работы многомодовом режиме выбирается кабель 62,5/125 мкм.

Световод кабеля передает импульсы света, генерируемые лазером или светодиодом. Стеклянная оболочка предназначена для отражения света обратно в световод. Оптоволоконный кабель может передавать данные со скоростями от 100 Мбит/с до 100 Гбит/с. Он используется для магистралей кабельных систем, например, укладывается между этажами одного здания или между разными зданиями, а также и на большие расстояния. Оптоволоконная магистраль между этажами иногда называется *толстой трубой* (fat pipe), поскольку имеет большую полосу пропускания, достаточную для обеспечения высокоскоростных коммуникаций с узкополосной и широкополосной передачей данных. Чаще всего оптоволоконный кабель применяется в кампусах (городских сетях) для связи различных зданий в соответствии со спецификациями ШЕЕ на кабельные системы. Также он может использоваться глобальных сетях и телекоммуникационных системах для объединения удаленных локальных сетей. Преимуществом оптоволокна является его высокая полоса пропускания и малое затухание сигнала, что позволяет обеспечивать его передачу на большие расстояния.

Поскольку для передачи данных используются импульсы света ("включено" и "выключено"), радио и электромагнитные помехи не влияют на работу оптоволоконного кабеля; при этом передача данных является чисто цифровой, а не аналоговой. Сравните это с принципом действия коаксиального кабеля или витой пары, в той или иной степени подверженных помехам, что является заметным недостатком этих типов передающей среды. Однако как коаксиал, так и витая пара могут использоваться и для аналоговых, и для цифровых коммуникаций, что в некоторых случаях может быть преимуществом по сравнению с цифровым оптоволоконным кабелем.

Еще одним достоинством оптоволокна по сравнению с коаксиальным кабелем или витой парой является то, что к оптоволоконному кабелю очень трудно получить неавторизованный доступ в силу его конструкции. Недостатком этого типа кабеля является его высокая хрупкость, относительно высокая стоимость и высокие требования к монтажному оборудованию и квалификации обслуживающего персонала.

Передача сигналов при помощи световых волн зависит от их длины. Некоторые волны проходят по оптоволокну лучше, чем другие. Длина волны изменяется в миллимикронах (nanometer, nm). Видимый свет с длиной волны 400–700 nm недостаточно хорошо передается по оптоволокну, чтобы использовать его для передачи данных. Более эффективны для этих целей волны инфракрасного диапазона с длиной 700–1600 nm. Для оптических коммуникаций существуют три идеальных длины волны: 850, 1300 и 1550 nm. Для высокоскоростной связи обычно используется длина 1300

nm.

Передаваемый оптический сигнал должен иметь мощность, достаточную для того, чтобы он достиг приемника и мог быть распознан. *Затухание,* или потеря сигнала, это часть сигнала, потерянная при его передаче по коммуникационной среде от источника (передающего узла) к приемному узлу. Затухание в оптоволоконном кабеле измеряется в децибелах (дБ). Потери оптического сигнала непосредственно связаны с длиной кабеля, а также с количеством и радиусом его изгибов. Также мощность сигнала теряется по мере его прохождения через коннекторы и стыки.

Чтобы световая волна могла быть точно распознана на принимающем узле, она должна иметь некоторую минимальную мощность при выходе из передающего устройства. Уровень минимальной мощности называется энергетическим потенциалом. *Энергетический потенциал* (power budget) для коммуникаций с использованием оптоволокна – это разница между излучаемой Мощностью и окончательной величиной сигнала (чувствительностью) на принимающем узле, измеренная в децибелах. Именно минимальная мощность передатчика и чувствительность приемника определяют, насколько сигнал успешно передается и принимается без искажений. Для высокоскоростные коммуникаций энергетический потенциал должен быть не менее 11 дБ.

Оптоволоконные кабели бывают двух видов: одномодовые и многомодовые. *Одномодовый кабель* (single-mode cable) главным образом используется для дальней связи, его центральная жила имеет диаметр 8–10 мкм, а оболочка – 125 мкм. Диаметр жилы такого кабеля намного меньше, чем для многомодового кабеля, и в каждый момент времени по нему передается толы одна световая волна.

В одномодовом кабеле для передачи сигналов используется луч лазера. Источник света, расположенный в передающем интерфейсе передатчика имеющий относительно большую полосу пропускания, обеспечивает передачу данных с высокой скоростью на большое расстояние – до 45 км. Одномодовый оптоволоконный кабель не имеет определенных ограничений скорости передачи.

Многомодовый оптоволоконный кабель (multimode cable) может обеспечить одновременную передачу нескольких световых волн, что необходимо для широкополосных коммуникаций. По сравнению с одномодовым кабелем возможная длина кабеля не так велика – всего 2 км, поскольку полоса пропускания меньше, а источник света слабее. В качестве источника сигнала для многомодового кабеля применяется светодиод, установленный в сетевом интерфейсе передающего узла.

Многомодовые кабели бывают на основе волокна двух видов: *со ступенчатым профилем показателя преломления* (step-index fiber) и *с плавно изменяющимся показателем преломления* (graded-index fiber). В первом случае свет внутри кабеля отражается как в зеркале, в результате чего разные сигналы передаются с различной задержкой, что увеличивает вероятность искажения при передаче на большие расстояния. Во втором случае световые лучи распространяются в кабеле по маршрутам равной кривизны, из-за чего все сигналы приходят одновременно, а искажения при передаче меньше, чем первом случае.

С оптоволоконными кабелями чаще всего используются два типа коннекторов: абонентский разъем (subscriber connector, SC) и прямой наконечник (straight tip, ST). Оба типа коннекторов соответствуют стандартам EIA/TIA 568. В общем случае, ST-коннекторы можно использовать как с одномодовыми, так и с многомодовыми оптоволоконными кабелями, а ST-коннекторы обычно применяются с одномодовыми кабелями (хотя и с многомодовыми кабелями они также могут использоваться). SC-коннекторы имеют квадратный профиль и для фиксации вставляются в гнездо. SC-коннекторы – круглые по форме и для фиксации в них применяется байонетный разъем, как в BNC-коннекторах.

Совет

Иногда можно услышать термин "темное оптоволокно" (dark fiber), относящийся к установленному оптоволоконному кабелю, но не используемому в данный момент.

В табл. 3.8 и 3.9 перечислены характеристики одномодового и многомодового оптоволоконного кабеля, отвечающего спецификациям EIA/TIA-568-B.

Таблица 3.8. *Спецификации EIA/TIA-568-B для одномодового оптоволоконного кабеля, используемого в качестве магистрали кабельной системы*

Параметр	Значение или характеристика

Параметр	Значение или характеристика
Максимальная длина одного магистрального сегмента	3000 м
Максимальная длина одного горизонтального сегмента (к настольной системе)	Не рекомендуется использовать для горизонтальной разводки
Максимальное количество узлов в сегменте	2
Максимальное затухание	Менее 0,5 дБ/км
Тип кабеля	8,3/125мкм
Коннектор	ST или SC

Таблица 3.9. *Спецификации EIA/TIA-568-B для многомодового оптоволоконного кабеля, используемого в качестве магистрали кабельной системы*

Параметр	**Значение или характеристика**
Максимальная длина одного магистрального сегмента	2000 м
Максимальная длина одного горизонтального сегмента (к настольной системе)	100 м
Максимальное количество узлов в сегменте	2
Максимальное затухание	3,75 дБ/км для коммуникаций с использованием длины волны 850 nm; 1,5 дБ/км для коммуникаций с использованием длины волны 1 300 nm
Максимальное количество сегментов	1024
Максимальное количество сегментов с узлами	1024
Максимальное количество концентраторов, включенных в цепочку	4
Тип кабеля	62,5/125 мкм
Коннектор	ST или SC

Комбинированная оптокоаксиальная кабельная система

Сети, использующие *комбинированные оптокоаксиальные кабельные системы* (hybrid fiber/coax, HFC), все чаще используются в существующих телекоммуникационных и широкополосных службах. При использовании гибридных систем необходимо учитывать несколько факторов, например, требования к уровню сигнала в разных точках сети, устойчивость к помехам, допустимые искажения сигнала и разводку силового питания.

Сетевые решения, реализуемые на базе кабельных сетей и комбинированных систем, начинают влиять на компьютерную индустрию. Кабельная инфраструктура, содержащая оптоволоконную магистраль и коаксиальные ответвительные кабели, обеспечивает высокую пропускную способность при приеме данных и относительно высокую скорость передачи информации от оконечных узлов. Скорость передачи обычно меньше скорости приема, поскольку предполагается, что скачивание файлов требует более высокой скорости и выполняется чаще, чем их передача.

Изначально системы кабельного телевидения предназначались для рассылки сигналов с использованием широкополосных рассылок. При таком подходе полоса пропускания для передачи информации от клиентов уменьшается (обычно она равна 5–40 МГц), и она совместно используется несколькими потребителями. В настоящее время комбинированные кабельные системы, применяемые в сетях кабельного телевидения, обеспечивают передачу аналогового нисходящего (downstream) потока с частотой от 5 до 450 МГ и пересылку цифровых данных с частотой от 450 до 750 МГц. Недостатком коммуникаций с

использованием сетей кабельного телевидения является то что значительная часть проводки представляет собой плохо экранированный коаксиальный кабель, из-за чего на передачу цифровых данных влияют помехи от электромоторов, портативных радиостанций, микроволновых плит видеомагнитофонов и телеприемников.

В настоящее время для обеспечения возможностей цифровых и других новых служб в больших кабельных сетях устанавливаются комбинированные оптокоаксиальные системы. Оптоволокно позволяет увеличить полосу пропускания восходящего (upstream) потока и уменьшить шум, что в результате повышает качество цифровых коммуникаций. Следует отметить, что свыше 90% существующих кабельных систем не являются оптокоаксиальными, а затраты на прокладку новой такой системы велики.

Комбинированные оптокоаксиальные системы являются весьма перспективными для глобальных коммуникаций по мере развертывания подобных систем в инфраструктуре кабельного телевидения. С их помощью операторы кабельной связи смогут предоставлять услуги телефонии и многоканального интерактивного телевидения, а также услуги высокоскоростной передачи данных для персональных компьютеров. Полноценная оптокоаксиальная система предоставляет следующие возможности:

- обычная телефонная сеть;
- до 37 каналов аналогового телевидения;
- до 188 каналов цифрового телевидения;
- до 464 цифровых точечных каналов (пользовательские службы);
- высокоскоростная двунаправленная передача данных для персональных компьютеров.

По сути, комбинированная система представляет собой единую кабельную инфраструктуру, состоящую из некоторой комбинации оптоволоконных и медных кабелей, соответствующей конкретным требованиям.

Высокоскоростные технологии с использованием витой пары и оптоволоконного кабеля

На основе витой пары и оптоволоконного кабеля разработаны новейшие высокоскоростные технологии локальных сетей, позволяющие передавать значительно больший сетевой трафик по сравнению с трафиком, возможным при первоначальной скорости, равной 10 Мбит/с. Вот эти технологии:

- Fast Ethernet;
- Gigabit Ethernet;
- 10 Gigabit Ethernet.

Fast Ethernet

Необходимость в высокоскоростных технологиях привела к быстрому развитию Ethernet-совместимых устройств, обеспечивающих передачу пакетов по витой паре со скоростью 100 Мбит/с. Чтобы удовлетворить все возрастающий интерес, институт ШЕЕ стандартизовал высокоскоростные технология Ethernet, получившие общее название *Fast Ethernet* ("быстрый" Ethernet).

Поскольку с самого начала производители разделились во мнении о способах реализации исходной концепции, были разработаны две технологии Fast Ethernet. Одна группа разработчиков, представленная компанией Hewlett-Packard, выбрала технологию 100BaseVG, или 100VG-AnyLAN. Другая группа, в состав которой входили компании Bay Networks (позднее приобретенная компанией Nortel Networks), Sun Microsystems и 3Com, разрабатывали технологию 100BaseX. Оба этих решения рассматриваются в следующих разделах.

Стандарт IEEE 802.3u

Стандарт IEEE 802.3u для сетей Fast Ethernet именуется 100BaseX, что представляет собой общее название для нескольких технологий передачи данных, которые, в свою очередь, названы 100BaseT, 100BaseTX, 100BaseTM, 100BaseT2 и 100BaseFX. Во всех перечисленных версиях, за исключением 100BaseT2, для передачи сигнала используется метод доступа CSMA/CD описанный в *главе 2*. Во всех версиях (кроме 100BaseT2) сигнал распространяется по сети в нескольких направлениях (в отличие от 100BaseVG/100VG-AnyLAN). В единственном исключительном случае – в технология 100BaseT2 – для устранения конфликтов сигналы передаются с фиксированной временной задержкой.

Передача сигналов осуществляется по витой паре или оптоволоконному кабелю. Чтобы сеть работала, алгоритмы стандартов 100BaseX запрещают передачу сигнала далее, чем через один повторитель Класса I или два повторителя Класса II (например, через концентраторы, имеющие функции повторителей, усиливающие и повторно синхронизирующие сигнал, или через устройства сопряжения разных коммуникационных сред). Подробнее повторители описаны в *главе 4*.

Требования к витой паре для сегментов 100BaseX аналогичны требованиям стандарта 10BaseT: длина отдельного сегмента – 100 м, максимальное количество сегментов, содержащих узлы, – 1024 (табл. 3.10). Повторитель Класса I преобразует линейный сигнал во входящем порту в цифровой сигнал обеспечивая сопряжение различных типов передающей среды Fast Ethernet, например, оптоволокна (100BaseFX) и витой пары (100BaseTX). При выполнении преобразований повторитель Класса I создает задержки, вследствие чего только один такой повторитель можно помещать в отдельный сегмент локальной сети Fast Ethernet.

Повторитель Класса II немедленно передает сигнал из входного порта во все свои порты. Обычно повторители Класса II имеют порты одного типа передающей среды, например, 100BaseTX. Быстрая передача данных через повторитель обеспечивает очень маленькую задержку, в результате чего в одном сегменте Fast Ethernet могут размещаться до двух повторителей Класса II.

Совет

Чтобы избежать проблем в высокоскоростных сетях Fast Ethernet, необходимо точно следовать стандартам.

Как показано в табл. 3.10, существуют различные способы реализации сетей 100BaseX в зависимости от типа используемой передающей среды.

Таблица 3.10. *Коммуникационные параметры стандартов 100BaseX*

Реализация стандарта 100BaseX	**Описание**	**Расстояние**
100BaseTX	Используется 150-омная экранированная витая пара (две пары проводников) EIA/TIA type 1 или 1A или 100-омная неэкранированная витая пара (две пары проводников) категории 5; скорость передачи – 100 Мбит/с	100 м
100BaseT	Используется 100-омная неэкранированная витая пара (две пары проводников) категории 3, 4 или 5; скорость передачи – 100 Мбит/с	100м
100BaseT4	Используется 100-омная неэкранированная витая пара (четыре пары проводников) категории 3, 4 или 5; скорость передачи –100 Мбит/с	100м в отличие от всех остальных вер- сии Fast Ethernet, не обеспечивает работу в дуплексном режиме (одновременная передача и прием данных)
100BaseT2	Используется 100-омная неэкранированная витая пара (две пары проводников) категории 3, 4 или 5; скорость передачи – 100 Мбит/с	100 м
100BaseFX	Используется дуплексный (двунаправленный) одномодовый или многомодовый оптоволоконный кабель; скорость передачи – 100 Мбит/с	20 км для одномодового кабеля и 2 км – для многомодового

Совет

Хотя в сетях Fast Ethernet вместо кабеля категории 5 (и выше) или оптоволокна можно использовать и

кабели других категорий, именно эти типы передающей среды обеспечивают наибольшую надежность при высокоскоростной передаче данных.

Стандарт IEEE 802.12

Технологая 100BaseVG/100VG-AnyLAN, принятая институтом IEEE в качестве стандарта 802.12, отказалась от CSMA/CD и использует в качестве способа передачи данных механизм, названный *приоритетным доступом по запросу* (demand priority). Этот механизм позволяет передавать сигнал только в одном направлении. Он применяется в звездообразных сетях, где рабочие станции связаны с центральным концентратором. При таком подходе каждый узел обращается к концентратору с запросом на передачу. Эти запросы обслуживаются поочередно. Входящие пакеты анализируются по их адресу назначения и отсылаются непосредственно принимающему узлу звезды. Таким образом, другие узлы этих пакетов не видят (рис. 3.7).

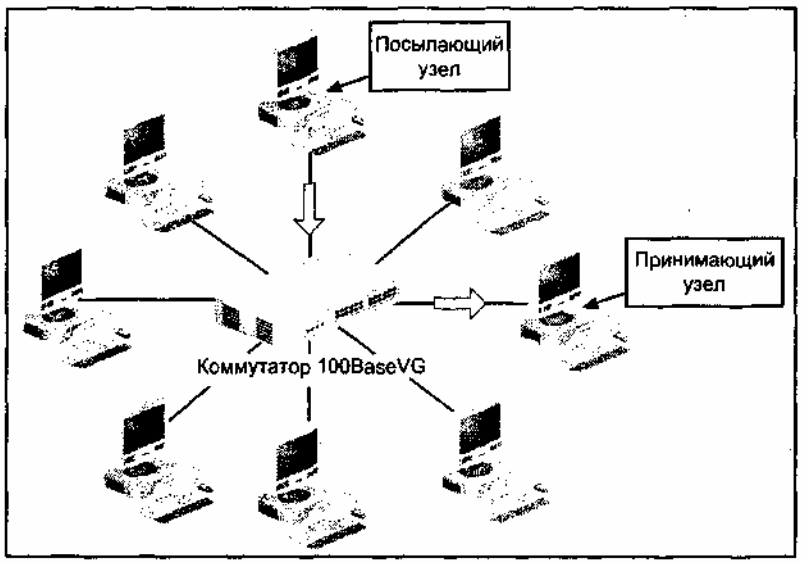


Рис. 3.7. Использование приоритетного доступа по запросу

Благодаря отсутствию конфликтов приоритетный доступ по запросу обеспечивает скорость передачи пакетов до 100 Мбит/с. Помимо высокой скорости, этот метод доступа имеет еще два важных достоинства. Во-первых – безопасность. Поскольку только принимающий узел видит переданный пакет, данные нельзя прочитать и декодировать на любом другом узле. Другим достоинством этого метода является возможность передачи мультимедийных и критичных по времени данных. Подобной информации можно назначить наивысший приоритет, в результате чего речевые сигналы и видео будут передаваться в соответствии с временными параметрами, что позволит минимизировать искажения. Преимуществ технологии 100BaseVG/100VG-AnyLAN заключается в том, что для ее реализации может использоваться витая пара категории 3 и выше, состоящая из четырех пар проводников. Применение кабеля категории 3 возможно благодаря тому, что технология 100BaseVG/100VG-AnyLAN позволяет одновременно передавать данные по всем четырем парам проводников, обеспечивая скорость до 30 Мбит/с по каждой из них (но по всем четырем парам общая скорость не превышает 100 Мбит/с).

Gigabit Ethernet

Технология Gigabit Ethernet, обеспечивающая передачу данных со скоростью до 1 Гбит/с, в первую очередь предназначена в качестве альтернативы перегруженным локальным сетям, когда Fast Ethernet уже не может обеспечить требуемую полосу пропускания. Эта технология представляет собой "истинный" Ethernet, т. к. в ней применяется метод доступа CSMA/CD и она разработана как непосредственное обновление для практически любых Ethernet-сетей 100BaseX, которые соответствуют всем установленным стандартам Gigabit Ethernet. Также проектировщики технологии Gigabit Ethernet стремились сделать ее притягательной для пользователей сетей с маркерным кольцом в звездообразных физических топологиях, которые могут быть преобразованы в комбинацию сетей Fast Ethernet и Gigabit Ethernet, обеспечивающую дополнительную полосу пропускания для развивающихся клиент-серверных, мультимедиа- и VPN-приложений. Технология Gigabit Ethernet одобрена ассоциацией Gigabit Ethernet Alliance, в которую входят свыше 120

компаний-участников.

В особенности технология Gigabit Ethernet ориентирована на конфигурации, которые используют маршрутизируемую передачу данных на Сетевом уровне (Уровне 3). Первым принятым стандартом Gigabit Ethernet был стандарт IEEE 802.3z на оптоволоконные многомодовые и одномодовые кабели. Вслед за ним был принят стандарт IEEE 802.3aЬ на витую пару. Существующие в настоящее время стандарты Gigabit Ethernet перечислены в табл. 3.11.

Таблица 3.11. *Спецификации Gigabit Ethernet*

Реализация технологии Gigabit Ethernet	**Описание**
100BaseCX (короткие соединения между коммутаторами)	Для соединения двух коммутаторов на расстоянии до 25 м используется экранированный медный двухпроводный кабель
100BaseLX (длинноволновый лазер)	Используется многомодовый оптоволоконный 62,5/125 мкм кабель на расстоянии до 550м; многомодовый 50/125мкм кабель на расстоянии до 550 м и одномодовый 1 0 мкм кабель на расстоянии до 5000 м

Стандарт IEEE 802.12

Технология 100BaseVG/100VG-AnyLAN, принятая институтом IEEE в качестве стандарта 802.12, отказалась от CSMA/CD и использует в качестве способа передачи данных механизм, названный *приоритетным доступом по запросу* (demand priority). Этот механизм позволяет передавать сигнал только одном направлении. Он применяется в звездообразных сетях, где рабочие станции связаны с центральным концентратором. При таком подходе каждый узел обращается к концентратору с запросом на передачу. Эти запросы обслуживаются поочередно. Входящие пакеты анализируются по их адресу назначения и отсылаются непосредственно принимающему узлу звезды. Таким образом, другие узлы этих пакетов не видят (рис. 3.7).Н

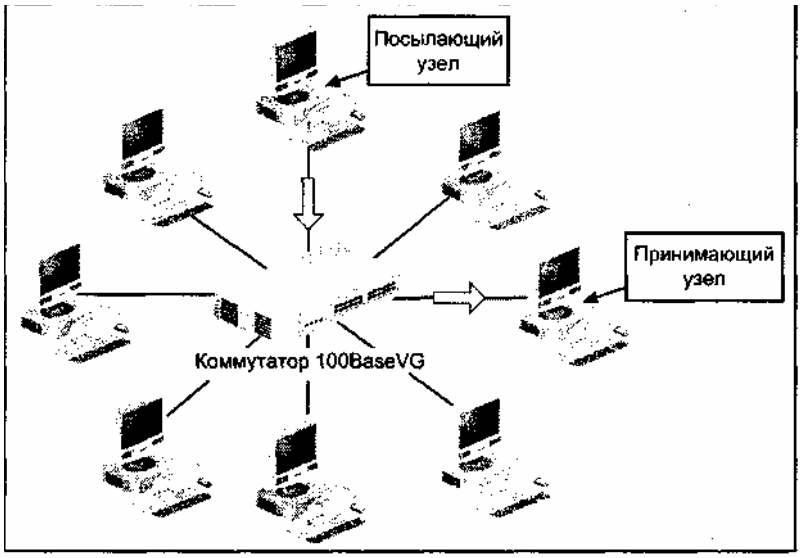


Рис. 3.7. Использование приоритетного доступа по запросу

Благодаря отсутствию конфликтов приоритетный доступ по запросу обеспечивает скорость передачи пакетов до 100 Мбит/с. Помимо высокой скорости, этот метод доступа имеет еще два важных достоинства. Во-первых – безопасность. Поскольку только принимающий узел видит Переданный пакет, данные нельзя прочитать и декодировать на любом другом узле. Другим достоинством этого метода является возможность передачи мультимедийных и критичных по времени данных. Подобной информации можно назначить наивысший приоритет, в результате чего речевые сигналы и видео будут передаваться в соответствии с временными параметрами, что позволит минимизировать искажения. Преимущество технологии 100BaseVG/100VG-AnyLAN заключается в том, что для ее реализации может использоваться витая пара категории 3 и выше, состоящая из четырех пар

проводников. Применение кабеля категории 3 возможно благодаря тому, что технология 100BaseVG/100VG-AnyLAN позволяет одновременно передавать данные по всем четырем парам проводников, обеспечивая скорость до 30 Мбит/с по каждой из них (но по всем четырем парам общая скорость не превышает 100 Мбит/с).

Gigabit Ethernet

Технология Gigabit Ethernet, обеспечивающая передачу данных со скоростью до 1 Гбит/с, в первую очередь предназначена в качестве альтернативы перегруженным локальным сетям, когда Fast Ethernet уже не может обеспечить требуемую полосу пропускания. Эта технология представляет собой "истинный" Ethernet, т. к. в ней применяется метод доступа CSMA/CD и она разработана как непосредственное обновление для практически любых Ethernet-сетей 100BaseX, которые соответствуют всем установленным стандартам Gigabit Ethernet. Также проектировщики технологии Gigabit Ethernet стремились сделать ее притягательной для пользователей сетей с маркерным кольцом в звездообразных физических топологиях, которые могут быть преобразованы в комбинацию сетей Fast Ethernet и Gigabit Ethernet, обеспечивающую дополнительную полосу пропускания для развивающихся клиент-серверных, мультимедиа- и VPN-приложений. Технология Gigabit Ethernet одобрена ассоциацией Gigabit Ethernet Alliance, в которую входят свыше 120 компаний-участников.

В особенности технология Gigabit Ethernet ориентирована на конфигурации, которые используют маршрутизируемую передачу данных на Сетевом уровне (Уровне 3). Первым принятым стандартом Gigabit Ethernet был стандарт IEEE 802.3z на оптоволоконные многомодовые и одномодовые кабели. Вслед за ним был принят стандарт IEEE 802.3ab на витую пару. Существующие в настоящее время стандарты Gigabit Ethernet перечислены в табл. 3.11.

Таблица 3.11. *Спецификации Gigabit Ethernet*

Реализация технологии Gigabit Ethernet	**Описание**
1000BaseCX (короткие соединения между коммутаторами)	Для соединения двух коммутаторов на расстоянии до 25 м используется экранированный медный двухпроводный кабель
1000BaseLX (длинноволновый лазер)	Используется многомодовый оптоволоконный 62,5/125 мкм кабель на расстоянии до 550 м; многомодовый 50/125 мкм кабель на расстоянии до 550 м и одномодовый 10 мкм кабель на расстоянии до 5000 м
1000BaseSX (коротковолновый лазер)	Используется многомодовый оптоволоконный 62,5/125 мкм кабель на расстоянии до 220 или 275 м (расстояние зависит от частоты в кабеле) и многомодовый 50/125мкм кабель на расстоянии до 500 или 550 м (расстояние зависит от частоты в кабеле)
1000BaseTX (витая пара)	Применяется витая пара категории 5, состоящая из 4-х пар проводников; длина кабельных сегментов - до 100 м

10 Gigabit Ethernet

Технология 10 Gigabit Ethernet, одобренная стандартом IEEE 802.3ae, представляет собой высокоскоростной сетевой протокол, конкурирующий другими скоростными технологиями региональных и глобальных сетей, в частности, с сетями SONET (описываемыми в этой главе ниже). Кроме того, она предназначена для реализации быстрых магистралей в локальных сетях. Эта технология соответствует "истинному" стандарту Ethernet, однако функционирует только в полнодуплексном режиме (одновременная двунаправленная передача данных в одной коммуникационной среде), из-за чего отпадает необходимость в использовании метода CSMA/CD в силу принципиального отсутствия конфликтов пакетов. На момент написания книги стандарт был определен только для оптоволоконного кабеля.

Технология 10 Gigabit Ethernet продвигается ассоциацией 10 Gigabit Alliance основанной

компаниями 3Com, Cisco, Extreme Networks, Intel, Nortel Sun Microsystems и World Wide Packets и имеющей в своем составе свыше 120 компаний-участников. В табл. 3.12 перечислены существующие на данный момент стандарты 10 Gigabit Ethernet. Для некоторых стандартов (например, для 10GBaseSR и 10GbaseSW) указаны одинаковые предельный расстояния и тип кабеля; однако это разные спецификации, поскольку они отличаются типом интерфейсов и коммуникационными параметрами.

Таблица 3.12. *Спецификации 10 Gigabit Ethenetr*

Реализация технологии 10 Gigabit Ethernet	**Описание**
10GBaseER	Одномодовый оптоволоконный 9/125мкм кабель для расстояний не более 40 000 м
10GBaseEW	Одномодовый оптоволоконный 9/125мкм кабель для расстояний не более 40 000 м
10GBaseLR	Одномодовый оптоволоконный 9/125мкм кабель для расстояний не более 10 000 м
10GBaseLW	Одномодовый оптоволоконный 9/125 мкм кабель для расстояний не более 10 000 м
10GBaseLX4	Многомодовый оптоволоконный 62,5/125мкм кабель для расстояний не более 300 м
10GBaseSR	Многомодовый оптоволоконный 50/125мкм кабель для расстояний не более 65 м
10GBaseSW	Многомодовый оптоволоконный 62,5/125мкм кабель для расстояний не более 65 м

Беспроводные коммуникации

В качестве альтернативы кабельным системам существует несколько беспроводных технологий передачи сетевых пакетов, при этом используются радиоволны, сигналы инфракрасного диапазона и СВЧ-волны. Во всех перечисленных технологиях сигнал передается по воздуху или через эфир, поэтому они являются удобным решением в тех случаях, когда затруднительно или невозможно применять кабель. Однако это же качество является и недостатком, поскольку передаваемый сигнал подвержен помехам со стороны других сигналов, существующих в данной среде (например, от солнечных пятен, изменений ионосферы и других атмосферных явлений).

В беспроводных технологиях несущий сигнал излучается обычной или параболической антенной ("тарелкой"). Излучаемая мощность и усиление регламентируются коммуникационными законами конкретной страны. Например, в США нелицензированная связь на частоте 2,4 ГГц ограничена коэффициентом усиления антенны, равным 6 dB (дБ на дюйм), и излучаемой мощностью в 1 Ватт. Лицензированные операторы (например, любительские станции пакетного радио) могут использовать и большую мощность, в зависимости от лицензии на широкополосную связь и занимаемую частоту. Конкретные частоты, выделенные для беспроводных коммуникаций, также регламентируются национальными и международными соглашениями и конвенциями по связи.

В беспроводных системах необходимо определить количество узлов, передающих широкополосный сигнал, для чего анализируется наличие излучаемого сигнала в антенне. Например, одним из простейших методов определения конфликтов Ethernet является фиксация минимально допустимого уровня принимаемого радиосигнала в антенне. Если минимальный порог превышен, то предполагается наличие конфликта. Другим способом распознавания конфликтов является применение в передаваемых фреймах сигналов RTS (Request To Send – готовность к передаче), CIS (Clear To Send готовность к приему) и АСК (Acknowledgement – уведомление). Эти сигналы координируют передачу данных в каждом узле беспроводной системы. Подробно беспроводные сети рассматриваются в *главе 9.*

, Я

Типы интерфейсов данных

Данные в сетях передаются в виде пакетов или ячеек. Сначала использовалась передача пакетов, которая до сих пор остается наиболее распространенным методом передачи данных в локальных

сетях. Передача ячеек (пакетов фиксированной длины) позволяет строить высокоскоростные каналы между локальными и глобальными сетями. Для каждого метода передачи необходимы специальные интерфейсы, управляющие сетевыми коммуникациями на физическом уровне. В следующих разделах описываются и сравниваются используемые в сетях пакеты и ячейки, а также предназначение
для них интерфейсы.

Передача пакетов

Как рассказывалось в *главе 1,* данные передаются от узла к узлу в виде больших фрагментов, называемых пакетами или фреймами. Коммуникационное программное обеспечение каждого узла разбивает данные на такие фрагменты. В зависимости от передающей среды, фрагмент данных преобразуется в электрический, радио- или световой сигнал, который и может быть передан между узлами. Требуется много пакетов данных, чтобы передать страницу текста или файл.

Формат пакетов определяется используемым в сети протоколом. Например, протокол определяет способ указания адреса узла, посылающего пакет, адреса принимающего узла, типа передаваемых данных, размера пакета, объёма передаваемых данных и метода обнаружения поврежденных пакетов или коммуникационных ошибок. Другой важной частью пакета является синхронизирующая информация для передачи множества пакетов, позволяющая отсылать пакеты через заданные интервалы времени. На рис. 3.8 показан общий формат пакета.

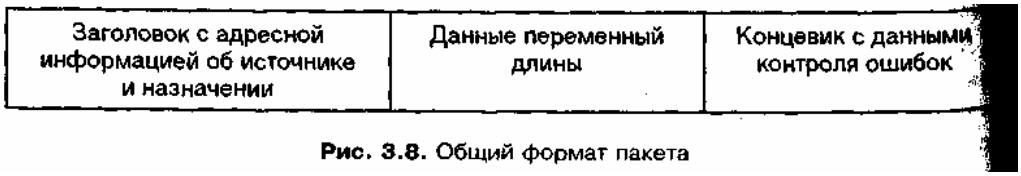


Рис. 3.8. Общий формат пакета

Для физической передачи пакетов в сеть служит карта сетевого интерфейса, или *сетевой адаптер* (network interface card, NIC). Сетевой адаптер позволяет подключить рабочую станцию, файл-сервер, принтер или другое устройство к сетевой передающей среде, например, к коаксиальному кабелю или витой паре. На одном конце адаптера располагается разъем (или коннектор), соответствующий типу сетевой среды.

Сетевой адаптер является приемопередатчиком, обеспечивающим канал передачи данных в сетевой среде. Его встроенные средства упаковывают во фрейм заголовок, исходный и целевой адреса, данные и хвостовик, а фрейм в виде законченного пакета передается в коммуникационную среду. Сетевой адаптер имеет алгоритмы для приема, распаковки, передачи и синхронизации данных, а также для управления конфликтами и ошибками. Программные алгоритмы, реализующие эти функции, хранятся в исполняемых и служебных файлах, называемых сетевыми *драйверами.* Для каждого сетевого адаптера необходимы определенные сетевые драйверы, соответствующие методу доступа к сети, формату инкапсуляции данных, типу кабельной системы и физической (MAC) адресации. В программных драйверах реализуются стандарты многоуровневых сетевых коммуникаций, заданные эталонной моделью OSI. Драйверы позволяют сетевому адаптеру выполнять передачу данных на Физическом (Уровень 1) и Канальном (Уровень 2) уровнях. Дополнительная информация о сетевых адаптерах содержится в следующей главе.

Передача ячеек

Обычно *ячейка* (cell) содержит фрагмент данных фиксированной длины в формате, пригодном для передачи с большими скоростями – от 155 Мбит/с до 1 Гбит/с и выше. Как показано на рис. 3.9, ячейка имеет заголовок (header), в котором содержится следующая информация:

- данные для управления потоком, координирующие передачу информации между исходным и целевым узлами;
- информация о маршруте и канале, позволяющая передавать данные по кратчайшему маршруту;
- признак, указывающий на то, содержит ли ячейка реальные данные или управляющую информацию для осуществления высокоскоростного соединения;

- сведения об ошибках.

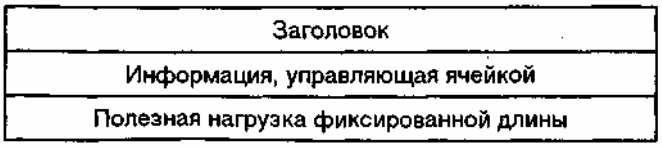


Рис. 3.9. Общий формат ячейки

Имеющая фиксированную длину полезная нагрузка ячейки отличается реальных данных, содержащихся в пакете. В зависимости от протокола, Л кеты содержат данные переменной длины, которая кратна байту (8 битам) Например, данные в пакете распространенного стандарта Ethernet моЯ иметь длину от нескольких сот до нескольких тысяч бит.

При асинхронном режиме передачи (asynchronous transfer mode, ATM) данные в ячейке всегда имеют длину 384 бита. Технология ATM (подробно описываемая в главе 8) представляет собой метод передачи данных, в котором ячейки и множество каналов используются для пересылки речевых сигналов, видео и данных в локальных и глобальных сетях. Фиксированная длина позволяет более точно синхронизировать передачу данных и обеспечить высокие скорости коммуникаций и качество обслуживания (Quality of Serve QoS). Качество обслуживания количественно описывает качество передачи данных, пропускную способность и надежность сетевой системы. Некоторые производители и телекоммуникационные компании предлагают Я своих систем или оборудования гарантированное качество обслуживания.

В первую очередь ячейки используются в сетях ATM, поэтому интерфейсы данных состоят из коммутаторов ATM, интерфейсов подключаемых устройств (AUI) и оптоволоконного кабеля. Сети ATM – это сложная тема и подробно она обсуждается в главе 8. Кроме этого, в главе 4 рассказывается о коммутаторах ATM. В состав AUI-интерфейса входят приемопередатчик и сетевые драйверы, построенные по тем же принципам, что и драйверы Я сетевых адаптеров, однако ориентированные на соединения по коаксиальному кабелю, витой паре или оптоволокну (см. практическое задание 3-8).

Согласно спецификациям ATM Forum и TIA Fiber Division, LAN Section, для передачи ячеек в магистралях локальных сетей, работающих на скорости 622 Мбит/с и на расстояниях до 500 м, требуется одномодовый оптоволоконный кабель. Многомодовый кабель с полосой пропускания 500 МГц на 1 км является наиболее выгодным решением для резервных магистралей, обеспечивающих скорость до 100 Мбит/с на расстоянии до 2000 м. Следовательно, наилучшая конструкция кабельной системы, удовлетворяющаяся современным и будущим требованиям к резервным магистралям, представляет собой комбинацию многомодовых (62,5/125 FDDI Grade) и одномодомовых оптических кабелей. Такие решения можно рассматривать как пример комбинированной кабельной системы.

Обычно кабельная магистраль содержит от 18 до 48 многомодовых оптических кабелей. При добавлении от 6 до 12 одномодовых кабелей (имеющих чрезвычайно высокие показатели полосы пропускания) можно обеспечить совместимость с будущими высокоскоростными приложениями. Свободные (или темные) оптические кабели можно оставить не разведенными до тех пор, пока в них не появится необходимость. В большинстве проектов затраты на установку избыточных кабелей невелики по сравнению с общими
расходами на монтаж и намного меньше, чем затраты на установку дополнительных кабелей в будущем.

Совет

Настоятельно рекомендуется устанавливать большее количество многомодовых и одномодовых оптоволоконных кабелей, чем это требуется при существующих требованиях к проекту.

Методы передачи сигналов в глобальных сетях

Для пересылки данных в глобальных сетях используется несколько методов передачи сигналов (типов коммуникационной среды). В данном разделе лишь кратко описаны методы передачи физических сигналов, принятые в различных глобальных технологиях; более подробно реальные технологии, включая форматирование фреймов, будут рассмотрены в последующих главах.

Чаще всего в глобальных сетях используются следующие методы передачи сигналов:

- двухточечные соединения;
- Т-линии;
- SONET;
- ISDN.

Ниже каждый из перечисленных методов описывается подробнее.

Двухточечные соединения

Самым распространенным способом передачи данных в глобальных сетях являются *двухточечные соединения* по общедоступным коммутируемым телефонным линиям или выделенным каналам. Например, простейшая глобальная сеть образуется всякий раз, когда выполняется межмодемное соединение по телефонной линии. Модем на отвечающей стороне может быть подключен к сети или к компьютеру, находящемуся на большом удалении (до нескольких тысяч километров). Физическая коммуникационная среда представляет собой аналоговую цепь, проходящую через телефонные станции и обеспечивающую соединение только на время сеанса связи.

Другим видом двухточечных соединений является связь по выделенным телефонным линиям (например, по специализированным цифровым Т-линиям), которые могут использоваться только между двумя точками (к примеру, между головным офисом компании и ее подразделением). В этом случае при установлении сеанса связи не нужно каждый раз набирать номер и искать коммутируемую цепь. Иногда в выделенных линиях используется подавление шума, и в целом они обеспечивают более надежную связь, чем коммутируемые линии. В зависимости от типа выбранной службы выделенных каналов, линия может поддерживать аналоговые или цифровые коммуникации.

Т-линии

Т-линии были описаны в *главе 2* как метод передачи данных в глобальных сетях, который обычно существует между телекоммуникационными компаниями (хотя собственные Т-линии могут быть и в крупных корпорациях). Базовые службы Т-линий часто имеют названия в виде Т-х или DS-х, где х означает уровень передаваемого сигнала. Эти названия взаимозаменяемы, однако между ними существует и различие. Название DS-х относится к Физическому уровню модели OSI, на котором определяются электрические параметры сигнала (например, его тип и напряжение в вольтах). Название Т-х относится к Канальному уровню, на котором решаются задачи выбора протокола и способов форматирования данных.

В Т-линиях, применяемых для построения глобальных сетей, используется цифровая передача данных, для которой обычно выбирается сигнал из группы каналов, предоставляемых телекоммуникационной компанией. Существуют пять типов сигналов группы каналов: с D-l no D-4 и Digital Carrier Trunk (транк, цифровая коммуникационная магистраль). Сигнал D-1 был первым типом сигналов для коммуникаций по Т-линиям. В нем для передачи информации используются семь разрядов, а один дополнительный разряд служит для управления и синхронизации. Отдельная группа каналов D-1 имеет 72 канала.

Сигналы D-2 разработаны для повышения производительности и уменьшения издержек сигналов D-1. В сигналах D-2 все восемь разрядов используются для передачи информации, и в каждом шестом фрейме, посылаемом по Т-линии, присутствуют команды управления и синхронизации. Благодаря этим усовершенствованиям, группа каналов D-2 имеет 96 каналов.

Развитие интегральных микросхем привело к увеличению емкости каналов канальных группах, в результате чего группы D-3 и D-4 имеют по 1,44 канала. Кроме того, в этих группах улучшены способы передачи фреймов по Т-линиям. Начиная с группы D-2, коммуникационные компании начали разработку так называемых суперфреймов (superframe) и смогли упаковать несколько 193-разрядных фреймов в один большой фрейм. Технология суперфреймов, состоящих из двенадцати 193-разрядных фреймов, получила распространение в канальных группах D-4.

Цифровая коммуникационная магистраль (Digital Carrier Trunk, DCT) – это новейший тип канальных групп, позволяющий уменьшить стоимость услуг, благодаря снижению затрат на оборудование и эксплуатацию. В некоторых DCT-магистралях используется новейшая методика форматирования фреймов, называемая расширенным суперфреймом (extended superframe, ESF). В ESF-фрейме используются 24 фрейма, а не 12 (как в группах D-4), и в нем применяется более развитый контроль ошибок. Благодаря имеющимся в ESF-фрейме возможностям управления ошибками и диагностики, коммуникационные компании могут быстрее устранять неисправности и тем самым уменьшить время

простоя.

Для передачи информации в Т-линиях используется один из двух методов коммутации: множественный доступ с временным разделением, или уплотнением (time division multiple access, TDMA), и комбинация TOMA со статистическим множественным доступом (см. главу 2). Такая комбинация представляет собой быструю технологию коммутации пакетов, позволяющую службам Т-линий учитывать различные приоритеты доступа к каналу, возникающие при передаче речевых сигналов, видео и данных. Физическое устройство, используемое для коммутации, называется мультиплексором. Это устройство принимает множество входных сигналов от нескольких источников и передает их в одну (чаще всего) или несколько совместно используемых высокоскоростных передающих сред. Оно просто переключает каналы, обеспечивая передачу принимаемой информации на нужный канал.

Для управления физическими сигналами в Т-линиях используется различное оборудование. Некоторые компании для связи с пользователями применяют системы цифрового доступа и коммутации (Digital Access Cross-connect System, DACS). Эти системы предоставляют несколько режимов работы. Во-первых – базовый канал DS-1 (или Т-1), во-вторых – для клиентов, которым не нужны целиком услуги Т-1, они предоставляют комбинированный или частичный канал DS-0. Частичный канал представляет собой комбинацию 64-Кбит/с каналов. В-третьих, системы DACS предоставляют отдельные каналы DS-0. Кроме DACS, для непосредственного предоставления клиентам всех услуг Т-линий коммуникационные компании используют канальные группы D-4 и DCT.

Многие клиенты подключаются к Т-линиям при помощи комбинации устройства обслуживания канала (channel service unit, CSU) и устройства обработки данных (data service unit, DSU). CSU – это физический интерфейс, связанный с Т-линией, как показано на рис. 3.10. DSU работает подобно Цифровому модему, преобразующему сигнал, принимаемый устройством обслуживания канала, в такой сигнал, который можно передавать в сеть к Рабочим станциям и серверам. Кроме этого, DSLJ получает сетевой сигнал и преобразует его в сигнал DS- , передаваемый через CSU в Т-линию. Оба Устройства обычно реализуются в виде одного автономного блока или могут быть объединены на одной плате в сетевом маршрутизаторе, концентраторе Или коммутаторе. Устройства CSU/DSU обеспечивают форматирование Фреймов Т-линий D-4 и ESF и должны поддерживать форматирование фреймов используемое системами цифрового доступа и коммутации (DACS) или группами каналов обслуживающей коммуникационной компании. Если клиент использует частичные службы Т-линий, то в его местоположении устанавливаются устройства CSU/DSU частичной Т-линии.

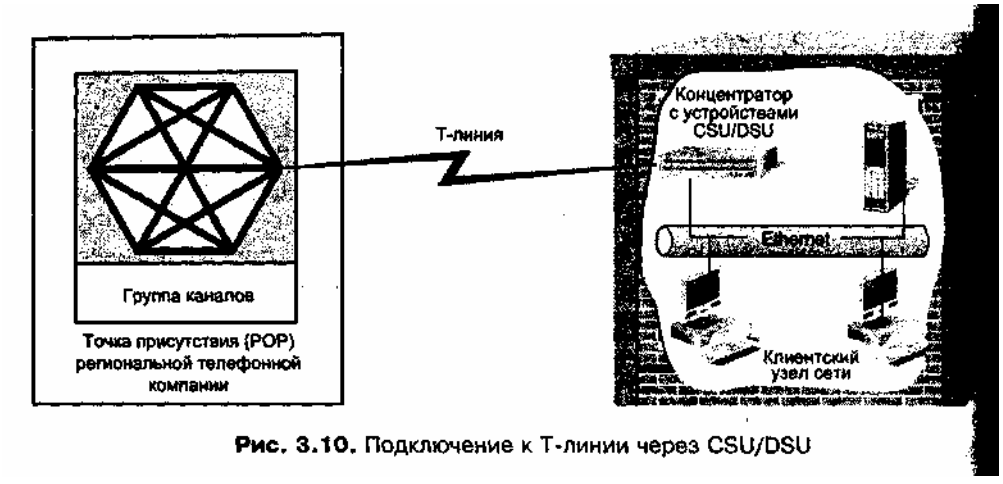


Рис. 3.10. Подключение к Т-линии через CSU/DSU

SONET

Synchronous Optical Network (SONET) (синхронная оптическая сеть) представляет собой высокоскоростную технологию глобальных коммуникаций, в торой используются одномодовый и многомодовый оптоволоконный кабель коммуникационные каналы, основанные на службах Т-3. Подробнее сети SONET описываются в *главе 7.* Базовый Т-3 уровень SONET называется Synchronous Transport Signal Level 1 (STS-1). Уровень STS-1 можно модернизировать до более высоких уровней, которые получаются путем добавления линий Т-3. Как показано на рис. 3.11, фрейм SONET STS-1 состоит из 810 октетов, представленных в виде матрицы из девяти рядов по 90 октетов Служебные данные ячейки занимают

первые три октета в каждом ряду, а оставшиеся 783 октета составляют синхронный конверт полезной нагрузки (synchronous pay10ad enve10pe, SPE). Ячейки передаются поочередно каждые 125 микросекунд, ряд за рядом, начиная с верхнего.

SONET преобразует электрические сигналы STS-x в световой сигнал, называемый оптической несущей (optical carrier, OC). Фреймы STS-1 можно преобразовывать и передавать одновременно пачками, при этом используется механизм, чередующий фреймы и позволяющий достичь более высоких скоростей для уровней STS-x и OC-x. Эти скорости, допустимые в сетях SONET, перечислены в табл. 3.13.

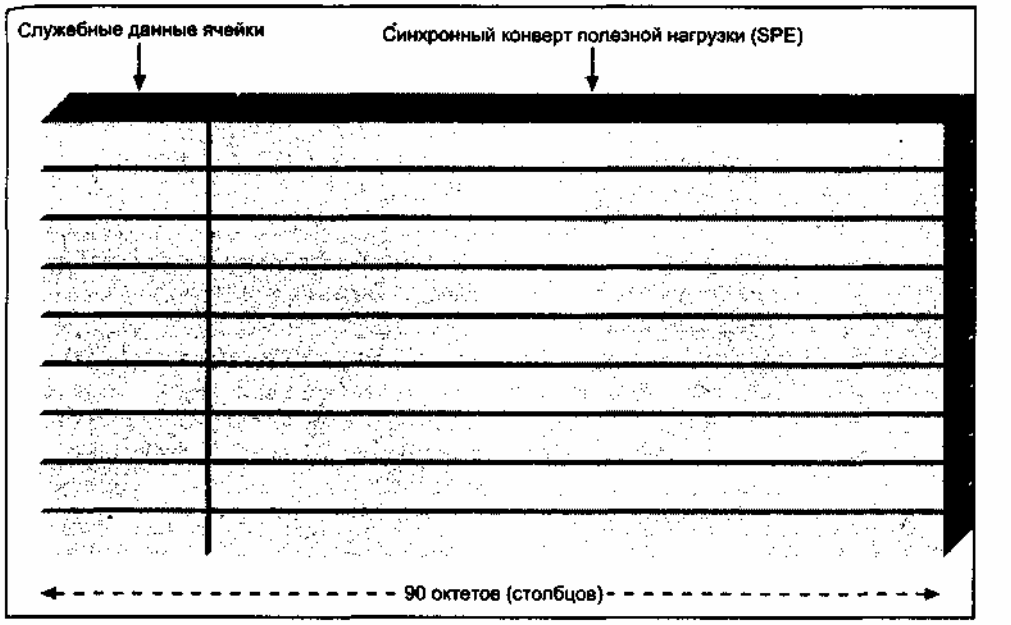


Рис. 3.11. Фрейм SONET STS-1

Таблица 3.13. *Скорости передачи данных уровней STS-x и OC-x в сетях SONET*

Уровень STS	**Уровень OC**	**Скорость передачи**	**Число линий T-3**
STS-1	OC-1	51,84 Мбит/с	1
STS-3	OC-3	155,52 Мбит/с	3
STS-9	OC-9	466,56 Мбит/с	9
STS-12 .	OC-12	622,08 Мбит/с	12
STS-18	OC- 18	933,12 Мбит/с	18
STS-24	OC-24	1,244 Гбит/с	24
STS-36	OC-36	1,866Гбит/с .	36
STS-48	OC-48	2,488 Гбит/с	48
STS-192	OC-192	9,95 Гбит/с	192

ISDN

Integrated Services Digital Network (ISDN) (Цифровая сеть связи с комплексными услугами) – это технология глобальных сетей, предназначенная для предоставления услуг передачи речевых сигналов, данных и видео по телефонным линиям. (Подробнее сети ISDN рассматриваются в *главе* 7.) В сетях ISDN применяются цифровые методы, что позволяет передавать информацию быстрее и надежнее, чем это возможно по линиям обычной телефонной сети. Физически линия ISDN представляет собой традиционную линию или линию T-1 (на основе витой пары или оптоволокна), однако при этом в помещениях коммуникационной компании и клиента устанавливается специальное оборудование ISDN.

Для передачи цифровых сигналов в сети применяются два метода. Первый метод – *уплотнение с временной компрессией* (time-compression multiplexing TCM). В этом случае 16- или 24-разрядные блоки

данных посылаются с некоторой регулярностью в виде цифровых пакетов. Между пакетами имеются периоды молчания, необходимые для адаптации линии перед передачей следующего пакета. Таким образом, первый пакет отсылается в одном направлении, после чего следует пауза. Затем пересылается пакет в обратном направлении. Скорость передачи пакетов в каждом направлении равна 288 Кбит/с. Из-за переключения направления общая скорость передачи данных уменьшается до 144 Кбит/с. Передачей пакетов данных управляет центральное синхронизирующее устройство.

Второй метод передачи сигналов – *эхоподавление* (echo cancellation). В даном случае данные передаются в обоих направлениях одновременно. Для связи передатчика и приемника с клиентской линией используется специальное устройство, называемое дифференциальной системой (hybrid). Часто при одновременной двунаправленной пересылке данных возникает отражение (или эхо) переданного сигнала. Эхосигналы в линии могут по мощности в три раза превосходить полезные сигналы, в результате чего данные невозможно выделить. Для подавления отраженных сигналов в сетях ISDN применяется эхокомпенсатор (echo canceler), который определяет амплитуду эхосигналов и вычитает ее из входящих сигналов. Поскольку мощность эхосигналов варьируется, в эхокомпенсаторе используется схема обратной связи, непрерывно измеряющая их амплитуду.

Резюме

- На первых этапах развития компьютерных систем производители могли практически без ограничений выпускать оборудование, работающее только с их собственными системами. При покупке устройств от разных поставщиков зачастую возникали проблемы совместимости. В конце концов, были образованы организации по стандартам, что позволило интегрировать оборудование различных производителей. Эти организации сыграли ключевую роль в развитии сетей и сетевых устройств, т. к. для надежной передачи данных требуется совместимость оборудования. Во многом именно благодаря наличию стандартов стало возможным повсеместное объединение сетей, вне зависимости от того, аппаратные средства каких фирм использовалось для их построения. Основную роль в развитии сетей сыграли следующие национальные и международные организации: ANSI, IEEE, ITU, ISO, ISOC, IETF и EIA/TIA.

- Средства передачи физических сигналов в локальных и глобальных сетях можно классифицировать по трем категориям: по типу коммуникационной среды, по типу интерфейса и по типу канала передачи данных в глобальной сети. В качестве коммуникационной среды используются самые разнообразные кабельные системы, а также беспроводные каналы. В настоящее время в локальных сетях для подключения настольных систем чаще всего применяется витая пара. Оптоволоконный кабель используется для организации локальных сетей и для их объединения в глобальную сеть. Развитие оптоволоконных кабелей делает также возможным их применение в качестве альтернативного варианта горизонтальной проводки в локальных сетях для подключения настольных систем (когда требуется высокая скорость соединения).

- П Различные спецификации и способы использования коммуникационных кабелей могут несколько осложнить их выбор. В табл. 3.14 содержится краткий перечень характеристик разных типов кабелей, что позволяет одним взглядом охватить их основные свойства.

Таблица 3.14. *Обзор типов кабелей и их характеристик*

Тип кабеля	Коаксиал	Витая пара	Оптоволокно	Комбинированный
Спецификации	10Base5 10Base2	10BaseT 100BaseT 100BaseTX 100BaseT2 100BaseT4 100BaseVG/100VG-AnyLAN 1000BaseCX 1000BaseTX	10BaseF 100BaseFX 1000BaseLX 1000BaseSX 10GBaseER 10GBaseEW 10GBaseLR 10GBaseLW 10GBaseLX4 10GBaseSR 10GBaseSW	Отсутствуют

Тип кабеля	Коаксиал	Витая пара	Оптоволокно	Комбиниро-ванный
Физичес-кая топология	Шина	Звезда Кольцо	Звезда Кольцо	Шина Звезда Кольцо
Скорость	10Мбит/с	10Мбит/с 100Мбит/с 1000Мбит/с	От 10Мбит/с до нескольких Гбит/с	10Мбит и выше в зависимости от структуры и сетевых приложений
Эксплуатационная гибкость	Средняя	Высокая	Низкая	От высокой до низой
Возможности модернизации (создание высокоскоростных сетей и объединение в глобальную сеть)	Ограниченные (однако некоторые типы допускают широкополосную передачу данных)	Высокие в зависимости от используемого типа; в особенности если применяется кабель категории 5 и выше	Предназначается для высокоскоростных коммуникаций и глобальных сетей	Предназначаете для высокоскоростных коммуникаций и глобальных сетей

- Высокоскоростные технологии на основе витой пары и оптоволокна: Fast Ethernet, Gigabit Ethernet и 10 Gigabit Ethernet. Fast Ethernet обеспечивает скорость в 100 Мбит/с при использовании стандарта 802.3u или 802,12. Чаще применяется стандарт 802.3и, использующий метод доступа CSMA/CD. Стандарт 802.12 предусматривает приоритетный доступ по запросу. Еще большие скорости передачи данных обеспечивает технология Gigabit Ethernet, что особенно важно для построения сетевых магистралей. Эта технология использует CSMA/CD. Новейшая Ethernet-технология – 10 Gigabit Ethernet – продвигается как альтернатива распространенным решениям в локальных и глобальных сетях, что обусловлено очень высокой скоростью передачи информации. В отличие от обычных сетей Ethernet, сетей 802.3u Fast Ethernet и Gigabit Ethernet, технология 10 Gigabit Ethernet не использует CSMA/CD в качестве метода доступа к передающей среде.

- Беспроводные технологии являются приемлемым решением в тех случаях, когда физически невозможно или экономически невыгодно создавать сеть на основе коммуникационного кабеля. На коротких расстояниях используются радиоволны и волны инфракрасного диапазона, а для связи на большие расстояния применяются СВЧ и спутниковые каналы.

- Передача пакетов и ячеек используется во многих типах сетей. Обычно передача ячеек применяется для высокоскоростных решений, а передача пакетов – для сетей с меньшей пропускной способностью. Для реализации обоих типов интерфейса данных требуются приемопередатчики, соответствующие кабельные сопряжения и сетевые драйверы. Однако каждый тип интерфейса имеет свои стандарты и реализует свои принципы работы.

Простейшим каналом глобальной сети является модемное соединение, по коммутируемой телефонной линии. Более сложные и скоростные каналы – SONET, ISDN и T-линии. SONET – это признанное высокоскоростное решение для глобальных сетей, предлагаемое несколькими телекоммуникационными компаниями. ISDN и T-линии являются надежными решениями среднего масштаба, которые предлагаются повсеместно многими операторами связи

Сетевое передающее оборудование

По прочтении этой главы и после выполнения практических заданий вы сможете:

- описать назначение оборудования локальных сетей, включая сетевые адаптеры, повторители, модули множественного доступа (MAU), концентраторы, мосты, маршрутизаторы, мосты-маршрутизаторы, коммутаторы и шлюзы;
- объяснить принципы работы оборудования локальных сетей;
- описать назначение оборудования глобальных сетей, включая мультиплексоры, группы каналов, частные телефонные сети, различные типы модемов, адаптеры ISDN, серверы доступа и маршрутизаторы;
- объяснить принципы работы оборудования глобальных сетей.
- Сети – это не просто коммуникационные кабели, электромагнитные волны и интерфейсы. Сети представляют собой функциональную структуру, включающую в себя широкий ассортимент сетевого передающего оборудования. Без такого оборудования локальные сети могли бы связывать лишь пары компьютеров, а глобальные сети практически не могли бы существовать. Сетевые приемопередающие устройства обычно скрыты от постороннего глаза в монтажных комнатах или машинных залах; однако они играют решающую роль при выполнении сетевых операций (например, при пересылке адресату сообщения электронной почты, доступе к важной базе данных, находящейся в Удаленном месте, успешной передаче файла в другую страну).

Одно сетевое оборудование усиливает передаваемый сигнал, позволяя ему достигнуть других помещений или знаний. Другое оборудование маршрутизирует, направляет сигнал из одной сети в другую в масштабах предприятия или глобальной сети. Третий тип оборудования преобразует данные, позволяя передавать их между сетями различного типа. В этой главе описывается сетевое передающее оборудование, применяемое в локальных и глобальных сетях. Некоторые типы оборудования, например, мосты, шлюзы, канальные группы и серверы доступа будут новыми для вас.

Примечание

Беспроводные технологии стремительно завоевывают компьютерную индустрии включая сетевое передающее оборудование. В этой главе вы бегло познаком тесь с тем, как они реализуются в сетевых адаптерах и мостах. Подробнее безпроводные технологии и их влияние будут рассматриваться в *главе 9.* |

Передающее оборудование 1 локальных сетей I

Коммуникационное оборудование локальных сетей предназначено для связи устройств в единую сеть, для создания и объединения множества сетей или подсетей, а также для развертывания сети предприятия (кампуса). Используемое в локальных сетях оборудование может применяться как для подключения отдельного узла, так и для связи множества узлов. В его состав входят следующие устройства:

- сетевые адаптеры;
- повторители;
- модули множественного доступа;
- концентраторы;
- мосты;

- маршрутизаторы;
- мосты-маршрутизаторы;
- коммутаторы;
- шлюзы.

Далее каждый тип устройств рассматривается подробно.

Сетевые адаптеры

Как вы узнали из предыдущей главы, сетевой адаптер служит для подключения к сети некоторого сетевого устройства, например, компьютера или другого сетевого оборудования. Конструкция сетевых адаптеров ориентирована на конкретные методы передачи сетевого сигнала, тип компьютерной шины и сетевую передающую среду. Для реализации сетевого соединения нужны четыре компонента:

1. коннектор, соответствующий сетевой передающей среде;
2. трансивер;
3. контроллер, поддерживающий подуровень MAC канального уровня OSI *(см. главу 2);*
4. микропрограммное обеспечение для управления протоколом.

Коннекторы и обрамляющие цепи разрабатываются для конкретного типа коммуникационной среды (например, для коаксиала, витой пары, оптоволокна или беспроводных технологий). Некоторые сетевые платы, подобные показанной на рис. 4.1, изготавливаются с несколькими разъемами, и поэтому могут использоваться с различными типами среды.

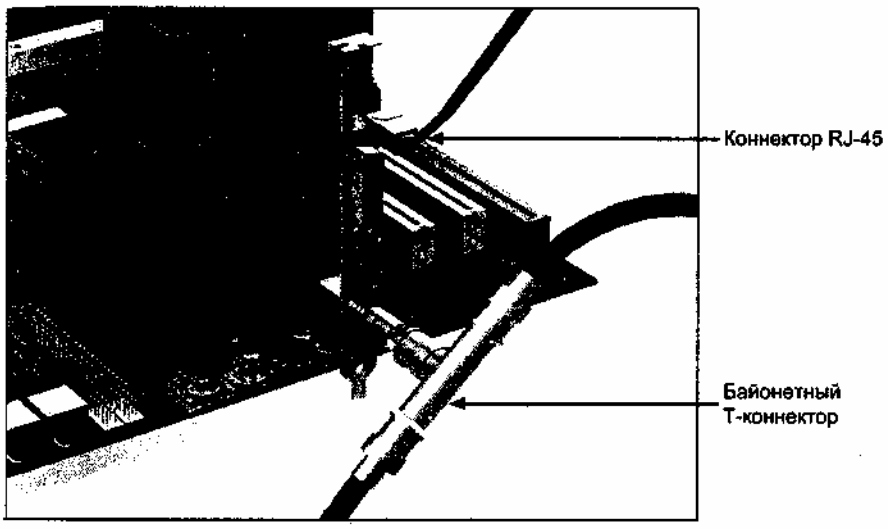


Рис. 4.1. Комбинированный сетевой адаптер

Комбинированные адаптеры чаще всего делаются с выходами под коаксиал и витую пару. Такие адаптеры поставляются с программными драйверами или программно-аппаратными средствами (firmware), соответствующими типам передающей среды. *Программно-аппаратные (микропрограммные) средства* представляют собой программы, хранящиеся в микросхеме, например, в постоянной памяти (ПЗУ). Кроме того, некоторые драйверы могут распознавать тип среды, подключенной к сетевому адаптеру, и соответствующий Драйвер устанавливается автоматически. В некоторых операционных системах, например, в Windows 2000 и Windows XP, драйверы аппаратных средств, включая сетевые, могут быть подписанными. *Подписанный драйвер* содержит некоторую цифровую подпись, которая гарантирует, что данный драйвер проверялся на совместимость с операционной системой, что устанавливаемый драйвер не заменит более свежую версию и что данный драйвер не содержит ошибок или вирусов. В практическом задании 4-1 будет рассказано о том, как определить, подписан ли драйвер сетевого адаптера в системах Windows 2000 и Windows XP Professional.

Примечание

Комбинированный адаптер может поддерживать две среды передачи сигнала более, однако для его правильной работы необходимо, чтобы в конкретный момент времени была подключена только одна среда.

Кабельный разъем подключается к трансиверу (приемопередатчику), который может быть или внешним, или встроенным в сетевой адаптер. *Трансивер* (transceiver) – это устройство, обеспечивающее передачу и прием сигналов по коммуникационному кабелю. В компьютерах, серверах и сетевом оборудовании трансивер чаще всего встраивается в плату интерфейса. В некоторых случаях, обычно в старом сетевом оборудовании, трансивер является внешним по отношению к адаптеру, и для его подключения к адаптеру применяется ответвительный кабель.

Совет

Ответвительный кабель для трансивера нужен только в том случае, когда трансивер является внешним по отношению к сетевому адаптеру. Он не должен использоваться, если трансивер встроен в плату адаптера.

Назначение блока контроллера MAC

Общая задача блока контроллера MAC и программно-аппаратных средств – правильно упаковать адреса источника и назначения (физические адреса передающего и принимающего сетевых адаптеров), передаваемые данные и контрольную сумму *(см. разд. "Эталонная модель взаимодействия открытых систем OSI" главы 2)*. Контроллер MAC работает на подуровне MAC Канального уровня OSI и форматирует фреймы. Кроме этого, блок контроллера функционирует на подуровне LLC того же уровня и выполняет следующие задачи:

- инициирует коммуникационный канал между двумя узлами;
- П обеспечивает целостность канала и надежную передачу данных;
- следит за тем, чтобы сетевые адаптеры на обоих коммуникационных узлах выдерживали паузу, равную 9,6 мкс между приемом одного фрейма и передачей последующего, для того чтобы у обоих адаптеров был небольшой запас времени на правильное переключение между режимами приёма и передачи.

Блок контроллера MAC и программно-аппаратные средства настроены на конкретную сетевую технологию, например:

- Ethernet;
- Fast Ethernet;
- Gigabit Ethernet;
- 10 Gigabit Ethernet;
- Token Ring;
- Fast Token Ring;
- FDDI;
- ATM.

Режимы передачи сигналов

Некоторые сетевые адаптеры могут работать с несколькими технологиями, в частности с Ethernet и Fast Ethernet, что позволяет легко модернизировать сеть для перехода на высокоскоростную передачу данных. Кроме того, многие адаптеры могут работать как в полудуплексном, так и в полнодуплексном режиме. *Полудуплексный* (half-duplex) режим работы не позволяет сетевому адаптеру и сетевому оборудованию передавать и принимать данные одновременно. *Полнодуплексный* (full-duplex), или просто *дуплексный* режим предусматривает возможность одновременной передачи и приема, что возможно благодаря буферизации данных в сетевом адаптере. С этой целью адаптер снабжается памятью для временного хранения информации, не обрабатываемой в данный момент.

Совет

Перед тем как конфигурировать в адаптере полудуплексный или дуплексный режим, определите настройки коммуникационного устройства, к которому адаптер подключен. Например, если компьютер с адаптером подключен к порту коммутатора и этот порт настроен на полудуплексную

работу, то сетевой адаптер необходимо настроить на этот же режим. Если режимы работы адаптера и коммуникационного устройства не согласованы, то они не смогут общаться друг с другом.

Сетевые адаптеры FDDI и ATM

Сетевые адаптеры FDDI и ATM выпускаются в различных модификациях, это зависит от того, какое оборудование они подключают к сети. Обычно с помощью адаптеров FDDI узлы и файловые серверы подключаются к сетевому оборудованию FDDI с использованием одного соединения (единичное подключение), а сетевое оборудование подключается к кабельной системе FDDI с применением двух соединений (двойное подключение). Сетевые адаптеры ATM чаще всего используются для подключения к ATM-сети Коммутаторов ATM или серверов. Кроме того, технология ATM доступна и Для настольных систем, что стимулирует разработку сетевых адаптеров ATM Для рабочих станций; однако такие адаптеры сравнительно дорогие.

Беспроводные сетевые адаптеры

Беспроводной адаптер обеспечивает передачу данных в одном из двух режимов. Один режим представляет собой выделенное, равноправное (peer-to-peer) взаимодействие с другим беспроводным адаптером. Другой

Режим – это взаимодействие с точкой (местом) доступа (access point), например, с беспроводным мостом (о них будет рассказано далее в этой главе). Если вы работаете с беспроводной точкой доступа, то нецелесообразно также использовать выделенные беспроводные коммуникации, поскольку они не будут работать стабильно в присутствии точки доступа.

Выпускаемые беспроводные адаптеры, совместимые со стандартом 802.11b, обычно рассчитаны на скорости 1, 2, 10 и 11 Мбит/с. Некоторые производители или также выпускают беспроводные адаптеры, совместимые со стандартом 802.11a. На и передающие данные со скоростью до 54 Мбит/с. Беспроводные адаптеры не всегда работают на максимально возможной скорости, они, «договариваются» о скорости, наиболее подходящей для текущих условий, и при этом учитывается загрузка равноправных компьютеров или точки доступа.

Совет

Быстрый сетевой адаптер в компьютере или сетевом устройстве будет загружен полностью, если только в компьютере установлен быстрый процессор (например, высококлассный Pentium, Itanium или RISC-процессор), который сможет обеспечить требуемую производительность адаптера.

Сетевые адаптеры и шины

Сетевые адаптеры должны соответствовать типу шины, используемой в компьютере. *Шина* – это компьютерная магистраль, по которой информация передается к процессору и периферийным устройствам, подключенным к компьютеру. Ниже перечислены основные типы шин в рабочих станциях и серверах:

- ✓ *Industry Standard Architecture (ISA)* – устаревшая конструкция шины расширения, поддерживающая передачу 8- и 16-разрядных данных со скоростью 8 Мбайт/с;
- ✓ *Extended Industry Standard Architecture (EISA* – более новая конструкция шины на основе ISA, способная передавать 32-разрядные данные. EISA позволяет использовать управление шиной (bus mastering) – процесс, уменьшающий нагрузку на центральный процессор при выполнении ввода/вывода;
- ✓ *Microchannel Architecture (MCA)* – конструкция 32-разрядной шины, использующаяся в устаревших компьютерах IBM;
- ✓ *Peripheral Computer Interface (PCI)* – современная конструкция шины обеспечивающая передачу 32- и 64-разрядных данных. В PCI используется идея локальной шины, позволяющая применять разные шины для сетевых интерфейсов и для дисковых накопителей;
- ✓ *SPARC Bus (SBUS)* – специализированная шина, предназначенная для рабочих станций SPARC компании Sun Microsystems;
- ✓ *NuBus* – специализированная шина с 96-контактным разъемом, используемая в

компьютерах компании Apple (от Macintosh II до Macintosh Performa);

- ✓ *Universal Serial Bus (USB)* – стандарт шины, позволяющей подключать устройства любого типа (например, клавиатуры, фотокамеры, указательные устройства, телефоны и ленточные накопители) к одному шинному порту компьютера;
- ✓ *локальная шина VESA (VL-bus)* – шина, использующаяся в некоторых 80486-компьютерах для пересылки 32-разрядных данных между сетевым адаптером и центральным процессором. Эта шина не используется на Pentium-совместимых компьютерах, где она замещена шиной PCI.

Выбор сетевого адаптера

Каждый сетевой адаптер определяющим образом влияет на эффективность сетевых коммуникаций. При покупке адаптера необходимо учитывать перечисленные ниже вопросы.

- Для чего используется сетевой адаптер – для хост-компьютера, сервера или рабочей станции? Адаптеры хост-компьютеров и серверов зачастую применяются для подключения к сети на скорости 100 Мбит/с и выше с целью увеличения общей производительности. Для этих типов адаптеров требуется быстрая системная шина (например, PCI). Требование высокой производительности для сетевых адаптеров рабочих станций определяется теми приложениями, которые на них выполняются.
- Какая сетевая среда и какой метод доступа к сети используются? Для каждой среды и метода доступа нужны свои сетевые адаптеры (например, для сетей с маркерным кольцом, Ethernet, Fast Ethernet и т. д.).
- Кто выпускает данную модель адаптера? Приобретайте только высококачественные сетевые адаптеры известных производителей и пользуйтесь самыми скоростными слотами расширения для адаптеров (например, слотами PCI).
- Какой тип шины используется в компьютере или сетевом оборудовании? Проверьте, подходит ли сетевой адаптер к имеющимся слотам расширения шины.
- Какая операционная система установлена на компьютере? Для любого сетевого адаптера необходим драйвер, совместимый с имеющейся системой (например, с Windows 2000, Windows XP и т. д.).
- Какой режим передачи данных используется в сети – полудуплексными или дуплексный? Сетевые адаптеры должны работать в обоих режимах это обеспечивает возможность изменения или модернизации сети.
- Если адаптер предназначен для специфических случаев (например, для FDDI), то как он подключается к сети? Адаптеры FDDI могут использовать как единичное, так и двойное подключение. Кроме того, в некоторых случаях применяются адаптеры, не имеющие встроенного трансивера; в этом случае трансивер должен приобретаться отдельно.

Один из лучших способов предотвращения сетевых проблем – приобретать высокопроизводительные сетевые адаптеры для всех станций, подключенных к сети. Также важно покупать адаптеры у тех производителей, которые регулярно обновляют драйверы адаптера, устраняющие возможные проблемы и повышающие производительность. Многие изготовители сетевых адаптеров имеют веб-сайты, с которых можно бесплатно скачать новейшие версии драйверов. (В практическом задании 4-2 вы потренируетесь в получении драйвера сетевого адаптера с веб-сайта какого-нибудь поставщика.)

Совет

Одним из узких мест в сети является сетевой адаптер сервера, который может быть медленным и требовать обновления (например, замены адаптера с шиной EISA на PCI-адаптер). Другим узким местом может оказаться сервер с быстрым сетевым адаптером, но с относительно "слабым" процессором. В обоих случаях пользователям будет казаться, что сеть работает медленно, хотя истинная проблема заключается в недостаточно мощном сетевом адаптере или процессами сервера. В практическом задании 4-3 рассказывается о том, как определить скорость сетевого адаптера и соответствующего сетевого соединения.

Повторители

'

Повторитель (репитер, repeater) соединяет два или несколько кабельных сегментов и ретранслирует любой входящий сигнал на все другие сегменты. *Сегмент* кабеля – это один отрезок кабеля, удовлетворяющий спецификациям IEEE, (например, отрезок кабеля 10Base2 длиной 185 м, к которому подключено не более 30 узлов, включая терминаторы и сетевое оборудование). Повторители представляют собой недорогое решение, реализующей передачу данных на Физическом уровне OSI (поскольку они работают с физическим сигналом) и позволяющее соединять пользователей, находящихся в удаленных концах здания – на расстояниях, не отвечающих требованиями IEEE на длину отдельного кабельного сегмента. Повторитель может выполнять следующие функции Физического уровня:

- фильтровать искажения сигнала или шум, вызванный радио или электромагнитными помехами;
- усиливать входящий сигнал и восстанавливать его форму для более точной передачи;
- синхронизировать сигнал (в сетях Ethernet);
- воспроизводить сигнал на всех кабельных сегментах.

Синхронизация позволяет избегать конфликтов сигналов в сети Ethernet, когда сигнал передается в кабель. Повторители позволяют выполнить следующие задачи:

- удлинить кабельную систему (например, на расстояние более 185 м для сегмента 10Base2 и свыше 500 м – для 10Base5);
- увеличить количество подключенных узлов и обойти ограничения, налагаемые на отдельный сегмент (например, подключить свыше 30 узлов в сети Ethernet);
- распознать сетевую ошибку и отключить сегмент кабеля;
- подключиться к компонентам в других сетевых устройствах, таких как концентраторы и коммутаторы, а также усилить и синхронизировать сигналы;
- соединить сегменты, работающие с разной передающей средой (например, подключить сегмент 10BaseT к сегменту 10Base2 или сегмент 10Base2 к сегменту 10Base5);
- удлинить сегменты магистрального кабеля в локальных и глобальных сетях;
- удлинить сегменты оптоволоконного кабеля;
- увеличить рабочее расстояние для Т-линий.

Если повторитель ретранслирует сигнал в два и более кабельных сегмента, он называется многопортовым повторителем. Например, повторитель может иметь порты для 2–8 дополнительных сегментов. Кабель, отходящий от некоторого порта, рассматривается как нормальный кабельный сегмент. То есть многопортовый повторитель сети 10Base2 ^может передавать сигнал в несколько кабелей длиной 185 м. Каждый кабель может иметь до 29 подключенных узлов, включая терминаторы на своих концах. На рис. 4.2 показана сеть старого образца, в которой сегменты 10Base2 подключены через повторитель к магистрали 10Base5.

Примечание

Необходимо иметь представление о сетях старой конструкции, поскольку многие из них по-прежнему находятся в работе и вполне возможно, что вам придется отвечать за их функционирование или же искать пути их модернизации.

Согласно спецификациям IEEE, можно использовать четыре повторителя, Чтобы увеличить длину толстого коаксиального кабеля до 2500 м, а длину Тонкого коаксиала – до 1000 м. В зависимости от топологии сети и используемой передающей среды, отдельный пакет данных может проходиться более чем через четыре повторителя. Если между двумя узлами расположен четыре повторителя, то, по меньшей мере, два связующих сегмента не должны иметь подключенных компьютеров.

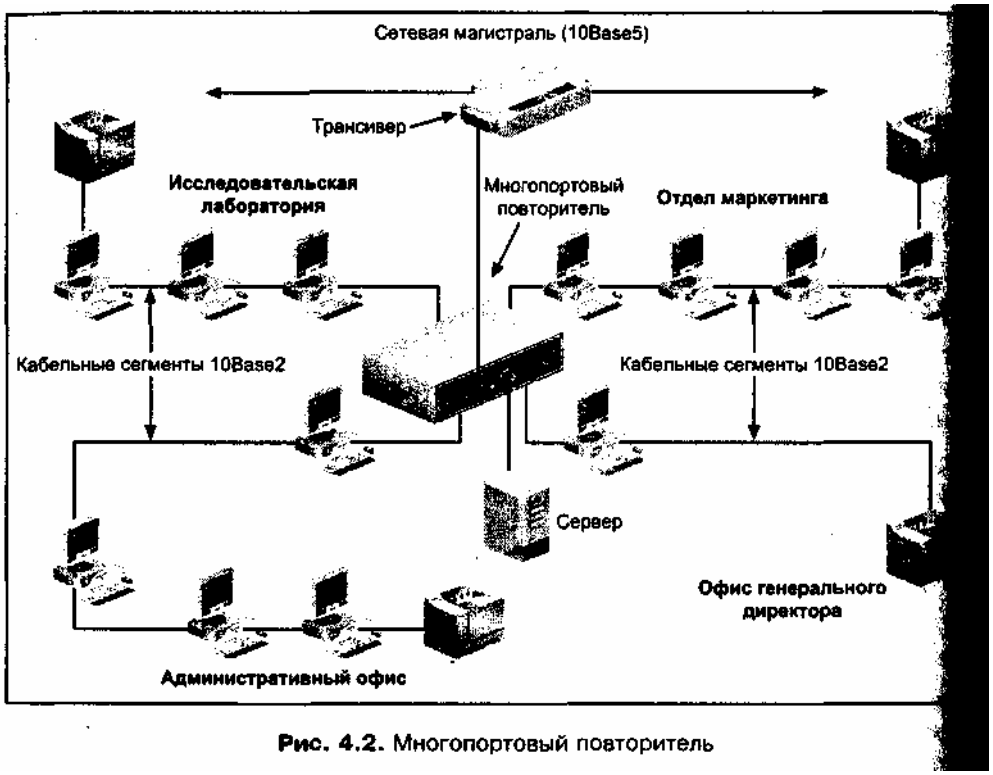


Рис. 4.2. Многопортовый повторитель

Примечание

Повторители применяются как в локальных и региональных сетях, так и глобальных сетях. Например, глобальную сеть на основе линии T-1 можно удлинять, помещая повторители через каждые 2,2 км.

В спецификациях IEEE 802.3u для Fast Ethernet описаны два типа повторителей: Класс 1 (Class I) и Класс 2 (Class II). Повторители Класса 1 работают медленнее, чем повторители Класса 2, и, следовательно, только один повторитель Класса 1 можно использовать в одной области коллизий (когда сегменты кабеля, отходящие от повторителей, имеют максимальную длиной 100 м). Таким образом, между двумя любыми конечными узлами можно поместить только один повторитель Класса 1. В этом случае *область коллизий* (collision domain) будет состоять из двух сегментов, соединенных одним или несколькими повторителями.
В сети с повторителями Класса 2 в области коллизий могут использоваться несколько повторителей, однако при этом между любыми двумя конечными узлами не должно быть включено более двух повторителей Класса 2. Когда в сеть стандарта IEEE 802.3u включаются два повторителя, максимальная длина кабеля между ними равна 5 м, а каждый повторитель может обслуживать кабельные соединения длиной до 100 м (что дает общую длину, равную 205 м).

Примечание

Хотя повторители Класса 1 и медленнее, чем повторители Класса 2, они важны при соединении различных передающих сред (например, при подключении кабельного сегмента 100BaseT4 к сегменту 100BaseTX). В этом случае повторитель Класса 1 успевает передавать пакеты между сегментами.

У многих повторителей имеются порты, предназначенные для различных типов входящих кабельных подключений (например, для толстого и для тонкого кабеля Ethernet). Многие повторители также имеют порт AUI для подключения к коаксиальной или оптоволоконной магистрали при использовании соответствующего трансивера. Выходные порты обычно рассчитаны на тонкий коаксиальный кабель, однако имеются и другие варианты.

Ниже перечислены некоторые пары кабельных сегментов, связываемых при помощи повторителя:

- толстый коаксиал и толстый коаксиал;
- тонкий коаксиал и тонкий коаксиал;
- толстый коаксиал и тонкий коаксиал;
- толстый коаксиал и оптоволокно;

- тонкий коаксиал и оптоволокно;
- витая пара и оптоволокно;
- толстый коаксиал и витая пара;
- тонкий коаксиал и витая пара;
- оптоволокно и оптоволокно.

Повторители непрерывно следят за исправностью каждого выходного кабельного сегмента (например, за ошибками передачи сигналов, вызванными отсутствием терминатора или повреждением кабеля). В случае ошибки повторитель перестает передавать данные в неисправный сегмент. Такой способ отключения сегмента называется *изолированием,* или *секционированием* (partitioning). Например, некоторый сегмент может быть изолирован, если на нем отсутствует терминатор или если неисправен сетевой адаптер какой-нибудь рабочей станции, и он создает избыточный сетевой трафик. Когда сегмент изолирован, ни один узел этого сегмента не может пересылать данные. Как только сетевая проблема устраняется, повторитель способен заново инициализировать сегмент и возобновить передачу информации. С изолированием сегмента вы познакомитесь в практическом задании 4-5. 1

Простые повторители являются недорогим решением для расширения устаревшей шинной топологии сетей на основе коаксиальных кабелей. Однако при развитии сети повторители, в конце концов, станут препятствием на пути создания высокоскоростной сети и могут быть узкими местами сетевой топологии. При разработке новой сети с самого начала используйте саке современное оборудование, имеющее встроенные возможности повторите (например, централизованные коммутаторы *(см. разд. "Коммутаторы")).*

Примечание

При использовании многопортового повторителя проектируйте сеть так, чтобы на одном сегменте располагалось минимальное количество узлов. Например, для сети с 40 рабочими станциями создайте четыре сегмента по 10 станции каждом (а не два сегмента с 12 и 28 узлами), в этом случае изолирование ней некоторого сегмента затронет минимальное число компьютеров.

Одним из достоинств повторителей является то, что они представляют собой недорогой способ расширения сети. Недостаток заключается в том, что они могут создать дополнительный трафик в загруженной сети, поскольку ретранслируют входящий сигнал во все исходящие сегменты. Большая часть этого трафика бесполезна, т. к. нет смысла передавать данные в те сегменты, в которых отсутствует целевой узел.

'

Совет

Некоторые коммутаторы и концентраторы (рассматриваемые далее в главе) фактически работают как повторители, поскольку они усиливают, синхронизируют и ретранслируют информационные сигналы. Перед тем как подключи подобные устройства к сети, просмотрите документацию и определите, Они дают ли порты свойствами повторителей. Если эти функции имеются, то уточните, к какому классу повторителей (Класс 1 или Класс 2) относятся данные порты. Принимайте во внимание полученную информацию, т. к. стандарты, определяющие характеристики повторителей, распространяются и на другие устройства, выполняющие аналогичные функции.

Модули множественного доступа Я

Модуль множественного доступа (multistation access unit, MAU) выполни функции центрального концентратора в сети с маркерным кольцом. Также встречается термин *интеллектуальный модуль множественного доступа* (smart multistation access unit, SMAU), если модуль обладает возможностью находить неисправности в соединениях с рабочими станциями и изолировать неисправные станции от всей сети. Модули MAU используются исключительно в сетях с маркерным кольцом, где они могут выполнять следующие функции:

- соединять рабочие станции в логическое кольцо в рамках физической звездообразной топологии;
- передавать по кольцу маркер и фреймы;

- усиливать информационные сигналы;
- соединяться в последовательные цепочки для расширения маркерного кольца;
- обеспечивать правильное перемещение данных;
- отключать порты, связанные с неисправными узлами.

Примечание

Аббревиатура MAU используется для двух не имеющих друг к другу отношения сетевых устройств: для описанного в *главе 3* модуля подключения к среде передачи данных (media access unit) и для рассматриваемого в *данной главе* модуля множественного доступа. Если вы помните, модуль подключения к среде передачи – это трансивер, применяемый для соединения с коммуникационной средой (например, с коаксиальным или оптоволоконным кабелем). Модуль множественного доступа – это концентратор, связывающий станции в сети с маркерным кольцом. Для его обозначения иногда используется аббревиатура MSAU.

Все сетевые устройства подключаются к маркерному кольцу через модуль MAU, при этом обычно используется витая пара типа 1, 2 (экранированная) или 3 (неэкранированная) (см. табл. 3.4). Модуль MAU передает фреймы от одного узла к другому, реализуя физическую топологию звезды, однако логически фреймы перемещаются так, будто они находятся в кольце. Модуль MAU выполняет функции центрального концентратора и работает на Физическом и Канальном уровнях OSI.

Простейший модуль MAU соединяет до восьми кабельных сегментов. Новейшие модули имеют 16 портов для подключения узлов. Модуль MAU может выполнять функции пассивного или активного концентратора. *Пассивный концентратор* (passive hub) лишь передает сигнал от станции к станции. Сигнал частично ослабляется при каждом прохождении через модуль MAU, что уменьшает максимальную пропускную способность сети. Например, сеть с пассивными концентраторами и кабелями типа 3 (UTP) реально может объединять не более 72 узлов.

Активный концентратор (active hub) регенерирует, синхронизирует и усиливает сигналы при каждом их перемещении к следующему узлу. В результате Удаленные узлы получают более мощный сигнал, что более чем в два раза. Увеличивает количество поддерживаемых узлов; при этом активный концентратор работает как повторитель. При использовании активных модулей MAU сеть на основе кабеля типа 3 может иметь до 150 узлов, а сеть на основе кабеля типов 1 или 2 может объединять до 260 узлов. Максимальное количество узлов при использовании кабеля типа 3 меньше, чем при использовании типов 1 и 2. Это объясняется тем, что в кабеле типа 3 значительно выше искажения сигнала, называемые "дрожанием", jitter.) и у любого модуля MAU имеются порт входа – Ring In (RI) и порт выхода Ring Out (RO), что отображено на рис. 4.3. Эти порты позволяют последовательно соединять модули MAU между собой (в виде цепочки). Кабели, используемые для связи модулей MALI, называются *соединительными* (pat|H cable), а кабели, соединяющие узел с модулем MAU, – *абонентскими* (lobe cable). Соединения между портами RI и RO обеспечивают расширение маркерного кольца, позволяя подключать к сети дополнительные рабочие станции. При использовании нескольких модулей MAU порт RI первого модуля подключается к порту RI второго модуля и так далее до тех пор, пока все модули не будут соединены.

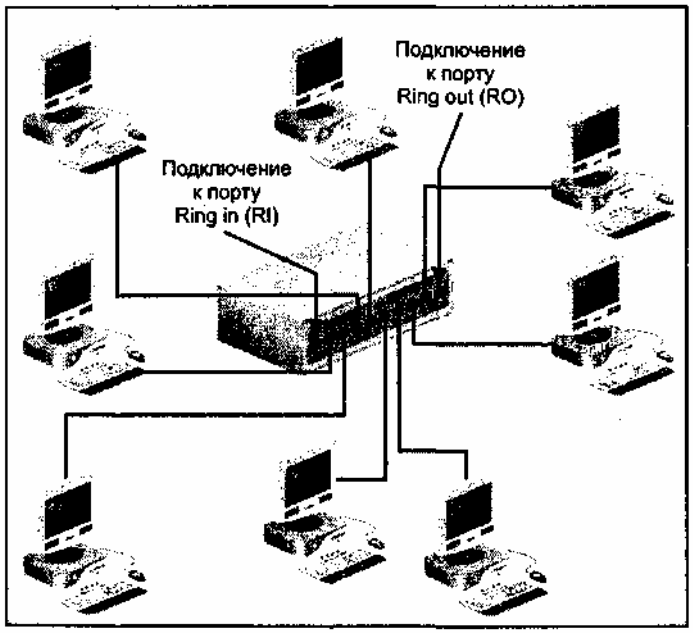


Рис. 4.3. Модуль MAU, соединяющий рабочие станции в сети с маркерным кольцом

Компания IBM – основной поставщик и идеолог технологии маркерных колец – рассматривает спецификации IEEE 802.5 в качестве стандартов для двух типов сетей. Первый тип – небольшое перемещаемое (movable) маркерное кольцо (на основе гибкого кабеля типа 6, имеющего ограниченную длину), второй тип – большое фиксированное (поп movable) маркерное кольцо (на основе кабеля типов 1 и 2, поддерживающего связь на большие расстояния). В табл. 4.1 перечислены спецификации для модулей MAU, работающих в маркерном кольце, при этом указаны отличия для перемещаемых малых и фиксированных больших сетей.

Таблица 4.1. *Спецификации на модули MAU сетей с маркерным кольцом*

Спецификация	**Диапазон значений**
Максимальное количество станций	96 для малой сети 260 для большой сети
Максимальное количество модулей MAU	1 2 для малой сети 33 для большой сети
Минимальная длина соединительного кабеля между модулями MAU	2,5 м
Максимальная длина соединительного кабеля между модулями MAU	STP: 200 м DTP: 45,5 м Оптоволокно: 1 км
Максимальная длина абонентского кабеля (между модулем MAU и подключенной станцией)	STP: 100 м DTP: 45,5 м Оптоволокно: 1 00 м

Усовершенствование технологии модулей MAU позволило создать новые типы устройств, например, блок управления доступом (Controlled Access Unit, CAU), который позволяет несколько соединенных между собой наращиваемых блоков рассматривать как единый модуль MAU сети с маркерным кольцом. Блоки CAU также имеют возможность сбора информации, необходимой для управления производительностью сети.

Совет

Одной из наиболее распространенных причин неисправности маркерного кольца или возникновения состояния "испускания маяка" (beaconing) является подключение узла на неправильной скорости (например, когда узел имеет скорость передачи, равную 4 Мбит/с, а остальная сеть работает на скорости 16 Мбит/с). Приобретайте модули SMAU, позволяющие автоматически отключать такие узлы и сохранять работоспособность сети. Другим достоинством моделей SMAU является то, что они меняют маршрут сетевого трафика в случае

неисправности соединительных кабелей, подключенных к порту RI или RO.

Концентраторы

Концентратор (hub) представляет собой центральное сетевое устройство, к которому в звездообразной топологии подключаются сетевые узлы (например, рабочие станции и серверы). Несколько входов и выходов концентратора могут быть активными одновременно. Концентраторы выполняют следующие функции:

- являются центральным устройством, через которое соединяется множество узлов сети;
- позволяют большое количество компьютеров соединять в одну или несколько локальных сетей;
- обеспечивают связь различных протоколов (например, преобразование протокола Ethernet в протокол FDDI и обратно);
- соединяют вместе сегменты сетевой магистрали;
- обеспечивают соединение между различными типами передающей среды
- позволяют централизовать сетевое управление и структуру.

Существуют различные типы сетевых концентраторов. Простейшие из них представляют собой единую точку подключения к сети, позволяющую физически реализовать в виде звезды логическую шинную сеть Ethernet или маркерное кольцо. Такие концентраторы называются неуправляемыми и предназначены они для очень маленьких сетей, содержащих до 12 узлов (иногда немного больше). Как следует из названия, неуправляемые концентраторы не поддерживают программ или протоколов, обеспечивающая функции управления сетью или собирающих информацию для этих целей. Такие концентраторы могут быть активными и пассивными, хотя активный концентраторы используются чаще всего. Оба типа концентраторов работают на Физическом уровне модели OSI. Активный концентратор выполняет функции многопортового повторителя, поскольку он регенерирует, синхронизирует и усиливает передаваемые сигналы.

Некоторые концентраторы позволяют работать на двух скоростях (напри мер, со скоростью 10 Мбит/с или 100 Мбит/с). Обычно порты таких концентраторов могут автоматически распознавать скорость, на которой работают подключенные к ним устройства. Кроме того, для повышения эффективности работы сети некоторые подобные концентраторы могут размещав в разные области коллизий порты, работающие с различными скоростями.

Концентраторы, непосредственно подключенные к рабочим станциям, часто называют концентраторами рабочей группы, поскольку они собирают подключенных пользователей в сетевую рабочую группу. Такие концентраторы могут соединяться с другими сетевыми устройствами (например, с коммутаторами или маршрутизаторами).

Некоторые концентраторы (в т. ч. концентраторы рабочей группы) являются наращиваемыми (этажерочного типа), что позволяет располагать их один на другой. В зависимости от конфигурации концентраторы обычно имеют 8, 12 или 24 порта. Отличительной особенностью наращиваемых концентраторов является то, что можно непосредственно подключить один к другому до восьми концентраторов, и при этом они рассматриваются как единый повторитель (рис. 4.4). Количество повторителей важно для реализации сети, поскольку для нормального функционирования сети оно должно отвечать требованиям стандартов Ethernet или маркерного кольца. Кроме того, наращиваемые концентраторы являются недорогим решением для расширения сети, для чего достаточно подключить новый концентратор к уже установленному.

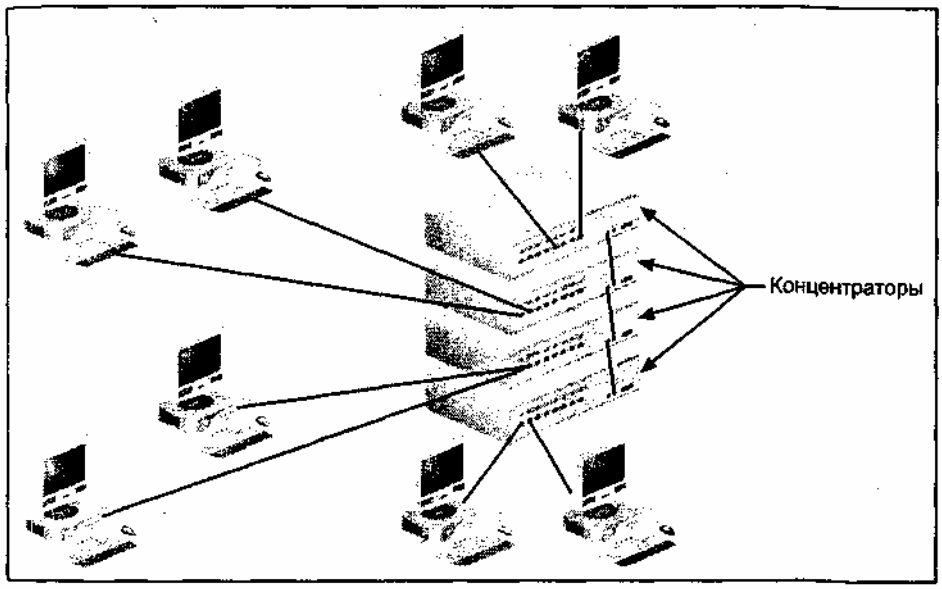


Рис. 4.4. Наращиваемые концентраторы

Стоечные концентраторы представляют собой модульные устройства, имеющие объединительную заднюю панель, в которую можно вставлять модули различных типов. Некоторые концентраторы поставляются с резервными объединительными панелями и источниками питания, а также имеют вентиляторы для охлаждения. Существуют модели, позволяющие заменять неисправные модули без выключения всей стойки. На объединительной панели концентратора установлены разъемы для подключения модулей, предназначенных для работы с различными типами сегментов (например, с Ethernet, Fast Ethernet, FDDI и ATM). Некоторые модели концентраторов поддерживают модули, выполняющие функции мостов, маршрутизаторов или коммутаторов. Активные стоечные концентраторы могут иметь модуль синхронизации, используемый в сочетании с усилителем сигналов. В практическом задании 4-4 вы будете сравнивать неуправляемые, наращиваемые и стоечные концентраторы.

Концентраторы могут также иметь функции коммутатора, при этом данные ретранслируются только в тот сегмент, в котором располагается целевой узел. Такие концентраторы работают на подуровне MAC (Уровень 2), что позволяет им читать адрес назначения каждого фрейма.

Многие концентраторы обладают некоторым "интеллектом", т. е. имеют программное обеспечение, позволяющее использовать эти устройства для управления сетью. Такое программное обеспечение поставляется вместе с концентратором и обычно может обновляться с целью добавления новых функций по мере изменения требований к сети. Программы могут собирать информацию о производительности сети, которую "видит" концентратор. С помощью этой информации администратор сети может с удаленной станции выключить отдельный порт или весь концентратор. Интеллектуальные (управляемые) концентраторы работают как на Физическом уровне (поскольку он непосредственно управляет передаваемым сигналом), так и на Канальном уровне (т. к. он считывает информацию из фреймов данных).

Примечание

Интеллектуальные концентраторы поддерживают протокол Канального уровня Simple Network Management Protocol (SNMP), который позволяет сетевым устройствам собирать данные о производительности сети. Подробнее этот протокол рассматривается в *главе 6.* я

Интеллектуальные, наращиваемые и стоечные концентраторы вместе с концентраторами рабочей группы могут использоваться для реализации общей стратегии унификации местоположения сетевого оборудования и управления сетью в контрольных точках. Такой подход позволит администратору сети определять данные о производительности практически в любой точке сети. При этом в случае необходимости сеть легко модернизировать и повысить ее эффективность. Если, например, в некотором крыле здания нужно установить новый сегмент Ethernet, то для этого достаточно добавить плату в стойку концентратора либо подключить один или несколько наращиваемых концентраторов.

Концентраторы поддерживают следующие технологии локальных сетей:

- Ethernet;
- Fast Ethernet;
- Gigabit Ethernet;
- 10 Gigabit Ethernet;
- FDDI;
- Token Ring;
- Fast Token Ring.

Подобно повторителям, концентраторы могут изолировать сегменты сети, в которых возникли проблемы. У большинства концентраторов имеются светодиодные индикаторы, которые загораются, если сегмент изолирован (блокирован). Обычно также имеется кнопка или тумблер, который следует нажать после устранения неисправности с целью инициализации сегмента и восстановления его рабочего состояния. Перед тем как нажать кнопку сброса, нужно узнать, как она влияет на работу пользователей в исправных сегментах, поскольку в некоторых простых концентраторах инициализируются все сегменты, вне зависимости от того, были они изолированы или нет. В практическом задании 4-5 вы познакомитесь ближе с изолированием сегментов.

> **Совет**
>
> В сетях Ethernet на витой паре концентраторы, являющиеся сердцевиной звездообразной топологии, используемой в таких сетях, по сути, являются многопортовыми повторителями. При установке концентраторов необходимо узнать из спецификаций конкретной модели, нужно ли считать порты концентратора повторителями, поскольку структура сети должна отвечать требованиям на количество повторителей в сети. Например, если вы используете наращиваемые концентраторы 100BaseTX, определите количество состыкованных друг с другом концентраторов, которые будут считаться одним повторителем, и узнайте к какому классу повторителей они относятся – к Классу 1 или к Классу 2.

Мосты

Мост (bridge) – это сетевое устройство, соединяющее между собой сегменты локальной сети. Мосты позволяют решать следующие задачи:

- расширить локальную сеть в случае, когда достигнут лимит на максимальное количество соединений (например, если сегмент Ethernet имеет 30 узлов);
- расширить локальную сеть и обойти ограничения на длину сегментов (например, если нужно нарастить сегмент Ethernet на тонком кабеле, который уже имеет длину 185 м);
- сегментировать локальную сеть для ликвидации узких мест в сетевом трафике;
- предотвратить неавторизованный доступ к сети.

Мосты весьма распространены в сетях Ethernet II/IEEE 802.3, хотя устройства, выполняющие только функции мостов, быстро были заменены устройствами, обладающими функциями и мостов, и маршрутизаторов. Поскольку Работа мостов незаметна для пользователей, то широко используется термин прозрачный мост. Мосты функционируют в так называемом *беспорядочном Режиме* (promiscuous mode), что подразумевает просмотр физического целевого адреса каждого фрейма перед его пересылкой. Этим мосты отличаются от повторителей, которые не имеют возможности анализа адресов фреймов.

Мосты работают на подуровне MAC Канального уровня OSI, поскольку они считывают исходный и целевой физические адреса фрейма. Мост перехватывает весь сетевой трафик и анализирует целевой адрес каждого фрейма определяя, следует ли пересылать данный фрейм в следующую сеть. В процессе своей работы мост просматривает MAC-адреса передаваемых через него фреймов и строит таблицу известных целевых адресов. Если мост знает, что фрейм предназначен для узла, который находится в том же сегменте что и отправитель фрейма, он отбрасывает сегмент, поскольку тот не нуждается в дальнейшей пересылке. Если мост знает, что целевой адрес располагается в другом сегменте, он транслирует фрейм только в нужный сегмент. Если мосту не известен целевой сегмент, он передает фрейм во все сегменты, за исключением исходного сегмента, и этот процесс называется *лавинной маршрутизацией* (адресацией) (flooding). Главным достоинством мостов является то, что они сосредотачивают трафик в конкретных сетевых сегментах. Мост может выполнять фильтрацию и

пересылку с довольно высокой скоростью, поскольку он просматривает информацию только на Канальном уровне и игнорирует информацию на более высоких уровнях. 1

Примечание

Если мост не подключен к *источнику бесперебойного питания (ИБП)* (имеющему резервные батареи) или не имеет встроенного ИБП, то при пропаже напряжения информация в таблицах адресов будет потеряна.

Мосты "прозрачны" для любого протокола или комбинации протоколов, поскольку от них не зависят. Мосты просматривают только MAC-адреса. Один мост может транслировать в одной и той же сети различные протоколы, такие как TCP/IP, IPX, NetBEUI, AppleTalk и X.25, безотносительно к тому, какие структуры фреймов передаются через него. На рис. 4.5 изображен мост, работающий с протоколами NetBEUI, IPX и TCP/IP.

Примечание

На рис. 4.5 обратите внимание на наличие компьютера Windows NT Server протокола NetBEUI. Это не случайно: несмотря на то, что многие организации перешли на системы Windows 2000 Server или Windows Server 2003, по-прежнему используется много систем Windows NT Server и часто применяется, протокол NetBEUI, что играет важную роль во всех типах сетей.

Мосты не конвертируют фреймы из формата одного протокола в формат другого, исключение составляют только транслирующие мосты *(см. главу 1)*. Транслирующие мосты преобразуют фреймы, относящиеся к одному методу доступа и передающей среде, во фреймы другого стандарта (например, из стандарта Ethernet в стандарт Token Ring) и наоборот. Такие мосты переформатируют адреса, например, отбрасывая адресную информацию стандарта Token Ring, которая не используется стандартом Ethernet. Далее перечислены базовые элементы, которые транслирующие мосты преобразуют во фреймах Token Ring и Ethernet:

- очередность битов в адресах;
- формат MAC-адреса;
- элементы маршрутной информации;
- функции, имеющиеся во фреймах Token Ring, не имеющие эквивалентов во фреймах Ethernet;
- зондирующие (explorer) пакеты Token Ring, которые не используются в сетях Ethernet.

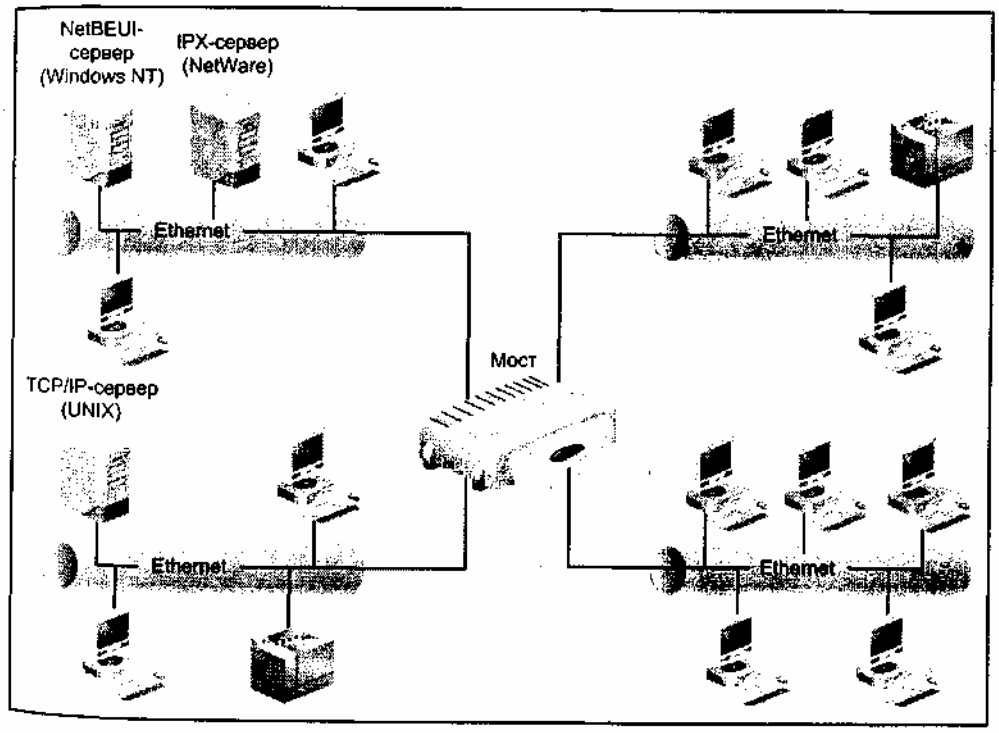


Рис. 4.5. Сеть с мостом

Мосты выполняют три важных функции – анализ, фильтрация и пересылка. После включения мост анализирует топологию сети и адреса устройств во всех подключенных сетях. Для этого мост просматривает исходный и целевой адреса во всех передаваемых ему фреймах и на основе этой информации строит свою таблицу, содержащую адреса всех узлов сети. Большинство мостов может хранить в таких таблицах значительное количество адресов. Затем таблица адресов используется для принятия решений о пересылки трафика.

Администратор сети может также ввести инструкции для моста, запрещающие лавинообразно передавать фреймы от определенных исходных адресов или же позволяющие отбрасывать некоторые фреймы без ретрансляции. Такая возможность фильтрации позволяет применять мосты для повышения безопасности (например, путем ограничения доступа к серверу, хранящему важную информацию).

Некоторые мосты могут связывать только два сетевых сегмента. Такие мосты используются для каскадирования (каскадного соединения) сегментов. Например, как показано на рис. 4.6, мост А соединяет локальные сети 1 и 2 а мост Б соединяет сети 2 и 3. Фрейм из сети 1 передается в сеть 3 через оба моста – А и Б. В

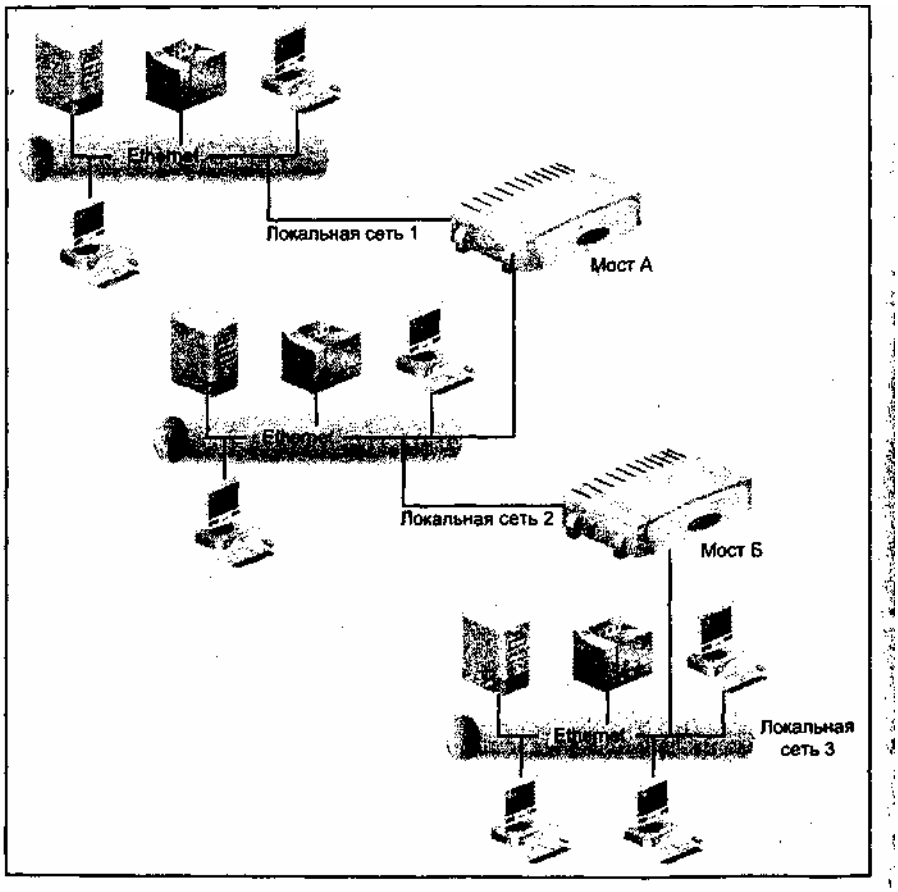


Рис. 4.6. Использование мостов для каскадирования сегментов сети

Существуют также многопортовые мосты, которые могут соединять несколько сетевых сегментов. Некоторые производители предлагают такие мосты, имеющие до 52 портов или интерфейсов. Если бы в предыдущем примере мост А был многопортовым, то имел бы три порта для связи сетей 1, 2 и 3. фрейм из любой сети проходил бы только через один мост и достигал бы целевого узла; таблица адресов моста содержала бы адреса всех узлов каждой сети.

Мосты могут заметно повысить производительность сети, поскольку они сегментируют сетевой трафик, изолируя его внутри сегмента от активности других сегментов. Этим мосты принципиально отличаются от повторителей и концентраторов, которые передают все фреймы во все подключенные сегменты. Другим достоинством мостов является то, что они могут использоваться как брандмауэры (сетевые экраны), запрещая посторонним доступ к сети. *Брандмауэрами* (firewall) называются программные или аппаратные средства, запрещающие доступ к данным из-за пределов сети, а также препятствующие пересылке информации из сети во внешние узлы.

Существуют два типа мостов: локальные и удаленные. *Локальный мост* (local bridge) используется

для непосредственного соединения двух близко расположенных локальных сетей (например, двух сетей Ethernet). Он также применяется для сегментации сетевого трафика с целью ликвидации узких мест. Локальный мост может связать два подразделения одной компании, позволяя всем пользователям обращаться к некоторым файлам и электронной почте. Пусть в одном (головном) подразделении сетевой трафик большой, что обусловлено большим количеством отчетов, генерируемых сервером базы данных в клиент-серверной прикладной программе. После того как мост проанализирует трафик, связанный с обращениями к этому серверу, он начнет фильтровать фреймы и не будет ретранслировать их в сеть другого подразделения, где внутренний трафик невелик.

В университетском кампусе мэйнфреймы, графические рабочие станции, бездисковые станции и персональные компьютеры, обращающиеся к файловым серверам, могут использовать одну и ту же сеть. Производительность в такой сети с большим трафиком может оказаться невысокой, если не разделить сеть на отдельные сегменты, ориентируясь на логику обращений к Устройствам и приложениям. С помощью мостов можно изолировать участки сети с высоким трафиком от других, менее нагруженных сегментов сети.

Беспроводные мосты представляют собой точки доступа, которые являются Подклассом локальных мостов и взаимодействуют с компьютерами, снабженными беспроводными сетевыми адаптерами. Беспроводной мост (например, мост 802.11b) может выбирать скорость обмена с каждым беспроводным адаптером и поэтому в зависимости от условий передачи он может одному адаптеру передавать данные со скоростью 11 Мбит/с, а другому – со скоростью 2 Мбит/с.
Беспроводной мост, совместимый со стандартом 802.Ha и работающий на скорости 54 Мбит/с, может обслуживать до 64 клиентов, а 802.11b-совместимый мост может работать на скорости до 11 Мбит/с и обслужить до 256 клиентов. Беспроводные мосты могут соединяться каскадно с другими внутренними или наружными мостами.

Внутренний мост располагается в том же самом здании, а наружный – в здании, находящемся поблизости. Рассмотрим пример применения этих мостов. Сеть одного университета связывалась по кабелю, проходящему по улице, при этом его концы располагались в двух различных зданиях. Несколько раз в неделю кабель оказывался поврежденным, и соединение пропадало, когда высокий мусоровоз проезжал по улице. Проблема была решена путем установки двух внешних мостов, через которые взаимодействовали локальные сети каждого здания.

Удаленные мосты (remote bridge) используются для связи сетей, находящихся на расстоянии. Для уменьшения затрат на эксплуатацию мосты могут быть связаны линией последовательной передачи. Это один из способов соединить сети, расположенные в разных городах или государствах, и объединить их в большую единую сеть. Однако, как вы узнаете чуть позже, для решения этой задачи чаще всего следует использовать маршрутизатор.

Мосты Token Ring с маршрутизацией от источника

Для пересылки пакетов мосты в сетях с маркерным кольцом используют так называемые *исходные маршруты* (source route) или *маршрутизацию от источника* (source-route bridging). Концепция мостов с маршрутизацией от источника была изначально предложена компанией IBM, а затем включена в спецификацию 802.5 на локальные сети с маркерным кольцом. Мосты с маршрутизацией от источника функционируют на сетевом уровне OSI.

При использовании мостов с маршрутизацией от источника передающий (исходный) узел вставляет во все пакеты, передающиеся между локальными сетями, информацию о полном маршруте от источника к целевому узлу. Мосты запоминают и ретранслируют пакеты в соответствии с маршрутом указанным в пакете. *Ш*

Если некоторый узел собирается послать пакет в сеть с мостами, он генерирует зондирующий пакет (explorer packet). Каждый мост, получивший этот пакет, копирует его во все исходящие порты. По мере прохождения зондирующих пакетов по всей сети информация о маршруте добавляется к содержащимся в них данным. Когда целевой узел получает зондирующие пакеты, посланные отправителем, он отвечает ему, используя всю собранную маршрутную информацию. После этого исходный узел должен выбрать некоторый маршрут к целевому узлу.

Путь, выбираемый исходным узлом, определяется тремя факторами: маршрутом, определенным для первого возвращенного пакета, минимальным количеством ретрансляций на пути к целевому узлу, а также путем, который попускает пересылку пакета максимального размера (в сетевых

сегментах, работающих со скоростью 4 Мбит/с, длина пакетов равна 4000 байт, а в сетях, имеющих скорость работы 16 Мбит/с, длина пакетов равна 17 800 байт). После того как путь определен, маршрутная информация помещается в поле RIF (routing information field) пакета 802.5. Наличие в таком пакете маршрутной информации определяется по состоянию индикатора RII (routing information indicator): двоичная единица указывает на присутствие маршрутной информации, а ноль – на ее отсутствие. Сети с маркерным кольцом могут иметь не более семи мостов.

Ретрансляция (hop – "прыжок") – это выполняемая мостом с маршрутизацией от источника или обычным маршрутизатором операция регенерации, усиления и передачи пакета из одной сети в другую. Например, пакет, переданный через три моста с маршрутизацией от источника, насчитывает три ретрансляции. Сведения о ретрансляции могут включаться во фреймы, обрабатываемые мостами с маршрутизацией от источника или маршрутизаторами, для того чтобы определить кратчайший маршрут к некоторому целевому узлу и для распознавания фреймов, которые могут "зациклиться" в сети (т. е. передаваться по замкнутому маршруту). Рассмотрим, к примеру, сеть, в которой для передачи пакетов от узла А к узлу Б существуют два различных маршрута. Один маршрут проходит через два моста с маршрутизацией от источника (две ретрансляции), а второй – через три таких моста (три ретрансляции). Пакет, отправленный от узла А к узлу Б, сначала проходит через мост, подключенный к сегменту сети, в котором располагается узел А. Этот мост определяет – посылать ли пакет по первому маршруту, содержащему еще один мост, или же по второму маршруту (еще через два моста). Пакет посылается по кратчайшему пути, при этом используется маршрут, имеющий только один дополнительный мост между узлами.

Алгоритм связующего дерева

Для реализации мостов и функционирующей на них системы проверок в сетях, имеющих несколько мостов, используется *алгоритм связующего дерева* (spanning tree algorithm). Этот алгоритм описан в стандарте IEEE 802. Id. Он призван решить две задачи. Во-первых, необходимо, чтобы фреймы не зацикливались в сети. Если мосты связывают множество сетевых сегментов, возможна ситуация, когда фреймы начинают передаваться по замкнутым Маршрутам и, следовательно, никогда не достигнут точки назначения. Как Минимум, при этом упадет пропускная способность сети. Большое же количество зациклившихся фреймов может создать слишком большой трафик, Провоцирующий *широковещательный шторм* (broadcast storm). Широковещательный шторм – состояние, когда используется вся пропускная способность сети. Это может быть вызвано чрезмерным количеством запросов на передачу данных от сетевых устройств, что создает эффект полного бездействия сети.

Во-вторых, алгоритм связующего дерева определяет наиболее эффективный маршрут для передачи фреймов. При этом эффективность оценивается по двум критериям: по расстоянию, проходимому фреймом, и по степени использования кабельной системы. Алгоритм формирует для фреймов однонаправленный сетевой путь. Все мосты, имеющиеся в сети, взаимодействуй друг с другом и определяют направление, по которому передаются фреймы в цепочке мостов. При этом выбирается так называемый корневой мост (root bridge). Каждый мост получает уникальный идентификатор и уровень приоритета. Наивысший приоритет имеет корневой мост. Протокол алгоритма связующего дерева позволяет мостам взаимодействовать при помощи специальных широковещательных фреймов (широковещательные посылки, в которых один фрейм передается в несколько целевых узлов, описывались в главе 2), называемых блоками данных протокола моста (bridge protocol data unit, BPDU). Эти блоки данных позволяют мостам получать сведения о других мостах. Формат фрейма BPDU показан на рис. 4.7.

Рис. 4.7. Побайтовое представление фрейма BPDU

Значения полей фрейма:

- Proto id – идентификатор протокола, равный 0 для всех фреймов BPDU
- vers – номер версии, всегда равный 0;
- Mess Type – тип сообщения, равный 0 для фреймов BPDU;
- Flags – поле флагов содержит разряд TC, указывающий на измерение топологии, и разряд TCA, являющийся подтверждением конфигурационного сообщения, имеющего установленный разряд TC. Остальные шесть разрядов не используются;
- Root ID – признак корневого моста, за которым следуют два байта приоритета и шесть байтов идентификатора моста;
- Root Path cost – "стоимость" пути от моста, отправившего конфигурационное сообщение корневому мосту (понятие "стоимости" будет описано позже);
- Brdg ID – приоритет и идентификатор моста, отправившего сообщение;
- port ID – идентификатор порта или интерфейса, с которого было послано конфигурационное сообщение. Это поле позволяет мосту обнаружить зацикленные сообщения;
- Mess Age – поле возраста содержит время, прошедшее с того момента, как корневой мост отправил сообщение;
- Max Age – поле максимального возраста указывает время, когда текущее сообщение должно быть удалено;
- Hello Time – интервал времени между двумя сообщениями корневого моста;
- Forw Delay – задержка пересылки, содержащая интервал времени, которое должно пройти перед тем, как мосты перейдут в новое состояние после изменения топологии (сообщения об изменениях топологии содержат только четыре байта: поле идентификатора протокола, содержащее 0; поле версии, содержащее 0, и поле типа сообщения, содержащее значение 128).

Первым шагом при создании сети с мостами является определение моста с наивысшим приоритетом. Такой приоритет получает мост, имеющий самый маленький MAC-адрес, он и становится корневым мостом. Другие мосты получают приоритеты в соответствии со своими MAC-адресами (в соответствии с алгоритмом связующего дерева – чем меньше MAC-адрес моста, тем выше его приоритет).

Мост, назначенный корневым (его порты называют "назначенными" портами), сразу же рассылает корневые фреймы BPDU для обнаружения замкнутых маршрутов. Другие мосты переводят выбранные порты в заблокированное (однонаправленное) состояние, чтобы замкнутые маршруты стали невозможными. Фрейм не может обойти весь связанный мостами путь более одного раза, в противном случае он превышает допустимое количество пересылок (hop) и уничтожается. Каждому порту назначается некоторое значение стоимости пути, которое либо выбирается по умолчанию, либо устанавливается администратором сети. Стоимость пути к корневому мосту определяется с учетом скорости линии и расстояния. Линия T-1, работающая со скоростью 1,544 Мбит/с, имеет более высокую скорость, чем линия Мбит/с Ethernet. Мост, находящийся дальше от корневого моста, заблокирует свои порты из-за более высокой стоимости передачи (т. е. из-за более длинного пути к корневому мосту).

Как только определена структура сети связующего дерева, корневой мост начинает каждые несколько секунд передавать фреймы BPDU типа Hello. Если другие мосты сети не получают этот фрейм в течение определенного промежутка времени (по умолчанию 20 секунд), предполагается, что корневой мост отключен или неисправен. Мост, который первым обнаружит это, для выбора нового корневого моста генерирует конфигурационный BPDU-фрейм, сообщающий об изменении топологии сети.

Совет

Фреймы BPDU типа Hello могут создавать избыточный сетевой трафик. Нужно отслеживать

частоту их появления и при необходимости увеличить интервал между их передачей.

В сетях Ethernet расчеты стоимости пути позволяют также обеспечить целостность переданного фрейма. Нередко администраторы сети устанавливая предельную стоимость, например, указывают, что в линейном маршруте между двумя узлами может быть более восьми мостов. При превышении этого числа алгоритмы CSMA/CD могут давать ошибки синхронизации фреймов. Хотя это ограничение на применение алгоритма связующего дерева не закреплено официально в стандарте, добросовестные сетевые администраторы придерживаются его.

Алгоритм связующего дерева может показаться сложным, однако можно выделить некоторые важные задачи, которые он решает, упрощая управление сетевым трафиком.

- Алгоритм связующего дерева допускает только один путь для каждого сегмента сети, имеющей мосты. Такой подход означает, что порты мостов, использующих этот алгоритм, работают только в одном направлении (подобно улице с односторонним движением), при этом некоторые порты допускают передачу только входящих фреймов, а другие порты пропускают только исходящие фреймы. На рис. 4.8 отображено сравнение возможных физических маршрутов между двумя узлами и логически однонаправленный маршрут, установленный с помощью алгоритма связующего дерева.
- Алгоритм связующего дерева не позволяет фреймам перемещаться в сети бесконечно, поскольку фреймы передаются в одном направлении и уничтожаются в том случае, если они не были приняты в течение одного прохода по сети. Для определения момента удаления фрейма используется число ретрансляций (hop). Если самый длинный маршрут в сети содержит три ретрансляции (три однонаправленных перехода через мосты) то фрейм уничтожается тем мостом, при переходе через который это число увеличилось бы до четырех. Увеличение числа ретрансляций не происходит, вместо этого мост уничтожает фрейм.
- Алгоритм связующего дерева позволяет мостам передавать фреймы по наилучшему маршруту.

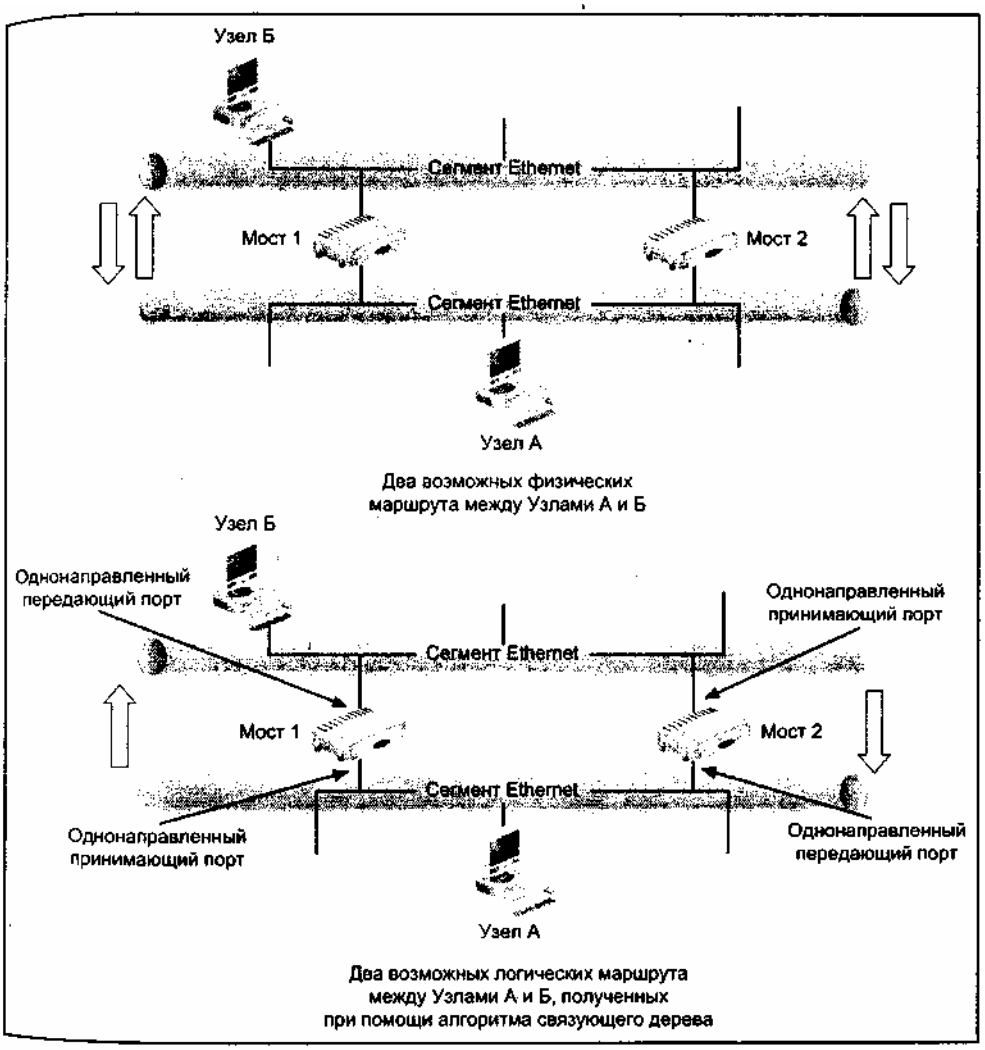


Рис. 4.8. Возможные физические маршруты в сравнении с логическим маршрутом, установленным с помощью алгоритма связующего дерева

Совет

Когда на мосте или коммутаторе включается алгоритм связующего дерева, процесс обнаружения замкнутых маршрутов может помешать автоматическому назначению IP-адресов в Windows-системах. Для устранения этой проблемы запустите в этих системах утилиту командной строки ipconfig, которая инициирует механизм автоматического выделения адресов, или же отключите данный алгоритм на этом мосте или коммутаторе.

Маршрутизаторы *т*

Маршрутизатор (router) выполняет некоторые функции моста, такие анализ топологии, фильтрация и пересылка пакетов. Однако, в отличие от мостов, маршрутизаторы могут направлять пакеты в конкретные сети, анализировать сетевой трафик и быстро адаптироваться к изменениям сети. Маршрутизаторы соединяют локальные сети на Сетевом уровне эталонной модели OSI, что позволяет им анализировать в пакетах больше информации, чем это возможно для мостов. На рис. 4.9 показан маршрутизатор, направляющий пакет в конкретную сеть и не рассылающий без надобности этот пакет во все связанные сети (т. е. не делающий широковещательных рассылок).

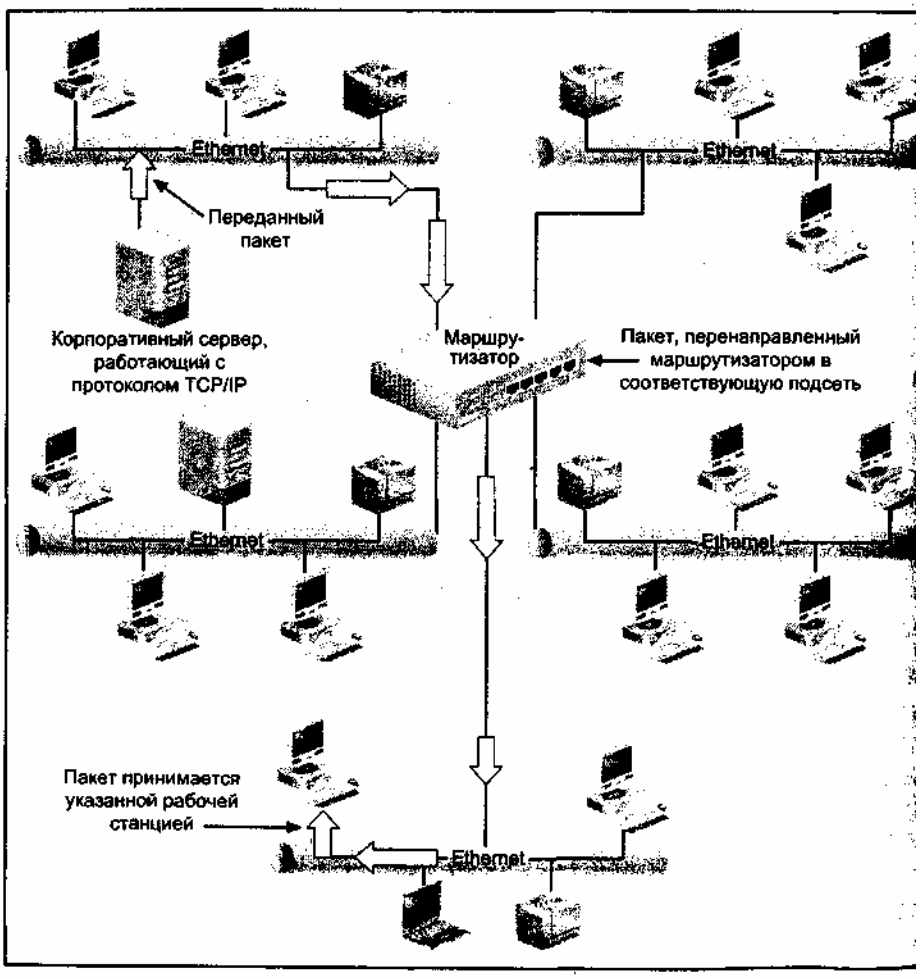


Рис. 4.9. Пересылка пакетов с помощью маршрутизатора

Главные задачи, которые могут решать маршрутизаторы:

- эффективно перенаправлять пакеты из одной сети в другую, устраняя ненужный трафик;
- соединять соседние или удаленные сети;
- связывать разнородные сети;
- устранять узкие места сети, изолируя ее отдельные части;
- защищать фрагменты сети от несанкционированного доступа.

В отличие от мостов, маршрутизаторы могут связывать сети, имеющие различные каналы данных. Например, сеть Ethernet на базе протокола TCP/IP можно подключить к коммутирующей сети с ретрансляцией кадров, в которой также используется протокол IP. Некоторые маршрутизаторы поддерживают только один протокол, например, TCP/IP или IPX. Многопротокольные маршрутизаторы могут выполнять преобразование протоколов разнородных сетей, т. е. осуществлять конвертацию протокола TCP/IP сети Ethernet в протокол AppleTalk сети с маркерным доступом, и наоборот. При наличии соответствующего аппаратного и программного обеспечения маршрутизаторы могут соединять различные сети, в том числе:

- Ethernet;
- Fast Ethernet;
- Gigabit Ethernet;
- 10 Gigabit Ethernet;
- Token Ring;
- Fast Token Ring;
- Frame Relay (сети с ретрансляцией кадров);
- ATM;
- ISDN;

- X.25.

Также в отличие от мостов, "прозрачных" для других сетевых узлов (например, рабочих станций или серверов), маршрутизаторы получают от Узлов регулярные сообщения, подтверждающие адреса узлов и их присутствие в сети. Маршрутизаторы пересылают пакеты по маршрутам, где трафик самый маленький и для которых минимальна стоимость использования сетевых ресурсов. Маршрут с наименьшей стоимостью определяется следующими факторами: расстоянием или длиной пути, нагрузкой в следующем пункте ретрансляции, имеющейся пропускной способностью и надежностью маршрута. Программные средства маршрутизатора представляют один или несколько перечисленных факторов в виде единого параметра, называемого *метрикой* (metric). Метрики применяются для определения наилучшего маршрута в сети. Для вычисления метрики могут использоваться дующие величины в любых комбинациях:

- количество входящих пакетов, ожидающих обработки, на определенном порту (подключении) маршрутизатора;
- количество ретрансляций между сегментом, к которому подключен передающий узел, и сегментом, к которому подключен принимающий узел;
- количество пакетов, которые маршрутизатор может обработать в течение определенного интервала времени;
- размер пакета (если пакет слишком большой, маршрутизатор может разделить его на несколько пакетов меньшего размера);
- пропускная способность (скорость) между двумя взаимодействующими узлами;
- доступность (работоспособность) некоторого сегмента сети.

Маршрутизаторы могут изолировать часть сети с высоким трафиком и распространять его на остальные участки сети. Эта способность маршрутизаров позволяет предотвратить потерю производительности сети и возникновение широковещательного шторма. Рассмотрим для примера более загруженную лабораторную сеть, в которой студенты учатся сетевому администрированию. При этом учащиеся часто перенастраивают различные протоколы, серверы и сетевые устройства, создавая тем самым очень большой трафик. Кроме этого, в сети работают два преподавателя, которым нужен доступ к главной университетской сети.

Для того чтобы управлять трафиком, создаваемым учебной лаборатории можно между сегментом лабораторной сети и главной сетью поместить маршрутизатор. Его можно настроить так, чтобы в главную университетскую сеть попадали пересылки пакетов только от двух преподавателей, а весь трафик, создаваемый учащимися на компьютерах и сетевых устройствах блокировался бы. Для определения транслируемых и блокируемых пакетов можно использовать IP-адресацию сетевого уровня, о чем будет рассказано в *главе 6.* Маршрутизатор будет пропускать в главную сеть пакеты, содержащие адреса преподавательских компьютеров, и отбрасывать пакеты со всеми другими адресами.

По мере усложнения структуры сети растет необходимость передачи пакетов по самому короткому и наиболее эффективному маршруту. Чтобы обеспечить полный контроль над растущим сетевым трафиком и избежать падение производительности сети, вместо мостов часто используют маршрутизаторы. Кроме того, маршрутизаторы намного эффективнее мостов в случае объединения больших сетей. Однако при модернизации следует учитывать скорость обработки пакетов в маршрутизаторе в сравнении со скоростью обработки фреймов мостом. В принципе мост работает быстрее маршрутизатора, поскольку он не анализирует и не обрабатывает данные о маршрутизации. Чтобы компенсировать эти издержки, некоторые маршрутизаторы оснащаются специализированными процессорами, позволяющими сделать соразмерными эти скорости.

Примечание

При модернизации сети нужно проанализировать, какие протоколы применяются. Некоторые протоколы, например, NetBEUI и DLC, не могут маршрутизироваться, что осложняет замену мостов маршрутизаторами в тех случаях, когда такие протоколы должны использоваться и в дальнейшем. Подробнее сетевые протоколы рассматриваются в *главе 5.*

Совет

Некоторые службы каталогов *(см. главу 3),* например, Microsoft Active Directory, создают большой трафик, вызванный частыми репликациями (копированиями) данных каталога между несколькими серверами. Эти данные включают в себя информацию об учетных записях пользователей и групп, общих файлах и принтерах. Одним из способов контроля над репликацией каталога Active Directory является размещение маршрутизаторов между удаленными серверами. После этого вы сможете указать маршрутизаторы в качестве мостов связей сайтов (site link bridge), после чего они смогут направлять трафик, вызванный репликацией, по наиболее эффективным маршрутам (выбранным в качестве связей сайтов Active Directory). Процесс настройки моста связей сайтов рассматривается в практическом задании 4-6.

Статическая и динамическая маршрутизация

Маршрутизация бывает статическая и динамическая. Для *статической маршрутизации* необходимы таблицы маршрутизации, которые создает сетевой администратор; в них указываются фиксированные (статические) маршруты между любыми двумя маршрутизаторами. Эту информацию администратор вводит в таблицы вручную. Администратор сети также отвечает за ручное обновление таблиц в случае отказа каких-либо сетевых устройств. Маршрутизатор, работающий со статическими таблицами, может определить факт неработоспособности какого-либо сетевого канала, однако он не может автоматически изменить пути передачи пакетов без вмешательства со стороны администратора.

Динамическая маршрутизация выполняется независимо от сетевого администратора. Протоколы динамической маршрутизации позволяют маршрутизаторам автоматически выполнять следующие операции:

- находить другие доступные маршрутизаторы в остальных сетевых сегментах;
- определять с помощью метрик кратчайшие маршруты к другим сетям;
- определять моменты, когда сетевой путь к некоторому маршрутизатору недоступен или не может использоваться;
- применять метрики для перестройки наилучших маршрутов, когда некоторый сетевой путь становится недоступным;
- повторно находить маршрутизатор и сетевой путь после устранения сетевой проблемы в этом пути.

Таблицы и протоколы маршрутизации

Базы данных используются маршрутизаторами для хранения информации об адресах узлов и состоянии сети. Базы данных таблиц маршрутизации содержат адреса других маршрутизаторов. Маршрутизаторы, настроенные на динамическую маршрутизацию, автоматически обновляют эти таблицы, регулярно обмениваясь адресами с другими маршрутизаторами.

Также маршрутизаторы обмениваются сведениями о сетевом трафике, топологии сети и состоянии сетевых каналов. Каждый маршрутизатор хранить эту информацию в базе данных состояния сети.

При получении пакета маршрутизатор анализирует протокольный адрес на значения, например, IP-адрес в пакете протокола TCP/IP. Направление пересылки определяется на основании используемой метрики, т. е. с учетом информации о состоянии сети и количестве ретрансляций, необходимых для передачи пакета целевому узлу.

Маршрутизаторы, работающие только с одним протоколом (например, с TCP/IP), поддерживают лишь одну базу данных адресов. Многопротокольный маршрутизатор имеет базу адресов для каждого поддерживаемого протокола (к примеру, базы данных для сетей TCP/IP и IPX/SPX). Маршрутизаторы обмениваются информацией с помощью одного или нескольких протоколов маршрутизации. Для осуществления взаимодействия многопротокольных маршрутизаторов требуются специальные протоколы.

Для общения маршрутизаторы используют различные методы. Например, маршрутизатор может проверить состояние всех непосредственно подключенных каналов и послать эту информацию другим маршрутизаторам с помощью сообщений о состоянии каналов. Или же маршрутизатор может разослать другим маршрутизаторам сети сообщение об обновлении маршрутов, содержащее частичные или полные данные своей таблицы маршрутизации.

Для взаимодействия между маршрутизаторами, находящимися в локальной системе, например,

внутри одной организации и в одной локальной сети обычно применяются два протокола: RIP и OSPF. Маршрутизаторы используют *Routing Information Protocol (RIP)* для определения минимального количества ретрансляций между ними и другими маршрутизаторами, после чего эта информация добавляется в таблицу каждого маршрутизатора. После этого сведения о количестве ретрансляций используются для нахождения наилучшего маршрута для пересылки пакета подобно тому, как мосты используют аналогичную информацию. Протокол RIP применяется реже, поскольку каждый RIP-маршрутизатор дважды в минуту посылает сообщение об обновлении маршрутов, и это сообщение содержит всю таблицу маршрутизации. В сети с несколькими маршрутизаторами это может создать заметный излишний трафик. Проблема еще больше обостряется, когда помимо этого специально выделяются серверы, хранящие информацию о маршрутизации и регулярно посылающие ее с помощью протокола RIP.

Ценность протокола RIP довольно ограничена, поскольку он в качестве метрик использует только количество ретрансляций. С его помощью нельзя найти наилучший маршрут, если имеются различные каналы, например, Ethernet и Fast Ethernet, или же маршрут с высоким трафиком и маршрут с низким трафиком. Несмотря на эти ограничения, протокол RIP по-прежнему применяется в небольших сетях, где не нужен более сложный протокол, а сетевой трафик относительно невелик. RIP-пакет содержит следующие данные: заголовок с управляющей информацией; IP-адрес, определяющий связанную сеть, и метрику, которая представляет собой расстояние или количество ретрансляций от широковещательного маршрутизатора до сети, указанной в IP-адресе.

Протокол *Open Shortest Path First (OSPF)* применяется чаще всего, он имеет несколько преимуществ по сравнению с протоколом RIP. Одним из достоинств является то, что при его использовании маршрутизатор пересылает только ту часть таблицы маршрутизации, которая относится к его ближайшим каналам; такая посылка называется "сообщением маршрутизатора о состоянии каналов". Ближайшие каналы маршрутизатора определяются путем установки граничных маршрутизаторов, или маршрутизаторов границы области, на концах сети. Все маршрутизаторы, находящиеся между ними, обращаются к общей таблице маршрутизации по протоколу OSPF (рис. 4.10).

Протокол OSPF имеет еще два преимущества:

- для упаковки информации о маршрутизации он использует пакеты меньшего размера, чем у протокола RIP;
- между маршрутизаторами распространяется не вся таблица маршрутизации, а только ее обновленная часть.

Поскольку протокол OSPF эффективнее протокола RIP, маршрутизатор с его помощью может быстрее построить таблицу маршрутизации. При первом включении маршрутизаторы, работающие с OSPF, определяют расстояние до сетей, непосредственно к ним подключенных. Это расстояние называется вектором расстояния (distance vector). Затем, используя векторы Расстояния, маршрутизаторы находят стоимость канала (пути) для каждой сети: чем дальше сеть от маршрутизатора, тем выше стоимость канала. Если сеть перемещается, то маршрутизатор пересчитывает стоимость канала. Кроме того, протокол OSPF периодически инициирует проверку на появление новых сетей, и для них также вычисляется стоимость канала.

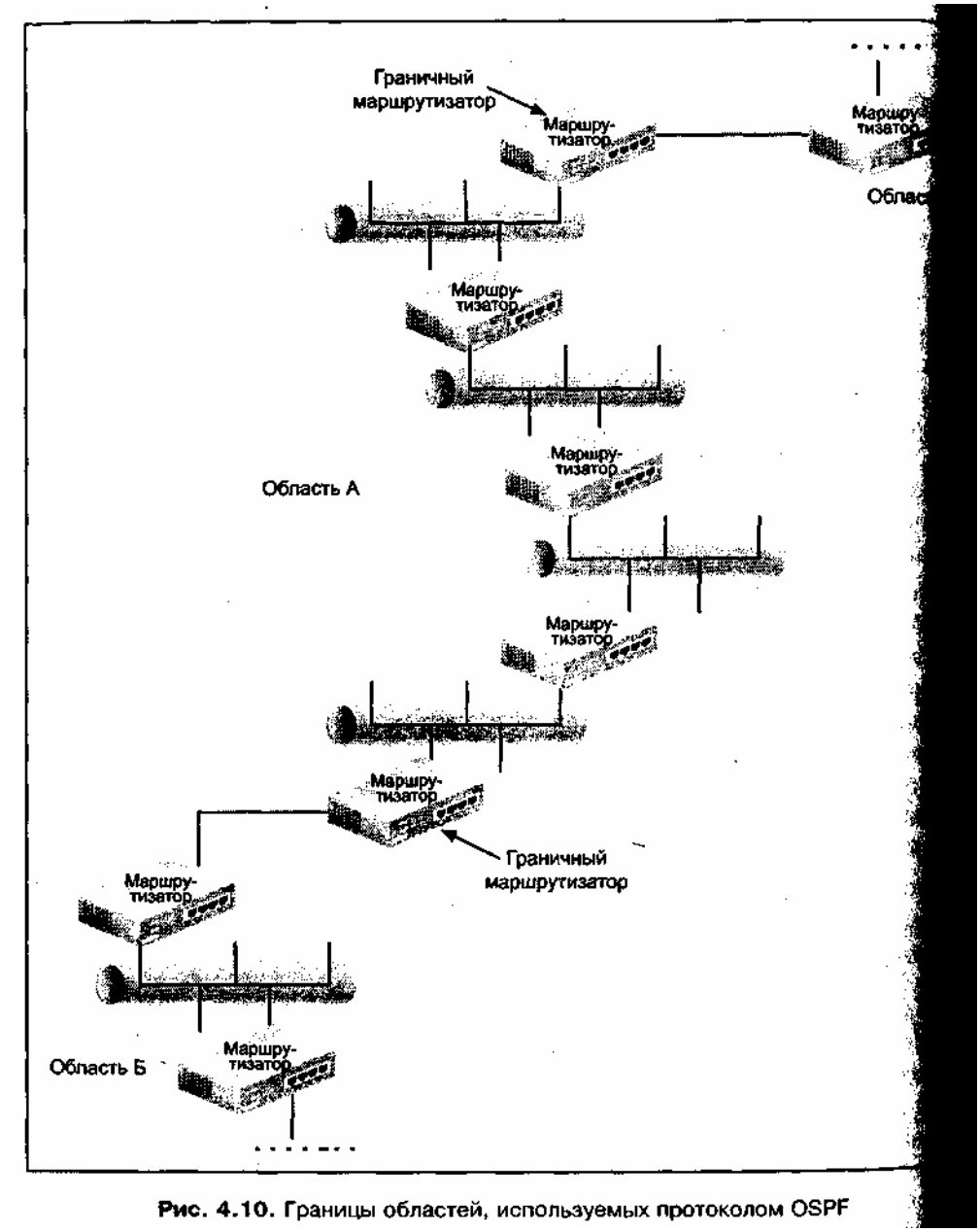


Рис. 4.10. Границы областей, используемых протоколом OSPF

Совет

Иногда в качестве маршрутизаторов конфигурируются серверы Windows или NetWare. Сервер Red Hat Linux 7.x, как и большинство систем UNIX, также может выполнять функции маршрутизатора. Во многих сетях, особенно в средних и больших, целесообразнее использовать не обычные серверы, а специализированные маршрутизаторы. Многие серверы настроены на работу с протоколом RIP и поэтому не могут работать так же эффективно, как OSPF-маршрутизаторы. Серверы и UNIX-системы будут работать быстрее, если на них не возлагаются функции маршрутизации. Практические задания 4-7 и 4-8 познакомят вас с тем, как отключить маршрутизацию на сервере Windows 2000 и запретить переадресацию (forwarding) в системе Red Hat Linux 7.x.

Маршрутизаторы, соединяющие локальные сети в пределах одного здания или связывающие смежные сети внутри кампуса, называются *локальными маршрутизаторами.* Например, локальный маршрутизатор может соединять две сети Ethernet, расположенные на одном этаже здания, или две сети, находящиеся в разных зданиях. Один локальный маршрутизатор может поддерживать 15 различных сетевых протоколов, включая TCP/IP, IPX/SPX и AppleTalk. Эти маршрутизаторы постоянно следят за подключенными к ним сетям и обновляют таблицы маршрутизации при изменениях в сетях. Они анализируют скорости каналов, нагрузку сети, сетевую адресацию и топологию сети.

Локальные маршрутизаторы используются для сегментации сетевого трафика и обеспечения безопасности. С их помощью можно запретить передачу некоторых типов пакетов из

определенного сетевого сегмента, а также управлять доступом к сегменту, содержащему важную информацию, со стороны других узлов сети. Если маршрутизатор используется для повышения безопасности, он работает как сетевой брандмауэр, защищающий сеть от хакеров и нежелательного трафика.

Мосты-маршрутизаторы

Мост-маршрутизатор (brouter) – это сетевое устройство, в некоторых случаях исполняющее функции моста, а в других случаях – функции маршрутизатора. Например, такое устройство может работать как мост для определенных Протоколов, таких как NetBEUI (поскольку тот является немаршрутизируемым), и как маршрутизатор для других протоколов, например, для TCP/IP. Мост-маршрутизатор может выполнять следующие функции:

- эффективно управлять пакетами в сети со многими протоколами, включая протоколы, которые являются маршрутизируемыми, и протоколы, которые маршрутизировать нельзя;
- уменьшать нагрузку на каналы, изолируя и перенаправляя сетевой трафик;
- соединять сети;
- обеспечивать безопасность некоторых фрагментов сети, контролируя доступ к ним.

Мосты-маршрутизаторы используются в сетях, работающих с несколькими протоколами, например, с NetBEUI, IPX/SPX и TCP/IP, поэтому они также называются многопротокольными маршрутизаторами. Функции (маршрутизация или пересылка), выполняемые ими по отношению к некоторому протоколу, зависят от двух причин:

- от директив сетевого администратора, заданных для этого протокола;
- от того, содержит ли входящий фрейм данные о маршрутизации (если не содержит, то пакеты этого протокола обычно пересылаются во все сети).

Если мост-маршрутизатор настроен не на маршрутизацию, а на пересылку протокола, он передает каждый фрейм, используя адресную информацию подуровня MAC Канального уровня так, как это делает мост. Это существенная возможность для сети, в число протоколов которой входит NetBEUI (поскольку этот протокол нельзя маршрутизировать). Для маршрутизируемых протоколов, таких как TCP/IP, мост-маршрутизатор пересылает пакеты в соответствии с адресной информацией и данными о маршрутизации, содержащимися на сетевом уровне.

Коммутаторы

IB

Коммутаторы (switch) обеспечивают функции моста, а также позволяют повысить пропускную способность существующих сетей. Коммутаторы используемые в локальных сетях, напоминают мосты в том смысле, что они работают на подуровне MAC Канального уровня (Уровня 2) и анализируют адреса устройств во всех входящих фреймах. Как и мосты, коммутаторы хранят таблицу адресов и используют эту информацию для принятия решения о том, как фильтровать и пересылать трафик локальной сети. В отличие от мостов, для увеличения скорости передачи данных и полосы пропускания сетевой среды в коммутаторах применяются методы коммутации.
В коммутаторах локальных сетей обычно используется один из двух методов

- при *коммутации без буферизации пакетов* (cut-through switching) фреймы пересылаются по частям до того момента, пока фрейм не будет получен целиком. Передача фрейма начинается сразу же, как только будет прочитан целевой адрес MAC-уровня и из таблицы коммутатора будет определен порт назначения. Такой подход обеспечивает относительно высокую скорость передачи (отчасти за счет отказа от проверки наличия ошибок).
- в процессе *коммутации с промежуточным хранением* (store-and-forward switching) (также называемой *коммутацией с буферизацией)* передача фрейма не начинается до тех пор, пока он не будет получен полностью. Как только коммутатор получает фрейм, он проверяет его контрольную сумму (CRC) перед тем, как отправлять целевому узлу. Затем фрейм поминается (буферизируется) до тех пор, пока не освободится соответствующий порт и коммуникационный канал (они могут быть заняты другими данными). Новейшие модели коммутаторов (иногда называемые маршрутизирующими коммутаторами), использующие коммутацию с промежуточным хранением, могут совмещать функции маршрутизаторов и коммутаторов и, следовательно, работают на' Сетевом уровне (Уровне 3),

чтобы определять кратчайший путь к целевому узлу. Одним из достоинств таких коммутаторов является то, что они предоставляют большие возможности для сегментации сетевого трафика, позволяя избегать широковещательного трафика, возникающего в сетях Ethernet.

Совет

Среди сетевых специалистов ведутся споры на тему, отвечают ли маршрутизирующие коммутаторы общему соглашению относительно того, что коммутаторы должны строго соответствовать требованиям к устройствам Уровня 2. Согласно первым определениям коммутатора, появившимся в 1980-х годах, коммутатор Уровня 3 фактически представляет собой маршрутизатор, использующий методы коммутации для более быстрой пересылки пакетов по сравнению с традиционными маршрутизаторами. В настоящее время имеются "коммутаторы", ориентированные на работу на Уровне 4 и выше, и обсуждается вопрос, соответствуют ли они определению истинного коммутатора или же должны позиционироваться как устройства иного типа.

Коммутация с промежуточным хранением распространена больше, чем коммутация без буферизации пакетов, и в некоторых коммутаторах, работающих по этому принципу, для повышения производительности используется встроенный центральный процессор. В принципе коммутаторы с собственным процессором работают значительно быстрее, чем "простые" коммутаторы. Однако в некоторых случаях и такие коммутаторы могут быть перегружены входящим трафиком, причем использование процессора может достигать 100% и коммутатор фактически будет работать медленнее, чем коммутатор без внутреннего процессора. Поэтому, если используется коммутатор с собственным процессором, важно определить мощность этого процессора и его соответствие ожидаемой сетевой нагрузке.

Коммутаторы локальных сетей поддерживают следующие стандарты:

- Ethernet;
- Fast Ethernet;
- Gigabit Ethernet;
- 10 Gigabit Ethernet;
- Token Ring;
- Fast Token Ring;
- FDDI;
- ATM.

Одной из наиболее распространенных задач, решаемой при помощи механизмов коммутации, является уменьшение вероятности конфликтов и повышение пропускной способности локальных сетей Ethernet. Коммутаторы сетей Ethernet, используя свои таблицы MAC-адресов, определяют порты, которые должны получить конкретные данные. Поскольку каждый порт подключен к сегменту, содержащему только один узел, то этот узел и сегмент получают в свое распоряжение всю полосу пропускания (10 или 100 Мбит/с, 1 или 10 Гбит/с), т. к. другие узлы отсутствуют; при этом вероятность конфликтов уменьшается. Другой распространенной областью применения коммутаторов являются сети с маркерным кольцом. Коммутатор Token Ring может выполнять только функции моста на канальном уровне или работать как мост с маршрутизацией от источника на Сетевом уровне.

Примечание

Хотя в некоторых случаях спецификации IEEE позволяют подключить два узла к сегменту концентратора или коммутатора Ethernet, сетевые администраторы обычно используют только один узел, позволяя тем самым повысить пропускную способность сети с помощью методов коммутации.

Переключаясь непосредственно к тому сегменту, который должен получать данные, коммутаторы могут значительно увеличить пропускную способность сети без модернизации, существующей передающей среды. Рассмотрим для примера не имеющий возможности коммутации концентратор Ethernet, к которому подключены восемь сегментов 10 Мбит/с. Скорость работы этого концентратора никогда не превысит 10 Мбит/с, поскольку каждый момент времени он может передавать данные только в один сегмент. Если концентратор заменить коммутатором Ethernet, общая пропускная способность сети увеличится в восемь раз, т. е. до 80 Мбит/с, поскольку коммутатор может посылать

пакеты в каждый сегмент практически одновременно. В настоящее время коммутаторы не намного дороже концентраторов, поэтому с их помощью проще всего повысить скорость работы сети с высоким трафиком.

Выпускаются управляемые коммутаторы, которые, как и управляемые концентраторы, имеют "интеллектуальные" способности. Для многих сетей имеет смысл потратить дополнительные средства на приобретение управляемых коммутаторов, поддерживающих протокол SNMP, что позволит повысить степень управления и мониторинга сети. Некоторые коммутаторы также могут поддерживать технологию *виртуальных локальных сетей* (Virtual LAN, VLAN). Эта технология, описанная стандартами IEEE 802.1q, представляет собой программный метод деления сети на подсети, не зависящие от ее физической топологии и содержащие логические группы. Члены рабочей группы VLAN могут располагаться в физически удаленных сетевых сегменте однако их можно объединить в один логический сегмент с помощью программного обеспечения и коммутаторов VLAN, маршрутизаторов и других сетевых устройств. Лучше всего для реализации сетей VLAN использовать маршрутизирующие коммутаторы, поскольку они позволяют уменьшить издержки на управление сетью, что объясняется их умением маршрутизировать пакеты между подсетями. Коммутаторы Уровня 2 в сети VLAN требуют, чтобы порты коммутаторов были связаны с MAC-адресами, что усложняет управление сетью VLAN.

> **Совет**
>
> Стоимость маршрутизирующих коммутаторов не намного выше, чем у обычных коммутаторов Уровня 2, поэтому они являются удачным решением для многих сетей. При проектировании сети рассмотрите возможность применения маршрутизирующего коммутатора вместо коммутатора Уровня 2, что даст возможность использования подсетей для управления сетевым трафиком и предотвращения широковещательного шторма.

Шлюзы

Термин *шлюз* (gateway) используется во многих контекстах, но чаще всего он обозначает программный или аппаратный интерфейс, обеспечивающий взаимодействие между двумя различными типами сетевых систем или программ. Например, с помощью шлюза можно выполнять следующие операции:

- преобразовывать широко используемые протоколы (например, TCP/IP) в специализированные (например, в SNA);
- преобразовывать сообщения из одного формата в другой;
- преобразовывать различные схемы адресации;
- связывать хост-компьютеры с локальной сетью;
- обеспечивать эмуляцию терминала для подключений к хост-компьютеру;
- перенаправлять электронную почту в нужную сеть;
- соединять сети с различными архитектурами.

Шлюзы имеют множество назначений, поэтому могут работать на любом Уровне OSI. Традиционно шлюз представляет собой сетевое устройство, Преобразующее один протокол в другой, структурно отличный. Такие шлюзы работают на Сетевом уровне модели OSI. Одним из лучших примеров Шлюза данного типа является шлюз, транслирующий протокол Systems Network Architecture (SNA) компании IBM, обеспечивающий взаимодействие Между мэйнфреймами, в другой протокол, например, в более распространенный протокол TCP/IP. SNA описывается в *главе 5*.

Недостаток традиционных шлюзов при трансляции протоколов состоит в том, что они работают медленнее по сравнению с другими решениями и, следовательно, используются все реже и реже. В настоящее время для взаимодействия с мэйнфреймами IBM существуют два более эффективных средства. Самое простое решение – протокол Data Link Control (DLC), который может использоваться для подключения к мэйнфрейму только рабочих станций под управлением Windows 95/98, Windows NT и Windows 2000/XP. Для сетей, в которых к мэйнфрейму должны обращаться другие операционные системы (например, UNIX), компания IBM предоставляет возможном доступа по протоколу TCP/IP, а также оснащает мэйнфреймы интерфейсами TCP/IP. Подробнее о протоколах SNA и DLC рассказывается в *главе 5*

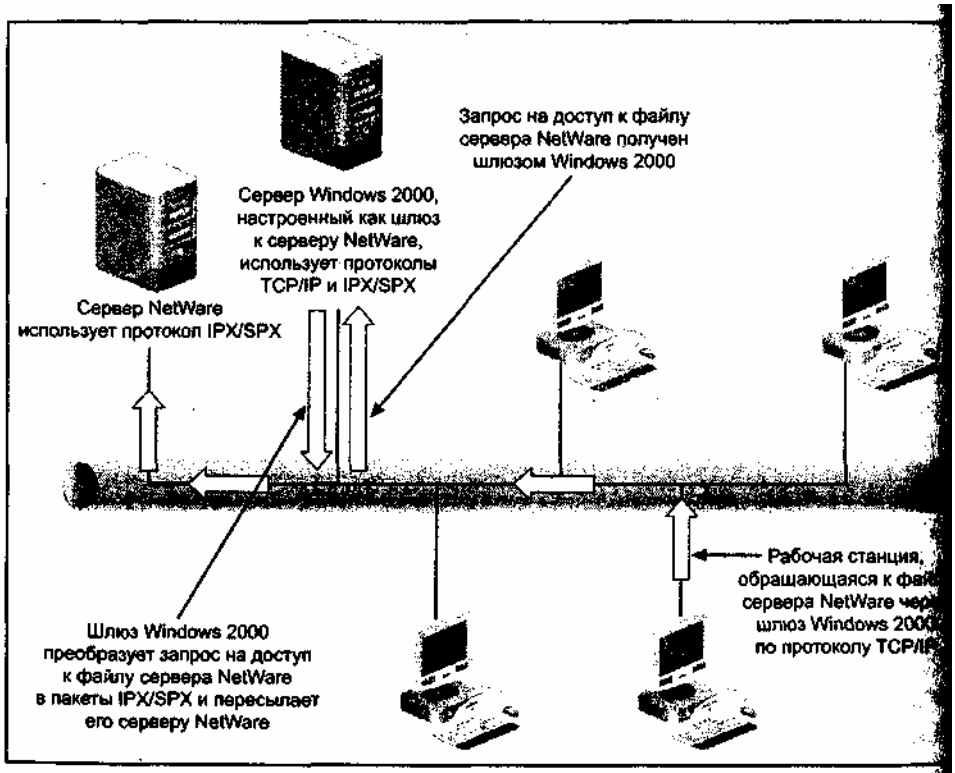


Рис. 4.11. Рабочая станция обращается к файлу сервера NetWare через шлюз, работающий на сервере Windows 2000

Другим примером шлюза, преобразующего протоколы, который к тому же транслирует запросы к службам каталога, являются службы Gateway Services for NetWare компании Microsoft. Они позволяют пользователям, зарегистрированным в системах Windows NT, Windows 2000 или Windows Server 2003 обращаться к ресурсам сервера NetWare через промежуточное обращения Windows-серверу. Если настроить сервер Windows 2000 как шлюз к серверу NetWare, то пользователи будут обращаться к серверу Windows 2000 по протоколу TCP/IP. Пройдя через этот сервер (рис. 4.11), они смогут получить доступ к серверу NetWare, настроенному на работу с протоколом IPX/SPX (1PX/SPX рассматривается в *главе 5).* Шлюз может также с помощью протокола LDAP обеспечить общий доступ к учетным записям пользователей и другой информации, хранящейся как в каталоге Active Directory, так и в службах каталога NetWare, называемых NetWare Directory Services. Этот протокол доступа к службам каталога будет описан в *следующей главе.*

Термин "шлюз" также часто используется для определения программных средств, преобразующих сообщения электронной почты из одного формата в другой. Шлюзы этого типа работают на Прикладном уровне модели OSI. Шлюзы электронной почты, такие как Mail and Messaging Services компании Microsoft, Lotus Notes (и Domino) и Mercury Mail, используются повсеместно на почтовых серверах.

Передающее оборудование глобальных сетей

Передающее оборудование глобальных сетей предназначено для работы в обычных телефонных сетях, а также на выделенных линиях, таких как T-линии и ISDN-линии. Они могут иметь аналоговые компоненты (например, модемы) или же быть полностью цифровыми (как для ISDN-коммуникаций). Чаще всего это оборудование либо преобразует сигнал для передачи на большие расстояния, либо создает множество каналов внутри одной коммуникационной среды, обеспечивая тем самым более высокую пропускную способность.

Основные виды передающего оборудования глобальных сетей:

- мультиплексоры;
- группы каналов;
- частные телефонные сети;
- телефонные модемы;
- адаптеры ISDN;
- кабельные модемы;

- модемы и маршрутизаторы DSL;
- серверы доступа;
- маршрутизаторы.

Мультиплексоры

Как было сказано в *главе 3, мультиплексоры* (multiplexer, MUX) – это сетевые устройства, которые могут принимать сигнал от множества входов и передавать их в общую сетевую среду. Мультиплексоры по сути представляют собой коммутаторы и используются в старых и новых технологиях, в том числе:

- в телефонии для коммутации физических линий;
- при коммутации телекоммуникационных виртуальных цепей для создания множества каналов в одной линии (например, в Т-линиях);
- в последовательных каналах для подключения нескольких терминалов к одной линии (в локальных или глобальных сетях), для чего эта линия делится на несколько каналов;
- в технологиях Fast Ethernet, X.25, ISDN, ретрансляции кадров, ATM других (для создания множества коммуникационных каналов в одной кабельной передающей среде).

В технологиях X.25, ISDN и ретрансляции кадров мультиплексоры применяются для передачи данных с коммутацией пакетов. При этом мультиплексор работает как узел коммутации пакетов, принимающий данные от многих узлов. Он подключен к одной кабельной передающей среде, которая делится на каналы или виртуальные сети. Мультиплексор хранит принятые пакеты до тех пор, пока не сможет открыть нужный канал; он просто переключается с одного канала на другой. Каждый пакет хранится до того момента, пока мультиплексор не откроет канал для передачи. Пример подключения мультиплексора приведен на рис. 4.12.

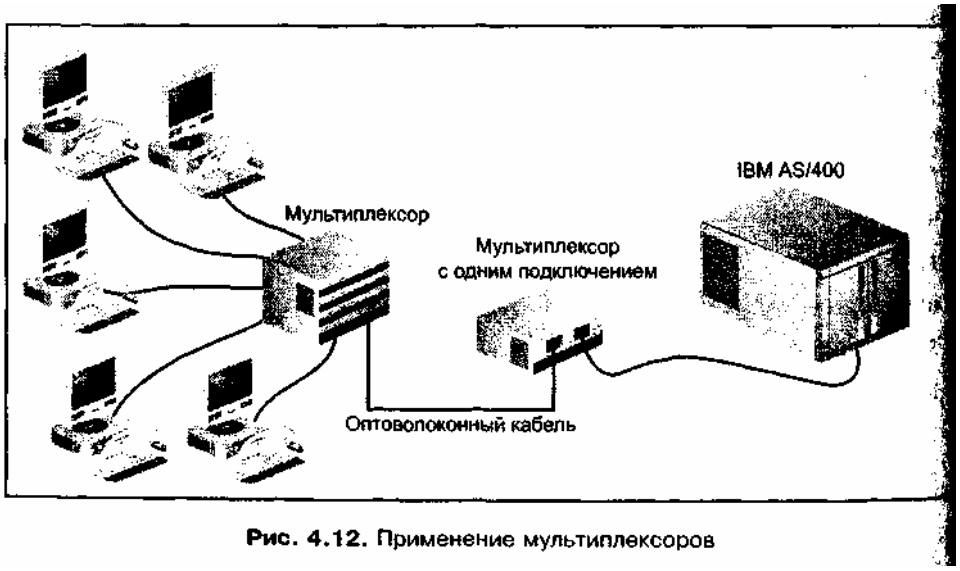


Рис. 4.12. Применение мультиплексоров

Мультиплексоры работают на Физическом уровне OSI, переключаясь между каналами. При этом используется один из трех методов электрической коммутации или единственный метод при передаче по оптической среде. Эти методы электрической коммутации описывались в *главе 2:* множественный доступ с уплотнением каналов (TDMA), множественный доступ с частотным разделением каналов (FDMA) и статистический множественный доступ.

При передаче по оптической среде применяется *спектральное разделение (уплотнение) каналов* (wavelength division multiplexing, WDM). Световую волну можно представить как спектр, состоящий из волн различной длины, изменяемой в ангстремах. Ангстрем равен 10^{-10} м, а световая волна состоит из отдельных волн длиной от 4000 до 7000 ангстрем. При использовании спектрального разделения несколько входящих соединений преобразуются в набор волн различной длины в пределах спектра света, передаваемого по оптоволоконному кабелю.

Совет

Некоторые мультиплексоры поддерживают протокол SNMP и обладают функциями управления,

что позволяет улучшить мониторинг и управляемость сети.

Группы каналов

При своем появлении группы каналов (channel bank), или канальные группы, представляли собой устройства, позволяющие пропускать несколько входящих речевых сигналов по одной линии, а мультиплексоры преобразовывали несколько сигналов данных для передачи по одной линии. Необходимость передачи голоса, данных и видео привела к быстрому развитию телекоммуникационных групп каналов, и в настоящее время с их помощью можно как передавать речевые сигналы, так и выполнять мультиплексирование данных, речи и видео. Таким образом, *группа каналов* – это крупный мультиплексор, объединяющий телекоммуникационные каналы в одном месте, называемом точкой присутствия (point of presence, POP). Эти каналы могут представлять собой частные линии T-1, полные линии T-1 и T-3, каналы ISDN или каналы с ретрансляцией кадров. Первые группы каналов типа D-1 *(см. главу 3)* состояли из мультиплексоров T-1. Усовершенствования групп каналов привели к появлению D-4 и менее дорогих систем цифрового доступа и коммутации (DACS). Там, где интенсивно используются выделенные линии, существуют также группы каналов T-3, ISDN и с Ретрансляцией кадров (технологии ISDN и ретрансляция кадров подробно рассматриваются в *главе 7).*

В пределах точки присутствия (POP) несколько групп каналов связываются Между собой для того, чтобы входящий трафик из одной группы каналов можно было переключать на другую группу каналов и отправлять к точке Назначения. Все каналы во входящей линии (например, линии T-1) объединяются и могут быть перенаправлены в другую группу каналов. Можно так же перенаправить в другую группу только один из входящих каналов. ДВ соединения групп каналов существуют два метода маршрутизации, которые, по сути, напоминают динамическую и статическую маршрутизацию в сетях. Таким образом, современные группы каналов располагают таблицами маршрутизации, которые либо поддерживаются автоматически, либо настраиваются администраторами. В зависимости от сетевой архитектуры точки присутствия, информация о маршрутизации может храниться либо централизованно в одной из групп каналов, либо распределяться между установленными группами.

Многие телекоммуникационные компании применяют группы каналов, поэтому при отказе основного маршрута передачи сигналов имеются альтернативные пути пересылки сигналов. Эти компании устанавливают минимальное время переключения на альтернативный маршрут, обычно оно равно нескольким секундам и зависит от временного интервала, в течение которого устройство передачи речи или данных может ждать перед тем, как считать соединение разорванным.

Частные телефонные сети

Некоторые организации для уменьшения числа линий, подключенных к региональной телефонной компании, разворачивают собственные телефонные службы. Например, компания может иметь 100 офисов, имеющих собственные телефоны, но при этом не более 50 сотрудников могут одновременно звонить за пределы этих офисов. Эта компания может сэкономив средства, установив собственную телефонную систему, имеющую 100 линий связи с офисами, подключаемыми к центральной АТС (автоматической телефонной станции) или коммутационному узлу, который 50-ю линиями соединен с региональной телефонной компанией. Первоначально наиболее распространенными частными системами были *офисные станции с исходящей и входящей связью* (private branch exchange, PBX). Они представляли собой коммутаторы с ручным управлением, для которых требовался оператор, выполняющий соединения внутри организации или при выходе во внешнюю телефонную сеть.

В результате усовершенствований появились автоматические учрежденческие телефонные системы, называемые *частными АТС без выхода в общую сеть* (private automatic exchange, PAX) и *частными АТС с исходящей и входящей связью* (private automatic branch exchange, PABX), В PABX-станциях по-прежнему используется коммутатор, и переключения выполняются как вручную, так и автоматически. В PAX-станциях коммутатор отсутствуя. В состав станций обоих типов входят телефонные магистральные линии (похожие на магистраль сети), обычные телефонные линии, линии связи с региональной телефонной компанией, телефоны и коммутирующая система на базе процессора или компьютер, имеющий память, жесткий диск и программное обеспечение. Эти станции могут помимо речи передавать видеосигналы и данные. Централизованная компьютерная система нередко предлагает возможности голосовой почты, переадресации и ожидания вызова,

функции учета времени и другие службы. Чаще всего такие системы имеют консоль для оператора, выполняющего специальные функции (например, обработку добавочных номеров, счетов и другой информации). Иногда имеются модемные линии для сотрудников, которые из дома по коммутируемой линии подключаются к компьютерной сети (возможности частной телефонной сети исследуются в практическом задании 4-9).

Примечание

Хотя неавтоматические PBX-станции встречаются редко, термин "PBX" по-прежнему широко (и неверно) используется для обозначения станций, которые правильнее называть PAX и PABX.

Некоторые крупные организации имеют собственные линии ISDN, T-1 или T-3, а также группы каналов для создания частных T-линий или глобальной сети на базе ISDN для связи удаленных площадок. Такой подход позволяет им иметь средства высокоскоростной передачи данных по сети, полностью находящейся под их контролем.

Телефонные модемы

Модемы долго играли важную роль в становлении глобальных сетей. Термин *модем* представляет собой сокращение от термина "модулятор/демодулятор". Модем преобразует выходящий компьютерный (цифровой) сигнал в аналоговый, который может быть передан по телефонной линии. Кроме того, модем преобразует входящий аналоговый сигнал в цифровой, понятный компьютеру.

Модемы для компьютеров бывают внутренние и внешние. Внутренний модем вставляется в компьютерный слот расширения на материнской плате. Внешний модем – это автономное устройство, подключаемое к последовательному порту компьютера с помощью специального модемного кабеля, совпадающего с разъемом последовательного порта.

Существуют три основных типа разъемов: устаревший разъем DB-25 с 25 штырьками (контактами), похожий на разъем параллельного принтерного порта (однако непригодный для работы с параллельным портом); разъем DB-9 на 9 контактов и круглый разъем PS/2 для последовательной связи (такой как на IBM PC). Также для последовательных соединений используется *универсальная последовательная шина* (Universal Serial Bus USB). Стандарт USB позволяет соединять любые типы периферийных устройств (например, принтеры, модемы и ленточные накопители) и во многих случаях заменяет обычные параллельные и последовательные порты. И внутренние, и внешние модемы подключаются к телефонной розетке с помощью обычного телефонного шнура, имеющего на обоих концах разъемы RJ-11.

Скорость передачи данных через модем измеряется двумя похожими, но не идентичными единицами: *скоростью в бодах* (baud rate) и *количеством битов переданных за секунду (бит/с)*. Скорость в бодах представляет собой количество изменений за секунду для волнового сигнала, передающего данные. Эта скорость достоверно определяла быстродействие модемов при их появлении (когда они могли при каждом изменении сигнала передавать только один бит данных).

Первые модемы были медленными и работали со скоростью от 300 до 1200 бод. Существовали модемы на 9600 бод, однако они были очень дороги. Технология модемов быстро развивалась и требовала новых способ! измерения их скорости. Производители разработали методы, позволяют» при каждом изменении сигнала передавать несколько бит данных. Поэтов в настоящее время скорость работы модема измеряется в битах за секунд Теперь модемы могут передавать данные со скоростью до 56 Кбит/с. .1

Основное влияние на модемные технологии оказала компания Microcom, первая разработавшая протокол *Microcom Network Protocol (MNP)*. Этот стандарт описывает классы коммуникационных служб (классы MNP со 2-й по 6-й, а также класс 10-й для передачи с использованием сотовых телефонов) и обеспечивает эффективную работу с помощью методов коррекции ошибок и сжатия данных.

Союз ITU также разработал стандарты на модемную связь, включив в свой стандарт V.42 многие классы MNP. Стандарты ITU-T для модемов перечислены в табл. 4.2.

Таблица 4.2. Стандарты ITU-T на модемы

Стандарт ITU-T	Описание
V.17	Факсимильная связь на скорости 14 400 бит/с по коммутируемым линиям
V.21	Передача данных на скорости 300 бит/с по коммутируемым линиям
V.22	Передача данных на скорости 1200 бит/с по коммутируемым и выделенным линиям
V.22bis	Передача данных на скорости 2400 бит/с по коммутируемым линиям
V.23	Передача данных на скорости 600/1 200 бит/с по коммутируемым 1 выделенным линиям
V.25	Стандарты для автоматического вызова и ответов
V.26	Передача данных на скорости 2400 бит/с по выделенным линиям
V.26bis	Передача данных на скорости 1 200/2400 бит/с по выделенным линиям
V.26ter	Передача данных на скорости 2400 бит/с по коммутируемым и выделенным линиям
V.27	Передача данных на скорости 4800 бит/с по выделенным линиям
V.27bis	Передача данных на скорости 2400/4800 бит/с по выделенным линиям
V.27ter	Передача данных на скорости 2400/4800 бит/с по коммутируемым линиям
V.29	Передача данных на скорости 9600 бит/с по выделенным линиям
V.32	Передача данных на скорости 9600 бит/с по коммутируемым линиям
V.32bis	Передача данных на скорости 14 400 бит/с по коммутируемым линиям с использованием синхронного обмена информацией
V.33	Передача данных на скорости 14 400 бит/с по выделенным линиям
V.34	Передача данных на скорости 28 800 бит/с по коммутируемым линиям с возможностью снижения скорости при ухудшении состояния линии
V.35	Передача данных на скорости 48 000 бит/с по выделенным линиям
V.42	Распознавание и коррекция ошибок на зашумленных телефонных линиях
V.42bis	Сжатие данных 4:1 для повышения пропускной способности линий
V.90	Передача данных на скорости 56 000 бит/с по коммутируемым линиям (при реальной скорости 33,6 Кбит/с от модема к удаленному узлу и 56 Кбит/с – от удаленного узла к модему)
V.92	Передача на скорости 56 000 бит/с (со скоростью восходящего потока, увеличенной до 48 Кбит/с) с возможностью временной приостановки передачи данных для речевого общения

Примечание

Суффикс bis получен от латинского слова, означающего "повторение", и служит для обозначения второй обновленной версии стандарта. Суффикс ter означает "трижды" и указывает на третье обновление стандарта.

При соединении персонального компьютера с модемом скорость передачи Данных для компьютера определяется коммуникационной скоростью терминального оборудования (data terminal equipment, DTE). Скорость модема называется коммуникационной скоростью аппаратуры передачи данных (data communications equipment, DCE). Параметры модемного порта компьютера (скорость DTE) должны совпадать или быть выше скорости DCE модема (в практическом задании 4-10 рассказывается о том, как определить скорость DTE в системах Windows 2000/XP).

Когда два модема взаимодействуют по телефонной линии (например, модем персонального компьютера передает данные сетевому модему), они могут работать на скорости, меньшей их максимального быстродействия. То есть при наличии помех в линии два модема V.34 или V.42 могут договориться о скорости передачи, равной не 28 800 бит/с, а 14 400 бит/с.

Модемы работают либо в синхронном, либо в асинхронном режиме. При *синхронных* коммуникациях повторяющиеся пакеты данных управляются синхросигналом, начинающим каждый пакет. В *асинхронном* режиме данные передаются отдельными блоками, разделенными стартовыми и стоповыми битами.

Адаптеры ISDN

Для подключения компьютера к линии ISDN необходимо устройство, напоминающее цифровой модем и называемое *терминальным адаптером* (terminal adapter, TA). Существующие терминальные адаптеры имеют почти такую же стоимость, как и высококачественные асинхронные или синхронные модемы, однако их быстродействие выше (например, от 128 до 512 Кбит/с). Терминальные адаптеры преобразуют цифровой сигнал в некоторый протокол, который пригоден для передачи по цифровой телефонной линии. Обычно у них имеется разъем аналогового телефона, с помощью которого можно подключить обычный телефон или модем и использовать их на цифровой линии. Чаще всего оборудование ISDN позволяет подключатся к одной телефонной линии или медной паре (такому же проводу, с помощью которого домашний или офисный телефон соединяется с телефонной станцией), однако оно обеспечивает раздельные каналы для компьютерных данных и обычной аналоговой голосовой связи. Одновременно можно использовать или одну аналоговую и одну цифровую линию, или две цифровых, или две аналоговых линии.

Кабельные модемы

Во многих регионах провайдеры кабельного телевидения также предлагают цифровые службы для офисного и домашнего применения. Для подключения к кабельным цифровым службам используются *кабельные модемы* (cable modem). Кабельный модем работает с восходящей (upstream) и нисходящей (downstream) частотами (каналами), которые уже используются в кабельной службе. Восходящий канал предназначен для передачи исходящего сигнала с помощью спектра (непрерывного диапазона) частот, несущих речевые телевизионные и цифровые сигналы. Нисходящий канал используется для приема сигналов, а также смешивается с другими сигналами (данными, речью и видео), поступающими абоненту.

Индустрия кабельных модемов разработала набор стандартов и связанных с ними сертификатов в рамках проекта, названного Certified Cable Modem Project (DOCSIS). Большинство коммуникационных компаний поддерживает этот проект, заменяя старые кабельные модемы новыми, удовлетворяющими стандартам DOCSIS. На момент написания книги были приняты следующие стандарты:

- DOCSIS 1.0 – этот стандарт, принятый в 1999 году, обеспечивает обычный доступ к Интернету по восходящему и нисходящему каналам, работающим со скоростью 5 Мбит/с;
- DOCSIS 1.1 – принятый в 2001 году стандарт предусматривает удвоенную скорость по сравнению с DOCSIS. 1.0 (т.е. 10 Мбит/с), а также обеспечивает криптографическую защиту данных;
- DOCSIS 2.0 (также называется Adv PHY) – предложенный, но еще не ратифицированный стандарт описывает непосредственные двухточечные коммуникации, например, между двумя организациями. Является альтернативой существующим системам на базе Т-линий.

Хотя кабельные модемы и рассчитаны на большие скорости, отдельный пользователь такого модема скорее всего получит ограниченную полосу пропускания и сможет работать со скоростью от 256 Кбит/с до 3 Мбит/с. Отчасти реальная скорость зависит от количества пользователей, подключенных к одному кабелю и активных одновременно. Сегмент кабеля может иметь максимальную полосу пропускания до 27 Мбит/с (хотя ведутся разработки гибридных кабелей с более высокими параметрами). Кроме того, провайдер кабельной службы может установить пользователю лимит на пропускную способность (т. е. ограничение на скорость приема и передачи), что делается для увеличения числа пользователей, получающих доступ к кабельной сети.

Кабельные модемы выпускаются в виде внутренних или внешних устройств. Внутреннее устройство напоминает плату модема, вставляемую в слот расширения компьютера. Более распространены внешние кабельные модемы, которые обычно подключаются к компьютеру одним из двух способов. Первый способ – непосредственно соединить модем с уже установленным в компьютере обычным сетевым адаптером при помощи витой пары и разъема RJ-45. Второй способ – непосредственное подключение к порту USB компьютера. После установки кабельного модема на компьютер другой конец модема подключается к широковещательному коаксиальному кабелю, применяемому для кабельного телевидения.

При покупке кабельного модема проверяйте, чтобы он был сертифицирован на соответствие стандарту DOCSIS 1.1. Если у вас несертифицированный Модем или модем, имеющий сертификат

DOCSIS 1.0, то рекомендуется обновить его на более новый. Помимо того, что кабельный модем стандарта DOCSIS 1.1 обеспечивает более высокую скорость передачи, в нем также предусмотрена криптографическая зашита, предотвращающая доступ к вашим данным.

Примечание

Чтобы обеспечить работу модемов, сертифицированных в соответствии с DOCSIS 1.0 или DOCSIS 1.1, провайдер кабельной системы должен в головном узле (в центральном подразделении; *см. главу 2)* иметь сертифицированные терминальные системы кабельных модемов (Certified Modem Termination System, CMTS). Такие системы имеют или развертывают многие операторы кабельной связи.

Достоинство коммуникаций с использованием кабельных модемов заключается в том, что в процессе работы, например, при загрузке большого файла пользователь может получить в распоряжение свободную в данный момент полосу пропускания хотя бы на несколько миллисекунд. Это означает, что если даже кабель занят (передает видеосигнал, речь или данные для других пользователей), система всегда динамически распределяет свободную полосу пропускания кабеля. Если некоторый пользователь подключен к кабельному модему, но не передает или не принимает информацию, то часть его полов пропускания передается другому пользователю, который более интенсивно использует канал.

Совет

Поскольку один кабель делится между несколькими пользователями, то квалифицированный пользователь может получить доступ к файлам, хранящим на вашем компьютере (в особенности, если модем не сертифицирован или сертифицирован на соответствие DOCSIS 1.0). Поэтому, если вы используете кабельный модем, то важно защитить свои файлы и компьютер с помощью средств файловой безопасности и персонального брандмауэра. Например, системы Windows XP и Red Hat Linux 7.x имеют встроенное программное обеспечение, выполняющее функции брандмауэра. Дополнительную информацию по безопасности Windows XP можно получить на сайте Microsoft, скачав пакет Security Tool Kit. Сведения о безопасности кабеля доступны на сайте **www.cablemodem.com,** принадлежащем организации CableLabs, которая представляет собой союз компаний, занимающихся кабельными телекоммуникациями и занимающихся разработкой соответствующих технологий.

Модемы и маршрутизаторы DSL

Другой высокоскоростной службой передачи цифровых данных, конкурирующей с ISDN и кабельными модемами, является технология *Digital Subscriber Line, DSL* (цифровая абонентская линия). Она подробно описывается в *главе 7* и представляет собой метод передачи цифровых данных по медному проводу, уже проложенному в большинстве офисов для телефонных служб (новейшие технологии DSL могут использоваться с оптоволоконными телефонными линиями). Как показано на рис. 4.13, для того, чтобы использовать DSL, можно установить на компьютер интеллектуальный адаптер, подключенный к сети DSL

ч

Рис. 4.13. Подключение к сети DSL

Интеллектуальный адаптер может по внешнему виду напоминать модем, однако адаптер является полностью цифровым, т. е. он не преобразует цифровой сигнал DTE (компьютера или сетевого устройства) в аналоговый, а посылает его прямо в телефонную линию. Две пары

проводников соединяют адаптер и телефонную розетку. Коммуникации по медному проводу являются симплексными (односторонними), т. е. одна пара используется для передачи исходящие данных, а другая – для приема входных сигналов, что в результате образует восходящий канал, идущий к телекоммуникационной компании, и нисходящий канал, направленный к пользователю. Максимальная скорость восходящего канала равна 1 Мбит/с, а нисходящая может достигать 60 Мбит/с. Максимальное расстояние без повторителя (усиливающего сигнал) от пользователя к телекоммуникационной компании равняется 5,5 км (что совпадает с требованиями ISDN).

Примечание

Реальная скорость обмена определяется несколькими факторами, в число которых входят следующие: тип используемой DSL-службы, состояние кабеля, расстояние до телекоммуникационной компании и быстродействие шины пользовательского компьютера.

Как и кабельный модем, адаптер DSL обеспечивает высокую скорость передачи данных, однако имеет некоторые преимущества по сравнению с ним. Например, линия кабельного модема может использоваться совместно несколькими абонентами, поэтому сигналы могут быть перехвачены и прочитаны неавторизованным пользователем. DSL-линия выделяется конкретному пользователю, что уменьшает вероятность перехвата сигналов злоумышленником. Кроме того, абонент DSL-линии имеет в своем распоряжении всю полосу пропускания линии, в отличие от пользователя кабельного модема, который делит эту полосу с другими.

К сетям DSL-линия подключается при помощи комбинированного адаптера DSL и маршрутизатора. В результате это устройство может использовать для распределения сетевого трафика и в качестве брандмауэра, обеспечивающего доступ к сетевым устройствам только авторизованным абонентам. При таком подключении множество пользователей может обращаться к одной DSL-линии через существующую сеть, при этом сеть будет защищена от вторжения через эту линию. Обычно для такого подключения имеется управляющее программное обеспечение, позволяющее выполнять мониторинг линии и ее диагностирование.)

Серверы доступа

Сервер доступа (access server) совмещает в себе функции нескольких устройств, применяемых для глобальной связи.

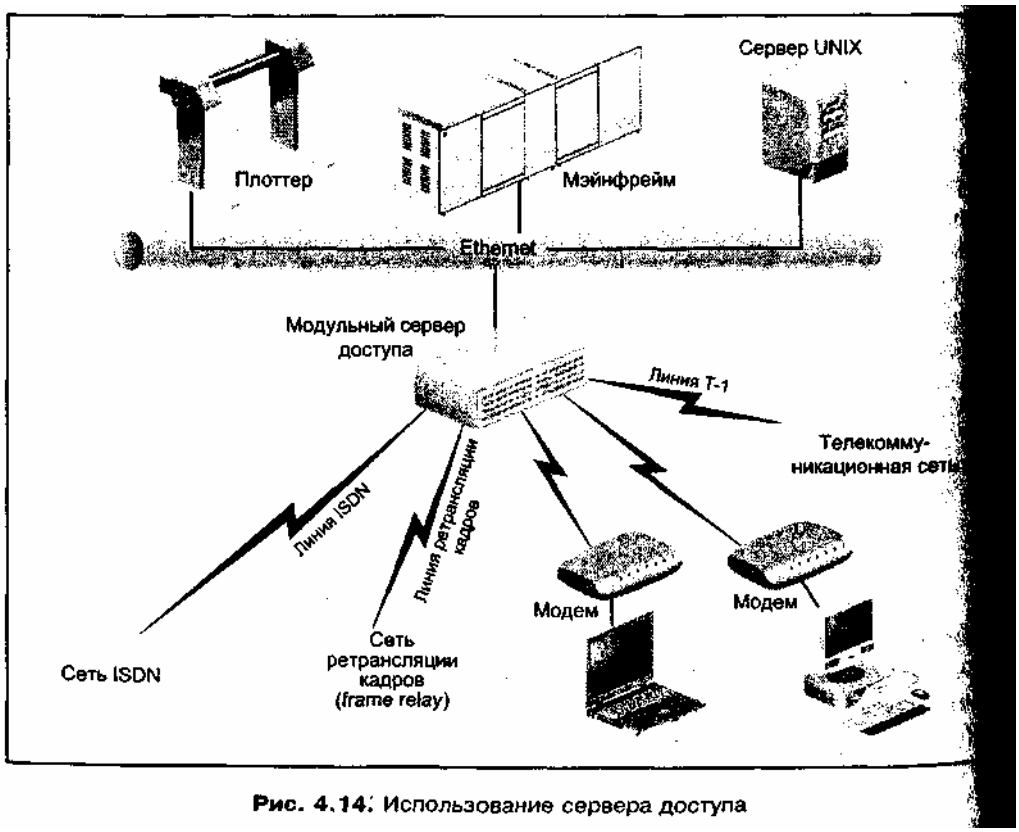


Рис. 4.14. Использование сервера доступа

Например, один сервер доступа может выполнять передачу данных с использованием модемных коммуникаций, X.25, линий T-1, T-3 и ISDN, а также ретрансляции кадров. Некоторые серверы доступа разработаны для небольших и средних по размеру сетей. Такие серверы для подключения к сети имеют адаптер Ethernet или Token Ring. Также у них существуют несколько синхронных и асинхронных портов для подключения терминалов, модемов, телефонов-автоматов, линий ISDN и X.25. У небольших серверов доступа обычно бывает от 8 до 16 асинхронных портов и один-два синхронных порта. Мощные серверы доступа имеют модульную конструкцию со слотами (от 10 до 20) для подключения коммуникационных плат, как показано на рис. 4.14. Одна плата, к примеру, может иметь 8 асинхронных портов и один синхронный. Другая плата может предназначаться для подключения к линии T-1, а еще одна – для работы с линией ISDN. Также могут быть модульные платы со встроенными модемами, например, с 4-мя модемами на одной плате. Некоторые серверы доступа модульной конструкции способны поддерживать почти 70 модемов. Для обеспечения отказоустойчивости серверы снабжаются также дополнительными источниками питания.

Маршрутизаторы

С помощью *удаленного маршрутизатора* сети, расположенные на большом удалении друг от друга (например, в разных городах), можно объединить в глобальную сеть. Один маршрутизатор, находящийся в одном городе, может соединить некоторую компанию с удаленным маршрутизатором, находящимся в другой компании, расположенной в любом другом городе.

Удаленные маршрутизаторы соединяют сети, использующие ATM, ISDN, технологии ретрансляции кадров и передачи данных по скоростной последовательной линии, а также X.25. Удаленный маршрутизатор, как и локальный, может поддерживать множество протоколов, позволяя соединять Удаленные сети различных типов. Аналогичным образом удаленный маршрутизатор может работать как брандмауэр, ограничивающий доступ к определенным сетевым ресурсам.

Некоторые удаленные маршрутизаторы имеют модульную конструкцию, что позволяет вставлять в слоты расширения различные интерфейсы (например, Интерфейс для ISDN-линии и интерфейс для ретрансляции кадров). Преимущество такого маршрутизатора состоит в том, что его можно постепенно Расширять по мере усложнения коммуникационных задач, а с этим сталкиваются многие организации. Чаще всего маршрутизаторы подключаются к глобальной телекоммуникационной линии при помощи некоторого последовательного интерфейса (например, CSU/DSU – для работы с линией T-1 *(см. главу 3)* или модульного адаптера X.25 – для подключения

к сети X.25).

Резюме

- Для обмена данными между компьютерами и сетями можно применять самые разнообразные приемопередающие устройства локальных и глобальных сетей. Основное значение имеют сетевые адаптеры, поскольку они связывают компьютеры и многие сетевые устройства с сетевым кабелем. Некоторые адаптеры являются специализированными, например, адаптеры FDDI и ATM. Растет популярность беспроводных сетевых адаптеров, поскольку они обеспечивают гибкость и удобство подключения.

- В первых и некоторых небольших современных сетях для расширения сети и увеличения длины сегментов (если длина не укладывается в спецификации IEEE) используются повторители. Некоторые сетевые устройства также выполняют функции повторителей в дополнение к своим основным, более сложным сетевым функциям (таким как фильтрация и переадресация пакетов и фреймов).

- В централизованных сетях со звездообразной топологией для связи отдельных сегментов и для объединения сетей используются концентраторы, мосты, маршрутизаторы и коммутаторы. Все эти устройства могут иметь "интеллектуальные" возможности для сбора сетевой информации при централизованном управлении сетью.

- Широкая популярность маршрутизаторов объясняется их возможностью управлять трафиком и выполнять передачу информации (как в локальных, так и в глобальных сетях). Распространены и коммутаторы из-за них более высокого быстродействия по сравнению с концентраторами, а также из-за способности работать в качестве устройств Уровня 2 (функции мостов) и Уровня 3 (функции маршрутизации). Маршрутизаторы и коммутаторы часто используются для устранения узких мест в сети (снижения нагрузки на отдельные сегменты).

- В глобальных сетях применяется разнообразное передающее оборудование, связанное с телекоммуникациями (например, мультиплексоры, группы каналов, PABX-станции, модемы, адаптеры ISDN, серверы доступа и маршрутизаторы).

- Мультиплексоры делят передающую среду на несколько каналов. Группы каналов, используемые сначала для передачи речи, в настоящее время могут интегрироваться с мультиплексорами и передавать помимо речи еще и данные, и видео.

- Многие организации (например, правительственные и образовательные) разворачивают собственные телефонные системы, такие как PABX и PAX; при этом обеспечивается экономия средств и больший контроль над телекоммуникационными возможностями этих организаций.

- Аналоговые модемы в сочетании с обычными телефонными линиями используются уже много лет, однако для обеспечения высокоскоростных коммуникаций их скорость и возможности постоянно увеличивались. Новые цифровые адаптеры, такие как терминальные адаптеры ISDN и DSL-модемы, могут передавать данные значительно быстрее, чем аналоговые модемы, однако требуют подключения к службам ISDN и DSL. Большое распространение получили кабельные модемы, поскольку они могут использоваться с уже имеющимися линиями кабельного телевидения и обеспечивают высокую скорость доступа. Для обеспечения совместимости многие операторы кабельной связи рекомендуют использовать сертифицированные кабельные модемы.

- Серверы доступа сочетают в себе все телекоммуникационные возможности, такие как модемная связь, передача по линиям T-1 и ISDN. Для объединения локальных сетей, располагающихся на значительном расстоянии друг от друга, в глобальную сеть, используются удаленные маршрутизаторы.

Глава 5

Протоколы локальных сетей

По прочтении этой главы и после выполнения практических заданий вы сможете:

- рассказать о следующих протоколах и об их использовании в различных сетевых операционных системах:
  - IPX/SPX;
  - NetBEUI;
  - AppleTalk;
  - TCP/IP;
  - SNA;
  - DLC;
  - DNA;

- обсуждать и внедрять методы повышения производительности локальных сетей.

В начале XX века социолог Георг Герберт Мид (George Herbert Mead), изучая влияние языка на людей, пришел к выводу о том, что человеческий интеллект в первую очередь развился благодаря языку. Язык помогает нам находить смысл в окружающей реальности и истолковывать ее детали. В сетях аналогичную роль выполняют сетевые протоколы, которые позволяют разнообразным системам находить общую среду для взаимодействия.

В этой главе описываются протоколы, чаще всего используемые в локальных сетях, а также сетевые операционные системы, в которых они применяются. Вы узнаете о преимуществах и недостатках каждого протокола, благодаря чему вам станут понятны области их использования. Самый популярный протокол локальных сетей – TCP/IP – рассматривается в этой главе лишь кратко, поскольку подробнее он будет описан в *главе 6*. В заключении текущей главы вы познакомитесь с методами повышения производительности локальных сетей и выбора тех протоколов, которые необходимы в конкретной ситуации.

Протоколы локальных сетей и их применение в сетевых операционных системах

Сетевые протоколы напоминают местный язык или диалект: они обеспечивают в сетях беспрепятственный обмен информацией между подключенными устройствами. Эти протоколы имеют значение и для простых электрических сигналов, передаваемых по сетевому коммуникационному кабелю. Я протоколов сетевые коммуникации были бы просто невозможны. Для та чтобы два компьютера могли свободно общаться друг с другом, они должны использовать один и тот же протокол подобно тому, как два человека вынуждены общаться на одном языке.I

В локальной сети несколько протоколов могут работать индивидуально и в некоторых сочетаниях. Сетевые устройства (например, маршрутизаторы) часто настраиваются на автоматическое распознавание и конфигурирование различных протоколов (в зависимости от операционной системы, используемой в маршрутизаторе). Например, в одной локальной сети Ethernet один протокол может использоваться для подключения к мэйнфрейму, другой для работы с серверами Novell NetWare, а третий – для серверов Windows (например, под управлением системы Windows NT Server) (рис. 5.1).

Можно установить мост-маршрутизатор, который будет автоматически распознавать каждый протокол и конфигурироваться соответствующим образом, в результате чего для одних протоколов он будет выступать в роли маршрутизатора, а для других – в роли моста. Наличие нескольких протоколов в сети эффективно тем, что такая сеть сможет одновременно выполнять множество функций (например, обеспечивать доступ к Интернета также к мэйнфреймам и серверам). Недостатком такого подхода является что некоторые протоколы будут работать в режиме широковещания, то есть, будут периодически посылать пакеты для идентификации сетевых устройств, генерируя значительный избыточный трафик.

Некоторые сетевые протоколы получили широкое распространение благодаря тому, что они связаны с конкретными сетевыми операционными системами (например, с Windows-системами, мэйнфреймами IBM, сервера UNIX и Novell NetWare). Имеет смысл изучать протоколы применительно тем операционным системам, где они применяются. В этом случае становится понятным, для чего конкретный протокол нужен в сети определенного типа. Кроме того, в этом случае вам легче будет понять, как один протокол (например, NetBEUI) можно заменить другими протоколами (такими как TCP/IP). Однако перед тем как изучать протоколы и их взаимосвязь операционными системами, важно узнать об общих свойствах протокол локальных сетей.

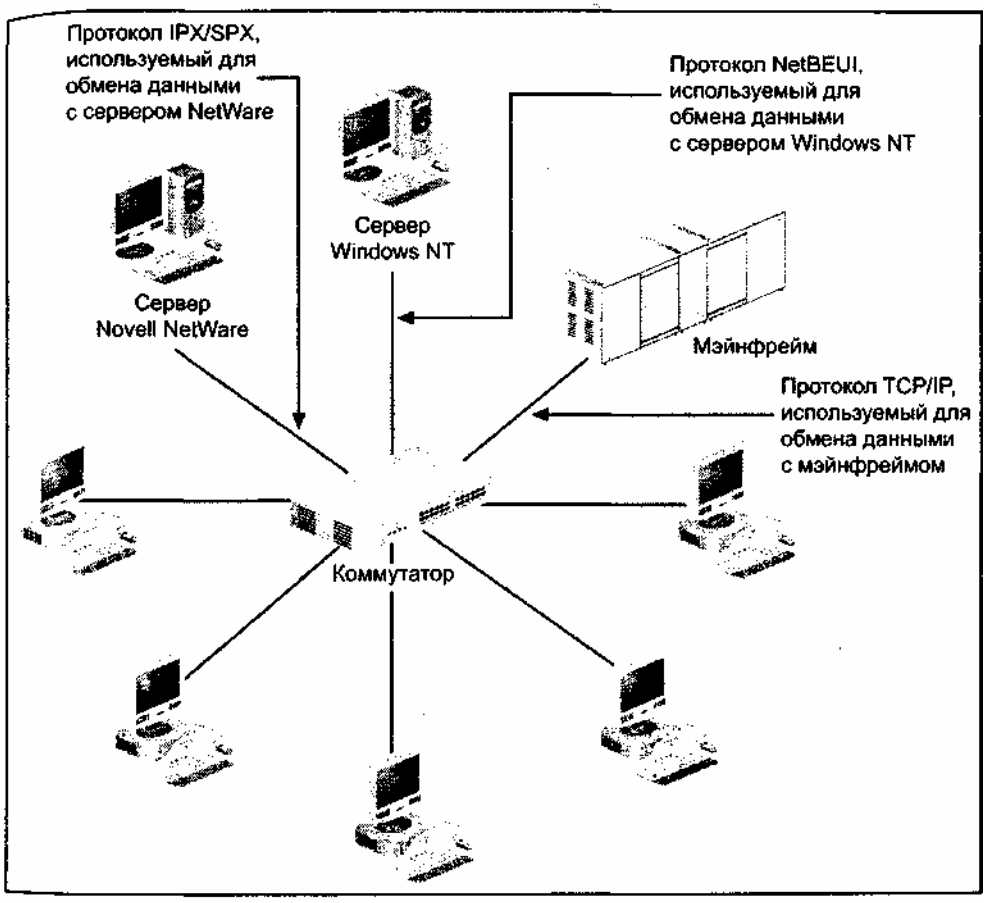


Рис. 5.1. Передача нескольких протоколов по одной сети

Общие свойства протоколов локальной сети

В основном протоколы локальных сетей имеют такие же свойства, как и Другие коммуникационные протоколы, однако некоторые из них были разработаны давно, при создании первых сетей, которые работали медленно, были ненадежными и более подверженными электромагнитным и радиопомехам. Поэтому для современных коммуникаций некоторые протоколы не вполне пригодны. К недостаткам таких протоколов относится слабая защита от ошибок или избыточный сетевой трафик. Кроме того, определенные протоколы были созданы для небольших локальных сетей и задолго до появления современных корпоративных сетей с развитыми средствами маршрутизации.

Протоколы локальных сетей должны иметь следующие основные характеристики:

- обеспечивать надежность сетевых каналов;
- обладать высоким быстродействием;
- обрабатывать исходные и целевые адреса узлов;
- соответствовать сетевым стандартам, в особенности – стандарту IEEE 802.

В основном все протоколы, рассматриваемые в этой главе, соответствуют перечисленным требованиям, однако, как вы узнаете позднее, у одних протоколов возможностей больше, чем у других.

В табл. 5.1 перечислены протоколы локальных сетей и операционные системы, с которыми эти

протоколы могут работать. Далее в главе указаны протоколы и системы (в частности, операционные системы серверов и хост компьютеров) будут описаны подробнее.

4 Таблица 5.1. *Протоколы локальных сетей и сетевые операционные системы*

Протокол	Соответствующая операционная система
IPX/SPX	Novell NetWare
NetBEUI	Первые версии операционных систем Microsoft Windows
AppleTalk	Apple Macintosh
TCP/IP	UNIX, Novel NetWare, современные версии операционных систем Microsoft Windows, операционные системы мэйнфреймов IBM
SNA	Операционные системы мэйнфреймов и миникомпьютеров IBM
DLC	Клиентские системы, взаимодействующие с мэйнфреймами IBM, настроенными на работу с протоколом SNA

Примечание

Компьютерная операционная система – это совокупность программных средств, выполняющих на компьютере две функции. Во-первых, они взаимодействуют с аппаратными средствами компьютера и базовой системой ввода/вывода (Basic input/output system, BIOS). Во-вторых, они взаимодействуют с пользовательским интерфейсом (например, с графическим пользовательским интерфейсом (GUI) системах Windows или с подсистемой X Window и рабочими столами в систем UNIX). Для *сетевых компьютерных операционных систем* имеется еще третий уровень взаимодействия, на котором эти системы могут общаться между собой по сети с помощью одного или нескольких протоколов.

Протоколы IPX/SPX и система Novell NetWare

Протокол *Internetwork Packet Exchange (IPX)* (межсетевой пакетный обмен) был разработан компанией Novell для одной из самых первых сетевых операционных систем, выполняющей серверные функции и названной NetWare. Первоначально эта система предназначалась для сетей Ethernet с шинной топологией, сетей с маркерным кольцом и сетей ARCnet, она была ориентирована на работу с одним файл-сервером. ARCnet – это одна из частных альтернативных сетевых технологий, в которой используются специальные пакеты с маркерами и смешанная топология (шина и звезда). В настоящее время операционная система NetWare стала аппаратно-независимой и может поддерживать различные топологии и протоколы.

В качестве прототипа протокола IPX компания Novell использовала один из первых протоколов локальных сетей – протокол *Xerox Network System (XNS),* адаптировав его для своей файл-серверной операционной системы NetWare. Компания Xerox Corporation предложила протокол XNS в качестве средства передачи данных по сетям Ethernet. В начале 1980-х годов некоторые производители выпустили собственные версии этого протокола. Вариант компании Novell определил возникновение протокола IPX, предназначенного для серверов NetWare. Одновременно эта компания разработала сопутствующий протокол, названный *Sequenced Packet Exchange (SPX)* и ориентированный на работу с прикладными программами, например, с базами данных.

Протоколы IPX/SPX широко используются в серверах NetWare до 4-й версии включительно. Начиная с версии NetWare 5.0, компания Novell предлагает пользователям переходить на стек протоколов TCP/IP. В настоящее время именно эти протоколы являются основными для версий NetWare 6.0 и выше, при этом пользователи могут по-прежнему применять протоколы IPX/SPX, в частности, для совместимости с устаревшими серверами и оборудованием (например, с принтерами).

Когда в сети Ethernet на основе серверов NetWare конфигурируются протоколы IPX/SPX, можно использовать фреймы Ethernet четырех типов:

- *802.2* – относительно новый тип фреймов, применяемый в сетях, базирующихся на

серверах NetWare версий с 3.21 по *4.x;*

- *802.3* – старый тип фреймов, применяемый в системах NetWare 286 (версий *2.x)* и первых версиях системы NetWare 386 (3.0 и 3.1x);
- *Ethernet II* – для обеспечения совместимости с сетями Ethernet II и более эффективного форматирования фреймов;
- *Ethernet SNAP* – реализация описанного в *главе 2* протокола SubNetwork Access Protocol (SNAP), предназначенного для работы специальных сл)Я и приложений фирм-изготовителей.

Достоинства и недостатки

Достоинством протокола IPX (несмотря на его солидный возраст) по сравнению с другими ранними протоколами является возможность его маршрутизации, т. е. то, что с его помощью можно передавать данные по многим подсетям внутри предприятия. Недостатком протокола является дополнительный трафик, возникающий из-за того, что активные рабочие станции используют часто генерируемые широковещательные пакеты для подтверждения своего присутствия в сети. При наличии множества серверов NetWare и нескольких сотен клиентов применяемые протоколом IPX широковещательные пакеты типа "я здесь" могут создавать значительный сетевой трафик (рис. 5.2).

Назначение протокола SPX

Протокол SPX, дополняющий IPX, обеспечивает передачу данных прикладных программ с большей надежностью, чем IPX. Протокол IPX работает несколько быстрее своего "компаньона", однако в нем используются службы без установления соединения, работающие на подуровне LLC Канального уровня. Это означает, что IPX гарантирует доставку фрейма в пункт назначения с меньшей вероятностью. В протоколе SPX применяются службы с установлением соединения, что повышает надежность передачи данных. Чаще всего при упоминаниях обоих протоколов (IPX и SPX) используют сокращение IPX/SPX.

Протокол SPX широко применяется для передачи по сети содержимого Я данных. Кроме того, на основе этого протокола работают утилита удаленной консоли и службы печати фирмы Novell. Удаленная консоль позволяет рабочей станции администратора видеть ту же информацию, которая отображается на консоли файл-сервера NetWare, благодаря чему пользователь может удаленно выполнять системные команды сервера, не находясь за его клавиатурой.

Развертывание протоколов IPX/SPX

Для установки протоколов IPX/SPX на компьютерах с системой DOS используются специальные DOS-драйверы, разработанные для NetWare. На 32-разрядных операционных системах (например, Windows 95 и старших версия), ля установки протоколов можно запустить программу Novell Client32, которая обеспечит командную среду для доступа к серверам NetWare.

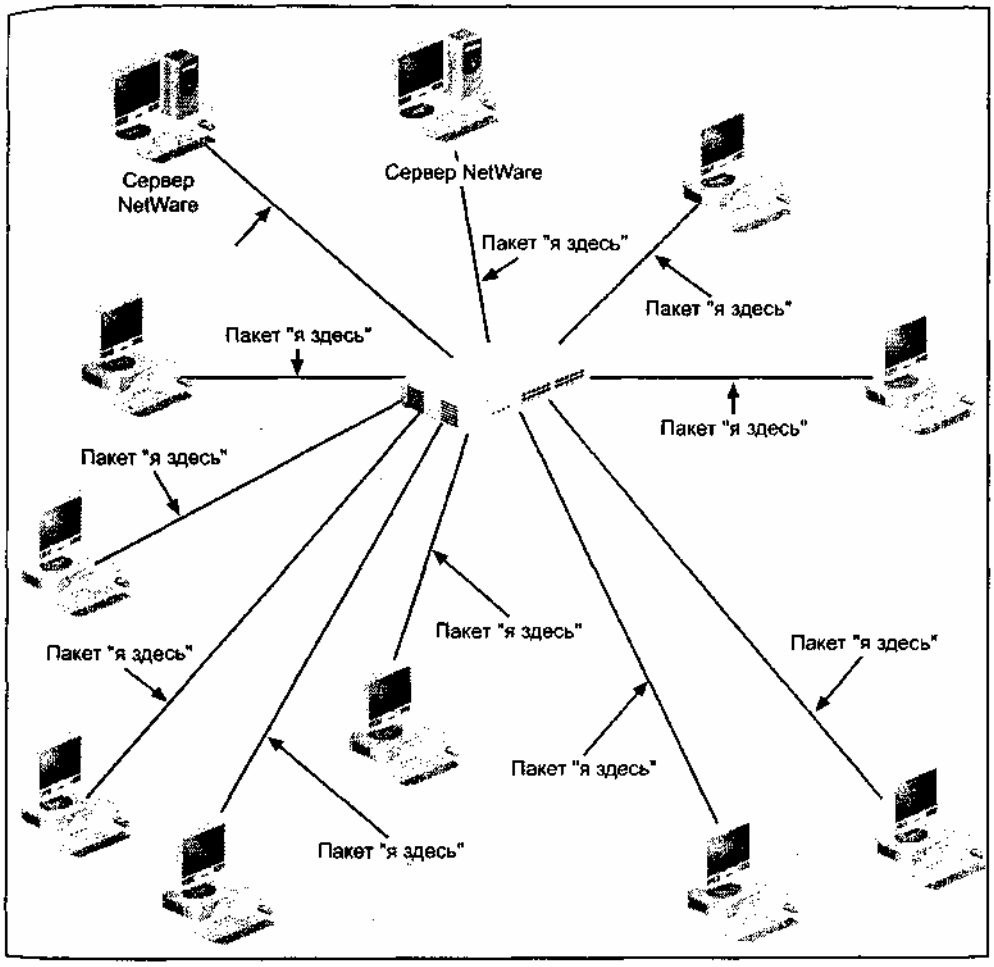


Рис. 5.2. Периодические широковещательные рассылки в сети с протоколами IPX/SPX

Для того чтобы компьютеры под управлением Windows-систем могли обращаться к NetWare, можно также использовать два типа драйверов, позволяющих работать с несколькими протоколами: Open Datalink Interface (ODI) и Network Driver Interface Specification (NDIS).

Когда в сети NetWare развернуты несколько протоколов (например, IPX/SPX и TCP/IP), серверы и клиенты зачастую используют драйвер *Open Datalink Interface, ODI* (открытый канальный интерфейс). Этот драйвер обеспечивает обмен данными с файл-серверами NetWare, мэйнфреймами и Мини-компьютерами, а также с Интернетом. ODI-драйверы можно применять в сетевых клиентах, работающих в среде MS-DOS и Microsoft Windows.

В ранних версиях Windows (Windows 3.11, Windows 95, Windows 98 и Windows NT) компания Microsoft реализовала GDI-драйвер как 1б-разрядное приложение, которое не могло в полной мере использовать быстродействие и возможности 32-разрядной системы Windows 95 и более поздних версий.

Начиная с Windows 95, для подключения к серверам NetWare по протоколу IPX/SPX применяются более совершенные решения компании Microsoft – протокол *NetWare Link (NWLink) IPX/SPX* и драйвер *Network Driver Interface Specification, NDIS* (спецификация стандартного интерфейса сетевых адаптеров). В практических заданиях 5-1 и 5-2 рассказывается о том, как настроить системы Windows 2000 и Windows XP Professional для работы с протоколом NWLink.

Как показано на рис. 5.3, драйверы NDIS (Microsoft) и ODI (Novell) работает на подуровне LLC Канального уровня, однако в отдельный момент времени к сетевому адаптеру может быть привязан только один из этих драйверов.

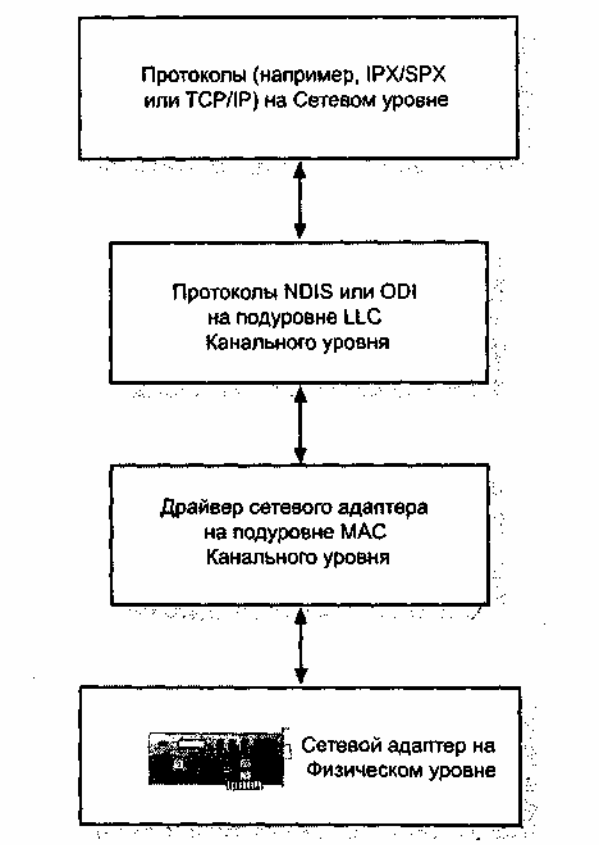


Рис. 5.3. Сетевая архитектура драйвера NDIS

Совет

На большинстве Windows-систем при конфигурировании протокола NWLink IPX/SPX по умолчанию устанавливается такой режим, когда операционная система автоматически распознает тип фрейма Ethernet, используемый в уже существующей сети. В последних системах Windows (например, Windows 2000 и Windows XP) при выборе ручной настройки и отмене автоматического распознавания система по умолчанию задает тип фрейма 802.2 (если вы сами не укажите другой тип).

Эмуляция IPX/SPX

Протокол NWLink эмулирует работу IPX/SPX, поэтому любая использующая его система Windows работает как компьютер или устройство, настроенное на работу с IPX/SPX. NDIS – это спецификация программного драйвера, используемая протоколом NWLink и позволяющая ему и другим сетевым протоколам взаимодействовать с сетевым адаптером компьютера. При этом используется процедура установления связи между протоколом и адаптером, называемая привязкой. *Привязка* (binding) некоторого протокола к определенному адаптеру позволяет этому адаптеру работать и обеспечивать интерфейс с сетевой средой.

Привязка к драйверу NDIS

Драйвер NDIS компании Microsoft может привязывать к одному сетевому адаптеру один или несколько протоколов, благодаря чему все эти протоколы смогут работать через данный адаптер. Если протоколов несколько, то между ними устанавливается определенная иерархия, и если в сети развернуто несколько протоколов, то сетевой адаптер в первую очередь попытается прочитать фрейм или пакет, используя протокол, находящийся на верхней ступени этот иерархии. Если форматирование фрейма или пакета соответствует другому протоколу, то адаптер попробует прочитать его с помощью следующего протокола, указанного в иерархии, и т. д.

Совет

С помощью драйвера NDIS один протокол можно привязать к нескольким сетевым адаптерам компьютера (например, в сервере). При наличии нескольких адаптеров можно распределить между

ними сетевую нагрузку и ускорить реакцию сервера на запросы при большом количестве пользователей. Кроме того, несколько адаптеров используются в том случае, если сервер также выполняет функции маршрутизатора. Привязка одного протокола к нескольким адаптерам позволяет также снизить объем занимаемой памяти, поскольку серверу не понадобится загружать в нее несколько экземпляров одного протокола.

Нужно заметить, что пользователь может сам организовывать иерархию протоколов, привязанных к адаптеру. Эта иерархия называется порядком привязки. Например, если первым в иерархии указан протокол IPX/SPX, а вторым – TCP/IP, то фрейм или пакет TCP/IP сначала интерпретируется как данные в формате IPX/SPX. Сетевой адаптер быстро определяет ошибку и повторно читает фрейм или пакет в формате TCP/IP, распознавая его правильно.

Порядок привязки протоколов можно задавать в большинстве операционных систем Microsoft Windows (например, в Windows 2000 и Windows XP). На рис. 5.4 изображен порядок привязки на компьютере, работающем под управлением Windows XP Professional. На этом рисунке протоколы, перечисления ниже строки **File and Printer Sharing for Microsoft Networks,** отображают nil док привязки протоколов, используемых для доступа к общим файлам и принтерам. Под строкой **Client for Microsoft Networks** показан порядок привязки протоколов, необходимых для доступа к сетевым серверам. В практических заданиях 5-3 и 5-4 вы узнаете о том, как установить порядок привязки протоколов в системах Windows 2000 и Windows XP Professional.

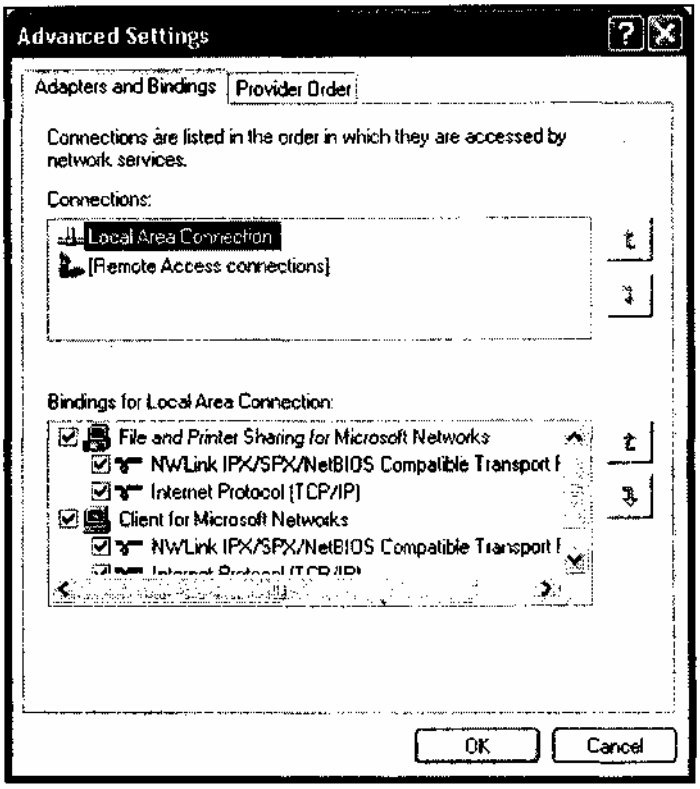


Рис. 5.4. Порядок привязки протоколов к сетевому адаптеру в системе Windows XP Professional

Другие протоколы, используемые вместе с серверами NetWare

Помимо IPX/SPX, операционная система Novell NetWare допускает использование и некоторых других протоколов при решении определенных задач (например, протокол RIP позволяет собирать информацию о маршрутизации; см. *главу 4).* Серверы NetWare можно настроить для работы в качестве маршрутизаторов, которые будут применять протокол RIP для обновления таблиц маршрутизации (впрочем, при этом необходимы также ручные настройки, выполняемые сетевым администратором, отвечающим за маршрутизацию). В табл. 5,2 перечислены протоколы, которые можно использовать в серверах NetWare.

Примечание

Как уже говорилось ранее в этой книге, не рекомендуется включать протокол RIP на серверах NetWare и Windows 2000/Server 2003, поскольку он создает в сети дополнительный трафик. Предпочтительнее, чтобы все задачи по маршрутизации выполняли специализированные сетевые маршрутизаторы.

Таблица 5.2. *Протоколы, используемые вместе с серверами NetWare*

Аббревиатура	**Полное название**	**Описание**	**Уровень модели OSI**
IPX	Internetwork Packet Exchange	Используется как основной протокол передачи данных для приложений Ethernet. Можно применять любые типы фреймов: Ethernet 802.2, Ethernet 802.3, Ethernet II и Ethernet SNAP	Сетевой и Транспортный
LSL	Link Support Layer	Используется вместе с ODI-драйвером для поддержки нескольких протоколов на одном сетевом адаптере	Канальный
MLID	Multiple Link Interface Driver	Соединяет два или несколько каналов в одну телекоммуникационную линию (например, два терминальных адаптера ISDN). В сетях Ethernet протокол MLID в сочетании с сетевым адаптером рабочей станции позволяет определить уровень конфликтов в сети, в сетях с маркерным кольцом он координирует передачи маркера	Канальный (подуровень MAC)
NCP	NetWare Core Protocol	Часть операционной системы, обеспечивает обмен данными между клиентами и серверами при обращении к приложениям или открытым файлам, находящимся на сервере NetWare	Сеансовый, Представительский и Прикладной
NLSP	NetWare Link Services Protocol	Обеспечивает пакеты IPX информацией о маршрутизации	Сетевой
RIP	Routing Information Protocol	Собирает информацию о маршрутизации для серверов, которые обеспечивают работу служб маршрутизации	Сетевой
SAP	Service Advertising Protocol	Позволяет клиентам NetWare идентифицировать серверы и сетевые службы, имеющиеся на них. Серверы генерируют широковещательные пакеты SAP каждые 60 с, а клиенты используют их для обнаружения ближайшего	Сеансовый Представительский Прикладной

Аббревиатура	Полное название	Описание	Уровень модели OSI
		сервера	
SPX	Sequenced Packet Exchange	Предоставляет прикладным программам механизм передачи данных, ориентированный на соединения	Транспортный

Протокол NetBEUI и серверы Microsoft Windows

Система Microsoft Windows NT начиналась как совместный проект компаний Microsoft и IBM по развитию серверной операционной системы LAN Manager. В начале 1990-х годов компания Microsoft перешла от LAN Manager к системе Windows NT Server, которая впоследствии стала широко распространенной операционной системой.

На основе продукта Windows NT Server были созданы системы Windows 2000 Server и Windows Server 2003. Как и современные версии Novell NetWare системы Windows NT, Windows 2000 и Windows Server 2003 совместимы локальными сетями Ethernet и Token Ring, они могут масштабироваться от небольших компьютеров с Intel-совместимыми процессорами до многопроцессорных систем. Чаще всего с указанными системами используются протоколы TCP/IP, однако до сих пор имеются системы Windows NT Server версий 3.51 и 4.0, в которых реализован родной протокол систем Windows NT – *NetBIOS Extended User Interface, NetBEUI.* Этот протокол был создан для операционных систем LAN Manager и LAN Server до того, как появилась Windows NT. NetBEUI был реализован в первых версиях Windows NT до сих пор имеется в системе Windows 2000 (хотя больше и не поддерживается в системах Microsoft, начиная с Windows XP).

Примечание

На компьютерах под управлением Windows NT и Windows 2000 протокол NetBEUI также встречается под именем NBF (NetBEUI frame – фрейм NetBEUI). Если для анализа сетевого трафика использовать анализатор протоколов, то фреймы NetBEUI будут отмечены именно такой аббревиатурой.

История NetBEUI

Протокол NetBEUI первоначально был разработан компанией IBM в 1985 году как улучшенная модификация *Network Basic Input/Output System, NetBIOS* (базовая сетевая система ввода/вывода). NetBIOS – это не протокол, а метод взаимодействия прикладных программ с сетевыми устройствами, а также службы распознавания имен, используемых в сетях Microsoft. NetBIOS-имена даются различным объектам сети (таким как рабочие станции, серверы или принтеры). Например, имя пользователя может служить для идентификации его рабочей станции в сети, по имени HPLaser может осуществляться доступ к сетевому принтеру, а сервер может иметь имя AccountServer. Подобные имена облегчают поиск нужных сетевых ресурсов. Они транслируются (преобразуются) в адреса, используемые в сетевых коммуникациях, с помощью NetBIOS-служб Name Query.

Область применения NetBEUI

Протокол NetBEUI разрабатывался в то время, когда компьютерные сети в первую очередь означали локальные сети для относительно небольшого количества компьютеров (от нескольких до двух сотен). В процессе проектирования не учитывались особенности корпоративных сетей с маршрутизацией пакетов. По этой причине протокол NetBEUI нельзя маршрутизировать и лучше всего его применять в небольших локальных сетях под управлением относительно старых операционных систем компаний Microsoft и IBM:

- Microsoft Windows 3.1 или 3.11;
- Microsoft Windows 95;
- Microsoft Windows 98;
- Microsoft LAN Manager;

- Microsoft LAN Manager for UNIX;
- Microsoft Windows NT 3.51 или 4.0
- IBM PCLAN;
- IBM LAN Server.

При переводе сети с Windows NT Server на Windows 2000 или Windows Server 2003 в первую очередь настройте серверы и рабочие станции, использующие NetBEUI, на работу с TCP/IP. Хотя системы Windows 2000 и поддерживают NetBEUI, компания Microsoft не рекомендует применять этот протокол более поздних операционных системах. Однако в том случае, если сеть небольшая (менее 50 клиентов) и не требуется доступ к Интернету, то протокол NetBEUI может оказаться более эффективным, чем TCP/IP.

NetBEUI и эталонная модель OSI

Протокол NetBEUI соответствует нескольким уровням модели OSI .Для взаимодействия сетевых интерфейсов используются Физический и Канальный уровни. В пределах Канального уровня для управления передачей кодирования и адресации фреймов задействуются подуровни LLC (Logical Link Control) и MAC (Media Access Control). Также протокол реализует функции, относящиеся к Транспортному и Сеансовому уровням (обеспечение надежности передачи, подтверждение приема пакетов, установка и завершения сеансов).

Почему NetBEUI хорошо работает в сетях Microsoft

Для ответа на вопрос, вынесенный в заголовок раздела, имеется несколько причин. Во-первых, протокол NetBEUI прост в установке, поскольку его не нужно конфигурировать как другие протоколы (например, для TCP/IP нужно указать адрес, а для IPX/SPX следует выбрать тип фрейма). Во-вторых протокол позволяет одновременно поддерживать в сети большое количество сеансов обмена информацией (до 254 в ранних версиях протокола, в предыдущих версиях это ограничение снято). Например, в соответствии со спецификациями Microsoft сервер Windows NT может обеспечивать работу 1000 сеансов на один сетевой адаптер (для серверов Windows 2000 такие проверки проводились). В-третьих, протокол NetBEUI расходует мало оперативной памяти и имеет высокое быстродействие в небольших сетях. В-четвертых в нем реализованы надежные механизмы обнаружения и устранения ошибок.

Недостатки NetBEUI

Невозможность маршрутизации является главным недостатком протокола NetBEUI в средних и крупных сетях, включая корпоративные сети. Маршрутизаторы не могут перенаправить пакет NetBEUI из одной сети другую, поскольку фрейм NetBEUI не содержит информации, указующие на конкретные подсети. Еще одним недостатком протокола является то, что для него имеется мало сетевых анализаторов (помимо тех инструментов, которые выпустила Microsoft).

> **Примечание**
>
> В практическом задании 5-5 рассказывается о том, как установить протокол NetBEUI на компьютере под управлением Windows 2000.

Протокол AppleTalk и система Mac OS

Компания Apple разработала семейство протоколов *AppleTalk* для организации сетей на базе компьютеров Macintosh, работающих под управлением операционной системы Mac OS. AppleTalk – это одноранговый сетевой протокол, т. е. он предназначен для обмена данными между рабочими станциями Macintosh даже при отсутствии сервера. Этот факт иллюстрируется на рис. 5.5, где показано, как для связи компьютеров Macintosh используется коммутатор. С протоколом AppleTalk могут работать операционные системы Novell NetWare, MS-DOS, Microsoft Windows *9x/ME* и Windows NT/2000/XP. Первая версия протокола называлась AppleTalk Phase I, она была выпущена в 1983 году. В 1989 году была разработана используемая до сих пор версия AppleTalk Phase II, которая позволяет работать большому количеству сетевых компьютеров и обеспечивает взаимодействие с большими гетерогенными сетями на основе нескольких протоколов.

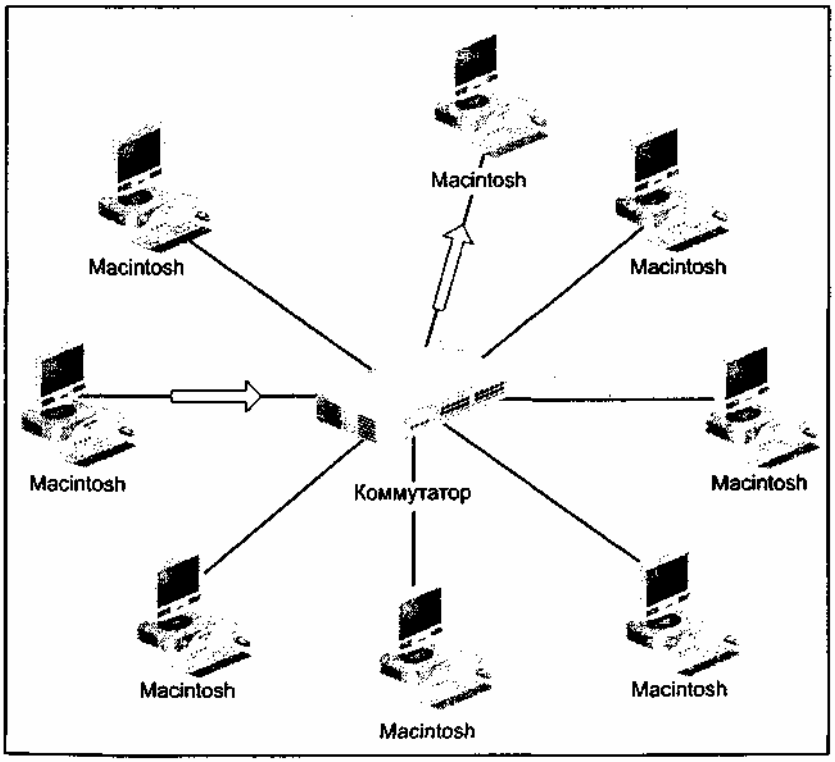


Рис. 5.5. Одноранговая сеть без сервера на основе протокола AppleTalk

Сравнение версий AppleTalk Phase I и AppleTalk Phase II

Между двумя этими версиями имеется несколько важных различий. Протокол AppleTalk Phase I не позволяет организовывать взаимодействие сетей (т. е. связывать несколько сетей вместе) и, следовательно, допускает только одну зону. Протокол AppleTalk Phase II не имеет этого недостатка и разрешает использование до 255 зон.

> **Совет**
>
> Зона (zone) – это группа компьютеров Macintosh в нескольких сетях, позволяющая упростить организацию совместного доступа к ресурсам, а также управление сетью. Нередко деление на зоны соответствует территориальному расположению компьютеров.

Максимальное количество станций в сети AppleTalk Phase I равно 254, а для сети AppleTalk Phase II этот параметр равен нескольким миллионам. Адресация в сетях первого типа осуществляется с применением идентификации узла (node identification, ID), а в сетях второго типа при адресации исполняется как идентификатор узла, так и идентификатор сети. И последним отличием является то, что протокол AppleTalk Phase I может работать только в таких сетях, где других протоколов нет. Протокол AppleTalk Phase II функционирует в сетях со многими протоколами (например, IPX/SPX и TCP/IP).

> **Примечание**
>
> Хотя протокол AppleTalk был разработан как одноранговый, он может применяться для обмена данными между серверами Mac OS X и Windows-системами настроенными на работу по этому протоколу.

Службы AppleTalk

В состав протокола AppleTalk входят три базовые службы:

- удаленный доступ к сетевым файлам с использованием программ средств AppleShare File Server (в сочетании с протоколом AppleTalk Filing Protocol);
- службы печати на основе программных средств AppleShare Print Server (которые используют

протоколы Name Binding Protocol и Printer Access Protocol);

- файловые службы на базе программ AppleShare PC для DOS- и Windows систем.

AppleTalk и эталонная модель OSI

В стеке AppleTalk исходным протоколом нижнего уровня (согласно модели OSI) является протокол *LocalTalk Link Access Protocol, LLAP,* работающий на физическом и Канальном уровнях и обеспечивающий устаревший метод доступа при передаче данных. При этом используются физические сетевые интерфейсы, разработанные для протокола LocalTalk, который может работать в небольших, медленных сетях при максимальном количестве станций в сети, равном 32 (для 300-метрового сегмента с шинной топологией). Допустимая скорость равна 230,4 Кбит/с, что чрезвычайно мало для современных сетевых технологий.

Для назначения адресов в сети LocalTalk используется процесс, называемый состязанием. После включения питания компьютер Macintosh "соревнуется" с другими компьютерами за свой адрес, в результате чего он получает уникальный идентификатор узла (ID). При последующих включениях питания компьютер может получить другой адрес.

Методы доступа AppleTalk

В современных сетях AppleTalk Phase II применяются методы доступа Ethernet или маркерное кольцо, при этом могут использоваться интерфейсы, подходящие для любых других устройств Ethernet или Token Ring. Для упрощения Ethernet-коммуникацией в стеке AppleTalk имеется протокол *EtherTalk Link Access Protocol, FLAP,* функционирующий на Физическом и Канальном уровнях. С его помощью в сетях AppleTalk с шинной или смешанной топологией реализуется метод доступа CSMA/CD *(см. главу 2).* В сетях с маркерным кольцом используется протокол *Token Talk Link Access Protocol, TLAP,* также работающий на Физическом и Канальном уровнях. При этом используется передача маркера и кольцевая/звездообразная топология (как и в любой другой сети с маркерным кольцом).

Сетевая адресация AppleTalk

Адресация в сетях AppleTalk, использующих протокол ELAP и TLAP, осуществляется с помощью протокола *AppleTalk Address Resolution Protocol, AARP,* который позволяет распознавать физические или MAC-адреса сетевых адаптеров, благодаря чему эти адреса можно вставлять во фреймы AppleTalk. (Если компьютер Macintosh настроен на работу с AppleTalk и IP, протокол AARP используется для распознавания физических и IP-адресов.)

Протоколы, входящие в стек AppleTalk

Помимо LLAP, ELAP, TLAP и AARP, имеются и другие протоколы, входящие в семейство AppleTalk. Все они перечислены в табл. 5.3.

Таблица 5.3. *Протоколы, входящие в стек Apple*

Аббревиатура	Полное название	Описание	Уровень модели OSI
AARP	AppleTalk Address Resolution Protocol	Используется для распознавания физических (MAC) адресов в сетях Ethernet и Token Ring. Если помимо AppleTalk применяется протокол IP, то AARP выполняет разрешение компьютерных и доменных имен в IP-адреса	Канальный и Сетевой
ADSP	AppleTalk Data Stream Protocol	Обеспечивает гарантированную передачу потоков данных в принимающем узле	Сеансовый
AFP	AppleTalk Filing Protocol	Позволяет рабочим станциям и серверам взаимодействовать друг с другом на Прикладном уровне	Представительский
ASP	AppleTalk Session Protocol	Инициирует, поддерживает и закрывает соединения между станциями.	Сеансовый

Аббревиатура	Полное название	Описание	Уровень модели OSI
		Определяет порядок передачи фрагментов данных для надежной доставки принимающему узлу	
ATP	AppleTalk Transaction Protocol	Обеспечивает надежный обмен данными между двумя узлами, для чего каждой транзакции назначается номер соединения	Транспортный
DDP	Datagram Delivery Protocol	Используется для доставки и маршрутизации данных между двумя взаимодействующими станциями	Сетевой
ELAP	EtherTalk Link Access Protocol	Обеспечивает Ethernet-коммуникации с применением метода доступа CSMA/CD в шинных или смешанных топологиях	Физический и Канальный
LLAP	LocalTalk Link Access Protocol	Устаревший метод доступа, управляющий коммуникациями на Физическом (через интерфейсы и кабели) и Канальном уровнях в определенных ситуациях (например, когда для обеспечения адресации возникают состязания за получение уникального ID)	Физический и Канальный
NBP	Name Binding Protocol	Управляет именами компьютеров и регистрацией IP-адресов, позволяя клиентам связывать сетевые службы и процессы с определенными именами компьютеров	Транспортный
PAP	Printer Access Protocol	Открывает и закрывает коммуникационные сеансы и обеспечивает передачу данных по сети для служб печати	Сеансовый
RTMP	Routing Table Maintenance Protocol	Используется для получения информации о сетевой маршрутизации при обновлении таблиц маршрутизации	Сетевой
TLAP	TokenTalk Link Access Protocol	Обеспечивает работу маркерных сетей с кольцевой/звездообразной топологией	Физический и Канальный
ZIP	Zone Information Protocol	Поддерживает таблицу зон, на которые делятся сети AppleTalk и соответствующие им таблицы маршрутизации	Сеансовый

Совместимость AppleTalk с системами Mac OS X, Windows 2000 и Netware

Родной серверной платформой для компьютеров Macintosh является продукт Mac OS X Server, созданный на базе операционной системы Mac OS X. С его помощью можно реализовать общий доступ к файлам и принтерам, управление сетевыми пользователями и группами, а также обеспечить работу веб-служб. Системы Mac OS X и Mac OS X Server поддерживают и AppleTalk, и TCP/IP.

Сервер NetWare или Windows 2000 можно использовать в качестве сервера Для компьютеров Macintosh при наличии протокола AppleTalk Phase II. Например, для того, чтобы сервер Windows 2000

можно было установить в компьютерной сети Macintosh, на него следует поставить следующие компоненты:

- AppleTalk Phase II;
- File Services for Macintosh;
- Print Services for Macintosh.

После установки протокола AppleTalk система Windows 2000 Server сможет взаимодействовать с компьютерами Macintosh, настроенными на работу с AppleTalk Phase II. Наличие служб File Services for Macintosh позволяет выделить на сервере Windows 2000 дисковое пространство, на котором компьютеры Macintosh смогут хранить файлы, используя для доступа протокол AppleTalk. Службы Print Services for Macintosh позволяют компьютерам Macintosh обращаться к сетевым принтерам, работу которых обеспечим сервер Windows 2000.

Практическое задание 5-6 познакомит вас с тем, как в системе Windows 2000 Server установить протокол AppleTalk Phase II, а также службы File Services for Macintosh и Print Services for Macintosh.

Примечание

Операционные системы Mac OS X и Mac OS X Server реализованы на ядре UNIX и даже имеют режим окна терминала, в котором можно выполнять многочисленные команды UNIX.

Протокол TCP/IP и различные серверные системы

Transmission Control Protocol/Internet Protocol, TCP/IP (Протокол управления передачей/Протокол Интернета) – самый распространенный в настоящее время стек протоколов, являющийся к тому же протоколом Интернета. В этом разделе дается лишь краткий обзор TCP/IP в контексте общего знакомства с важнейшими протоколами. Более подробно стек TCP/IP рассматривается в *главе 6.*

Большинство операционных систем сетевых серверов и рабочих станций поддерживает TCP/IP, в том числе серверы NetWare, все системы Windows, UNIX, последние версии Mac OS, системы OpenMVS и z/OS компании IBM, а также OpenVMS компании DEC. Кроме того, производители сетевого оборудования создают собственное системное программное обеспечение для TCP/IP, включая средства повышения производительности устройств. Стек TCP/IP изначально применялся на UNIX-системах, а затем быстро распространился на многие другие типы сетей.

Достоинства TCP/IP

Среди многих достоинств стека TCP/IP можно упомянуть следующие:

- он применяется во многих сетях и в Интернете, что делает его международным языком сетевых коммуникаций;
- имеется множество сетевых устройств, предназначенных для работы с этим протоколом;
- многие современные компьютерные операционные системы используют TCP/IP в качестве основного протокола;
- для *этого* протокола существует много диагностических средств и анализаторов;
- многие специалисты по сетям знакомы с протоколом и умеют его использовать.

Протоколы и приложения, входящие в стек TCP/IP

В табл. 5.4 перечислены протоколы и приложения, входящие в стек TCP/IP. О некоторых из них уже рассказывалось ранее. Более подробное описание имеется в *главе 6,* а также и в последующих главах.

Таблица 5.4. *Протоколы и приложения, входящие в стек протоколов TCP/IP*

Аббревиатура	Полное название	Описание	Уровень модели OSI
ARP	Address Resolution Protocol	Обеспечивает разрешение IP-адресов в MAC-адреса	Канальный и Сетевой
DNS	Domain Name System (приложение)	Поддерживает таблицы, связывающие IP-адреса компьютеров с их именами	Транспортный
FTP	File Transfer Protocol	Используется для передачи и приема файлов	Сеансовый, Представительский

Аббревиатура	Полное название	Описание	Уровень модели OSI
			и Прикладной
HTTP	Hypertext Transfer Protocol	Используется для передачи данных в сети World Wide Web	Представительский
ICMP	Internet Control Message Protocol	Используется для генерирования отчетов об ошибках в сети, в частности, при передаче данных через маршрутизаторы	Сетевой
IP	Internet Protocol	Управляет логической адресацией	Сетевой
NFS	Network File System (приложение)	Используется для передачи файлов по сети (предназначается для компьютеров UNIX)	Сеансовый, Представительский и Прикладной
OSPF	Open Shortest Path First (протокол)	Используется маршрутизаторами для обмена информацией (данными по маршрутизации)	Сетевой
PPP	Point-to-Point protocol	Используется как протокол уда ленного доступа в сочетании с технологиями глобальных сетей	Сетевой
RIP	Routing Information Protocol	Используется при сборе данных по маршрутизации для обновления таблиц маршрутизации	Сетевой
RPC	Remote Procedure Call (приложение)	Позволяет удаленному компьютеру выполнять процедуры на другом компьютере (например, на сервере)	Сеансовый
SLIP	Serial Line Internet Protocol	Используется как протокол удаленного доступа в сочетании с технологиями глобальных сетей	Сетевой
SMTP	Simple Mail Transfer Protocol	Используется для передачи электронной почты	Представительский
TCP	Transmission Control Protocol	Протокол, ориентированный на установление соединений, что повышает надежность передачи данных	Транспортный
Telnet	Telecommunications Network (приложение)	Позволяет рабочей станции эмулировать терминал и подключаться к мэйнфреймам, серверам Интернета и маршрутизаторам	Сеансовый, Представительский и Прикладной
UDP	User Data Protocol	Протокол без установления соединений; используется как альтернатива TCP в тех случаях, когда не требуется	Транспортный

Аббревиатура	Полное название	Описание	Уровень модели OSI
		высокая надежность	

Протокол SNA и операционные системы IBM

В устаревших мэйнфреймах IBM обычно используются протоколы стека *Systems Network Architecture, SNA,* который был изначально разработан в 1974 году. Фактически SNA – это набор частных протоколов, в которых в качестве метода доступа используется маркерное кольцо. Многие детали маркерных сетей, созданных компанией IBM, впоследствии были включены в стандарт IEEE 802.5. Однако в сети SNA кабельный участок обязательно строится на базе экранированной витой пары (STP), причем кабели имеют строго ориентированную маркировку (и разводку) (например, определенный конец кабеля должен идти к мэйнфрейму, а другой – к устройствам, подключенным к мэйнфрейму, таким как контроллеры дисковых накопителей или коммуникационных каналов). Это означает, что в сети SNA также используются частные (фирменные) кабельные разъемы и сетевые интерфейсы,

Стек протоколов SNA и эталонная модель OSI

Стек протоколов SNA базируется на семиуровневой модели (табл. 5.5), напоминающей эталонную модель OSI.

Таблица 5.5. *Семиуровневая модель SNA*

Уровень SNA	Эквивалентный уровень OSI	Назначение
Службы транзакций (Transaction Services)	Прикладной	Самый высокий уровень, управляет службами, от которых зависит работа прикладных программ (например, распределенных баз данных и приложений, выполняющихся одновременно на нескольких мэйнфреймах)
Представитель-ские службы (Presentation Services)	Представитель-ский	Управляет форматированием и преобразованием данных (например, перекодировкой из ASCII в EBCDIC и наоборот), также выполняет сжатие данных (хотя, в отличие от Представительского уровня OSI, этот уровень не обеспечивает шифрование данных)
Управление потоком данных (Data Flow Control)	Сеансовый	Устанавливает и поддерживает коммуникационные каналы между узлами, управляет потоками данных и обеспечивает восстановление после коммуникационных ошибок
Управление (Transmission Control)	Транспортный	Обеспечивает надежность передачи данных передачей от исходного узла к принимающему, а так же управляет шифрованием данных
Управление маршрутом (Path Control)	Сетевой	Управляет маршрутизацией и созданием виртуальных каналов, фрагментирует сообщения на блоки меньших размеров при передаче данных через разнородные сети (эту задачу выполняет Транспортный уровень OSI)
Управление(Data	Канальный каналом	Форматирует данные на фреймы,

Уровень SNA	Эквивалентный уровень OSI	Назначение
Link Control)		обеспечивает маркерный доступ к сети при одноуровневых обменах данными между компьютерами
Управление Физическим Устройством (Physical Control)	Физический	Обеспечивает генерирование и кодирование электрических сигналов, работу физических интерфейсов, топологию сети и коммуникационную среду (например, кабель)

Достоинства и недостатки SNA

Аналогично любому стеку протоколов, SNA имеет как достоинства, так и недостатки. Отмечая достоинства, следует сказать, что архитектура SNA существует уже более четверти века и обеспечивает надежные и проверенные средства обмена данными с системами IBM. Существенным недостатком является то, что SNA – это частный (фирменный) стек протоколов, для которого нужны специальные устройства и дополнительное обучение процедурам конфигурирования, управления и отладки. По этим причинам сети SNA с мэйнфреймами IBM обычно работают очень хорошо, но это требует больших затрат на обучение персонала и поддержку сети.

Физические элементы сети SNA

В традиционной сети SNA с компьютерами IBM терминалы рассматривав как физические модули типа 2 (type 2). Физический модуль – это некоторое устройство, которое может подключаться к мэйнфрейму или управлять доступом к нему.

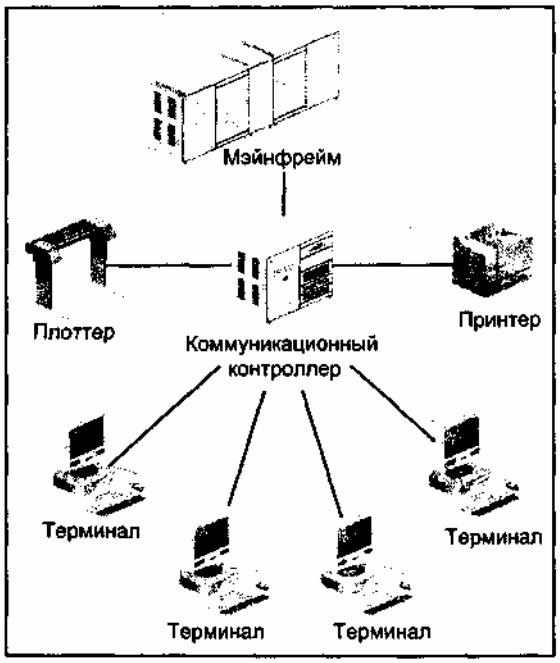


Рис. 5.6. Физические модули, подключенные к мэйнфрейму в сети SNA

К физическим модулям типа 2 относятся как терминалы, так и принтеры. Более сложные физические модули, обменивающиеся данными с мэйнфреймом, относятся к типу 2.1. В их число входят шлюзы (например, устройства, подключающие компьютеры с протоколом TCP/IP к мэйнфрейму IBM, работающему с SNA), мини-компьютеры и устройства, называемые контроллерами кластеров и позволяющие нескольким мэйнфреймам работать в тандеме. Терминалы и принтеры подключаются к физическим модулям типа 4, представляющим собой коммуникационные контроллеры, которые непосредственно соединены с мэйнфреймом и управляют

трафиком обращений к нему (рис. 5.6).

Протоколы и приложения, работающие в стеке SNA

В табл. 5.6 перечислено множество протоколов и приложений, входящих в стек SNA.

Таблица 5.6. *Протоколы и приложения, входящие в стек протоколов SNA*

Аббревиатура или название	Полное название	Описание	Уровень модели SNA
APPN	Advanced Peer-to-Peer Networking (улучшенный протокол одноранговых сетей)	Обеспечивает одноранговые взаимодействия между устройствами, такими как мэйнфреймы, миникомпьютеры, шлюзы и контроллеры кластеров	Управление передачей
CICS	Customer Information Control System (абонентская информационно управляющая система)	Программная среда, предоставляющая программистам базовые средства взаимодействия с архитектурой SNA (в том числе безопасный доступ, управление файлами и накопителями). Альтернативой IMS является CICS	Управление потоком данных и Предста-вительские службы
DDM	Distributed Data Management (управление распределен-ными данными)	Программы, обеспечивающие удаленный доступ к информации, хранящейся на мэйнфреймах IBM (например, по удаленному подключению со стороны другого мэйнфрейма, находящегося в удалении)	Службы транзакций
IMS	Information Management System (информационно - управляющая система)	Программная среда, предоставляющая программистам базовые средства взаимодействия с архитектурой SNA (в том числе безопасный доступ, управление файлами и накопителями). Альтернативой IMS является CICS	Управление потоком данных Предста-вительские службы
NCP	Network Control Program (программа управления сетью)	Обеспечивает адресацию физических устройств и дополнительную логическую адресацию, а также маршрутизацию. Используется для шлюзовых коммуникаций SNA и управления ими (должна устанавливаться на любом шлюзе SNA для того, чтобы рабочие станции могли обращаться через шлюз к мэйнфрейму; см. *главы 1* и 4, где шлюзы рассматриваются	Управление каналом и Управление маршрутом

Аббревиа-тура или название	Полное название	Описание	Уровень модели SNA
		подробнее)	
SDLC	Synchronous Data Link Control (синхронное управление передачей данных)	Создает логические соединения (виртуальные каналы) в сетевом кабеле и координирует передачу данных по этим соединениям обеспечивает в каналах полудуплексную и полнодуплексную связь	Управление физическим устройством и Управление каналом
SNADS	SNA Distributed Services (распределенные службы SNA)	Программные средства, управляющие передачей документов. Используются системами электронной почты для передачи сообщений по указанным адресам	Службы транзакций
SSCP	System Services Control Point (точка управления системными службами)	Программное обеспечение, управляющее VTAM	Управлений передачей
Token Ring	Token Ring	Метод доступа, используемый сетях SNA	Управление физическим устройством Управление каналом
VTAM	Virtual Telecommuni-cations Access Method (виртуальный телекоммуника-ционный метод доступа)	Управляет передачей данных в сети SNA (например, с помощью методов управления потоками). Обеспечивает обмен цифровыми данными	Управление передачей

Протокол DLC для доступа к операционным системам IBM

Если для доступа к мэйнфрейму, работающему с SNA, используются компьютеры под управлением Windows *9x,* Windows NT и Windows 2000, то альтернативой SNA-шлюзу является установка протокола *Data Link Control, DLC.* Этот протокол эмулирует SNA, и он может также применяться для подключения к некоторым устаревшим моделям сетевых принтеров, которые могут работать только с ним (например, старые принтеры Hewlett-Packard).

> **Совет**
>
> Протокол DLC не поддерживается в Windows XP. Если вы рассматриваете возможность перехода на эту систему, то учтите, что с ней вы не сможете использовать DLC для доступа к мэйнфреймам IBM и, возможно, вам потребуется SNA-шлюз.

В основном протокол DLC является альтернативой TCP/IP в тех случаях, когда некоторый хост использует SNA-коммуникации. Недостатком этого протокола является то, что он не маршрутизируется. Кроме того, он на самом деле не предназначен для одноранговых взаимодействий между рабочими станциями, а служит только для подключения к старым

мэйнфреймам IBM (например, ES9000) или мини-компьютерам IBM (например, AS/400). В практическом задании 5-7 рассказывается о том, как установить DLC в системе Windows 2000.

Протокол DNA для операционных систем компьютеров Digital (Compaq)

Созданная в 1974 году архитектура *Digital Network Architecture (DNA)* имеет такой же возраст, что и SNA. DNA использовалась в первых сетях компании Digital Equipment Corporation (DEC) и по-другому называлась DECnet. Затем этот стек протоколов применялся значительно реже.

Архитектура DNA предусматривает использование фреймов Ethernet II (или DIX – аббревиатура от названий компаний-разработчиков Digital, Intel и Xerox) в шинной топологии. Одним из достоинств DNA является то, что с самого начала эта архитектура близко следовала эталонной модели OSI. Не-Достаток DNA – то, что эта архитектура частная. Кроме того, после приобретения фирмы DEC компанией Compaq оригинальные компьютеры DEC и сети DNA стали менее популярными. Даже некогда известные компьютеры ча базе процессора DEC Alpha все чаще заменяются продаваемыми под маркой Compaq рабочими станциями и серверами, реализованными с использованием процессоров Intel Itanium.

Поскольку DNA все реже встречается в сетях, уменьшается вероятность того, что вы столкнетесь с этой архитектурой на практике. Однако для общего представления в табл. 5.7 перечислены некоторые из протоколов и приложений, образующих стек DNA.

Таблица 5.7. *Протоколы и приложения, входящие в стек протоколов*

Аббревиатура	Полное название	Описание	Уровень модели OSI
CLNS	Connectionless-Mode Network Service (сетевая служба без установления соединения)	Обеспечивает работу служб без установления соединения *(см. главу 2),* а также маршрутизации	Сетевой
CONS	Connection Oriented Network Service (сетевая служба с установлением соединения)	Обеспечивает работу служб с установлением соединения для маршрутизации и контроля за ошибками маршрутизации	Сетевой
DDCMP	Digital Data Communications Message Protocol (протокол сообщений передачи цифровых данных)	Обеспечивает работу служб с установлением соединения и контролем ошибок. На уровне электрических сигналов позволяет осуществлять полудуплексную и полнодуплексную связь	Физический Канальный(подуровень LLC)
FTAM	File Transfer, Access, and Management (передача файлов, доступ и управление)	Позволяет передавать файлы с текстовым и двоичным содержимым	Прикладной
HDLC	High-Level Data Link Control (высокоуровневое управление каналом)	Создает логические соединения (виртуальные каналы) в сетевом кабеле и координирует передачу данных между ними. Управляет форматированием фреймов	Физический и Канальный
MAILbus	MAILbus	Соответствует стандарту X.400 на почтовые службы	Прикладной
Naming Service	Naming Service (служба имен)	Предоставляет сетевым устройствам службы именования, преобразующие адрес устройства в его имя и наоборот (что упрощает пользователям работу с устройствами)	Прикладной

Аббревиатура	Полное название	Описание	Уровень модели OSI
NVTS	Network Virtual Terminal (служба сетевых виртуальных терминалов)	Транслирует символы между Service терминалами, сетями DNA и хост-компьютерами	Представительский и Прикладной

Повышение производительности локальных сетей

Проще всего повысить производительность сети, если уменьшить количество протоколов, передаваемых через каждый маршрутизатор. При этом уменьшается рабочая нагрузка на маршрутизаторы, что позволяет им быстрее обрабатывать сетевой трафик. При меньшем количестве протоколов уменьшается и ненужный трафик, создаваемый в сети.

Вопросы для обсуждения

При выборе протоколов, используемых в сети, рассмотрите следующие вопросы.

- Должны ли пакеты маршрутизироваться?
- Какого размера сеть – маленькая (менее 100 узлов), средняя (100 – 500 узлов) или крупная (свыше 500 узлов)?
- Какие серверы используются и какие протоколы для них нужны?
- Имеются ли мэйнфреймы и какие протоколы для них требуются?
- Имеется ли непосредственный выход в Интернет или подключение к интранет-приложениям, использующим веб-технологии (виртуальная частная сеть)?
- Какая скорость требуется для подключений к глобальной сети?
- Имеются ли ответственные приложения?

Если фреймы нужно маршрутизировать (например, в корпоративной сети), то лучше всего применять протокол TCP/IP, поскольку он ориентирован на маршрутизацию и распространен во многих сетях. Для маленьких и средних немаршрутизируемых сетей (менее 200 узлов) на базе серверов Windows NT и при условии отсутствия подключения к Интернету наилучшим выбором остается протокол NetBEUI, обеспечивающий быстрые и надежные коммуникации. В сетях NetWare (с серверами версий ниже 5.0) можно использовать IPX/SPX, хотя в смешанной сети, где имеются старые серверы NetWare и новые серверы Windows 2000, могут понадобиться протоколы IPX/SPX и TCP/IP. Протокол NWLink является хорошим средством для подключения систем Windows 9x/NT/2000 к старым серверам NetWare.

Проблема каналов связи

Наличие подключения к Интернету или веб-службам требует развертывания Протокола TCP/IP, при этом службы FTP могут использоваться для передачи файлов. Также протокол TCP/IP лучше всего применять для связи с со временными мэйнфреймами и компьютерами UNIX, поскольку для подключения к мэйнфрейму или к приложению, работающему на компьютере UNIX, может потребоваться эмуляция терминала по протоколу Telnet. Для подключения к мэйнфреймам IBM и мини-компьютерам (если они работа ют в среде SNA) можно также использовать протокол DLC. И, наконец, протокол DNA по-прежнему может понадобиться в сети, где имеются старые компьютеры DEC (например, DEC VAX).

Примечание

TCP/IP – наилучший протокол для средних и крупных сетей. Он может маршрутизироваться, обладает надежностью для ответственных приложения имеет надежный механизм контроля ошибок. В таких сетях важно иметь средства мониторинга сети и анализа неисправностей. Как изложено в *главе* 6, стек TCP/IP имеет протоколы, необходимые для решения подобных задач.

Во многих случаях для разных сетевых приложений нужно использовать различные протоколы

локальных сетей. Иногда в современных сетях в любых сочетаниях применяются протоколы TCP/IP, NetBEUI, IPX/SPX, SM и даже DNA. Как вы уже знаете, развернутые протоколы связаны с типом используемых операционных систем. Также на их выбор влияет наличие связи с глобальными сетями (например, для выхода в Интернет нужен протокол TCP/IP, который может также потребоваться для связи локальных сетей между собой через глобальную сеть). Если, скажем, TCP/IP используется серверами в одной локальной сети, а рабочие станции из другой сети должны обращаться к этим серверам, то обе локальные сети и связывающая их глобальная сеть должны обеспечивать передачу протокола TCP/IP.

Удаление ненужных протоколов

Иногда рабочие станции в сети остаются настроенными на использование нескольких протоколов даже после того как все хосты и серверы переведены на протокол TCP/IP. В этом случае легко можно повысить производительность сети, удалив с рабочих станций ненужные протоколы. В практическом задании 5-8 рассказывается, как удалить протокол DLC из системе Windows 2000, а в задании 5-9 вы узнаете, как удалить службу Client Service for NetWare (и протокол NWLink IPX/SPX) из систем Windows 2000 и Windows XP Professional.

Резюме

- В значительной степени архитектуру сетей определяют протоколы. Во многих сетях используется несколько протоколов, с помощью которых осуществляется доступ к различным операционным системам сетевых серверов и хост-компьютеров.

- Обычно применяемые протоколы локальных сетей определяются типом сетевой серверной операционной системы, используемой в конкретной сети. Одной из старейших сетевых систем является NetWare, работающая со стеком протоколов IPX/SPX и обеспечивающая передачу данных между старыми версиями серверов NetWare и рабочими станциями (а также и другими серверами), подключенными к серверам. Протокол IPX/SPX реализован в тысячах локальных сетей, поскольку NetWare является одной из распространенных сетевых операционных систем. Однако в настоящее время благодаря тому, что многие сети связаны с Интернетом, новые версии NetWare (5.0 и выше) ориентированы на работу с более универсальным стеком протоколов TCP/IP.

- Родным протоколом для систем Windows NT Server является NetBEUI, появление которого связано с разработкой сетевой операционной системы LAN Manager, которую компания Microsoft начинала совместно с фирмой IBM. В средних и крупных сетях с серверами Windows NT чаще используется стек TCP/IP. С появлением систем Windows 2000 и Windows Server 2003 протокол TCP/IP пришел на замену NetBEUI, что определяется требованиями службы Active Directory и необходимостью доступа к Интернету.

- AppleTalk – это протокол, используемый компьютерами Macintosh с операционными системами Mac OS и Mac OS Server. Системы Windows NT, Windows 2000, Windows Server 2003 и Novell NetWare также поддерживают AppleTalk.

- Некоторые сетевые серверные операционные системы (в частности, UNIX) изначально были ориентированы на работу со стеком TCP/IP (а также и с Интернетом). В других сетевых операционных системах (например, NetWare, Windows NT и Mac OS Server) стек TCP/IP был реализован уже после создания этих систем.

- В первых системах IBM использовался стек протоколов SNA, который обеспечивал обмен данными между мэйнфреймами (мини-компьютерами) и терминалами, контроллерами и принтерами, а также между различными компьютерами. В операционных системах Windows имеется возможность установки протокола DLC для эмуляции коммуникаций SNA.

- Стек протоколов DNA был разработан для использования в сетях на базе компьютеров DEC, однако в настоящее время он применяется редко, поскольку количество таких компьютеров в сетях значительно уменьшилось.

- Простым и эффективным способом повышения производительности локальной сети

является периодически проводимый анализ применяемых протоколов и удаление тех протоколов, которые больше не используются .Для доступа к компьютерам и принтерам.

- Вплоть до начала 1990-х годов сетевые технологии в первую очередь разбивались в области протоколов локальных сетей. В настоящее время архитектура этих протоколов нашла логическое завершение в стеке TCP/IP, а частные протоколы (такие как IPX/SPX и NetBEUI) используются реже.

Прошлое, настоящее и будущее протокола TCP/IP

По прочтении этой главы и после выполнения практических заданий вы сможете:

- рассказать историю появления TCP/IP;
- объяснить принципы работы протоколов TCP и IP, а также методы использования протоколов UDP вместо TCP;
- рассказать об адресации IP и понять способы ее реализации в локальных и глобальных сетях;
- рассказать о новом протоколе IP version 6 и его назначении;
- обсудить способы использования прикладных протоколов, входящих в стек TCP/IP;
- понять назначение прикладных протоколов стека TCP/IP;
- соотнести реализацию TCP/IP с эталонной моделью OSI.

Когда компьютеры общаются через Интернет, то в качестве языка общения они используют Transmission Control Protocol/Internet Protocol (TCP/IP). Также протоколы TCP/IP широко распространены в большинстве средних и крупных сетей. Эти протоколы поддерживают сети на основе платформ Novell NetWare, UNIX и Windows, в особенности – развивающиеся сети и сети, в которых используются клиент-серверные или веб-ориентированные приложения. Широкое распространение, проверенные технологии и возможности расширения делают TCP/IP удачным выбором для большинства проектов, обеспечивающих взаимодействие локальных и глобальных сетей. Даже в небольших сетях развертывание TCP/IP может оказаться жизненно важным для дальнейшего развития сети.

В данной главе будет подробно рассказано о протоколах TCP/IP, включая описание пакетов TCP и IP, а также способы адресации IP. Также вы узнаете об альтернативе TCP – протоколе User Datagram Protocol (UDP), который применяется тогда, когда подтверждение переданных данных не так важно, как скорость и малая нагрузка на сеть. В главе обсуждается новейшая версия протокола IP, названная IPv6, и сравнивается с предшествующей версией, IPv4. Кроме того, рассказывается о прикладных протоколах входящих в стек TCP/IP и предназначенных для эмуляции терминалов передачи файлов и сообщений электронной почты, преобразований и назначения IP-адресов, а также для управления сетями. И, наконец, вы узнаете как архитектура TCP/IP соотносится с эталонной моделью OSI.

Краткая история стека TCP/IP

В конце 1960-х годов управление ARPA работало над тем, чтобы сделать сеть ARPANET доступной для общего пользования, обеспечивая компьютерам университетов, исследовательских учреждений и Министерства обороны возможность взаимодействия через глобальную сеть. Одним из заметных препятствий на пути достижения этой цели было наличие собственных стандартов у производителей компьютеров, и информацию о принципами боты своих систем производители охраняли как коммерческую тайну.

Первая попытка создания средств взаимодействия различных компьютеров была предпринята несколькими университетами, которые разработали сетевой протокол, названный *Network Control Protocol (NCP)* и позволивший хост-компьютерам разных компаний, включая DEC и IBM, обменивал информацией. NCP был простейшим протоколом, который обеспечивал различным типам компьютеров DEC и IBM возможность сетевых взаимодействий и запуска приложений через сеть, в которой хосты были географически удалены друг от друга. Например, одним из приложений протокола NCP была передача файлов между компьютерами. Это было хорошее начало, однако протокол NCP не мог обеспечить достаточно надежной передачи данных, поэтому управление ARPA для его модернизации запустило проект. Разработанный протокол на самом деле являлся комбинацией двух протоколов – *Transmission Control Protocol (TCP)* и *Internet Protocol (IP)* названия которых обычно сокращаются до аббревиатуры TCP/IP.

Примечание

Протокол NCP по-прежнему используется в старых сетях DEC и IBM, хотя его очень сложно конфигурировать. Этот протокол создает большую нагрузку на центральный процессор, поскольку он содержит некоторый уровень коммуникаций при выполнении сетевых операций, который не используется протоколом TCP

Внимание

Компания IBM использует аббревиатуру NCP для названия Программы управления сетью – Network Control Program. Эта программа представляет собой приложение, выполняющееся на оконечном процессоре (небольшом компьютере) или на шлюзе SNA, который подключен к мэйнфрейму, обеспечивая последнему возможность сетевых взаимодействий.

Основы стека TCP/IP

Протокол TCP, описанный в RFC 793, первоначально был разработан для двухточечных взаимодействий между компьютерами одной сети, а протокол IP (RFC 791) предназначался для обеспечения коммуникаций между компьютерами, подключенными к разным сетям или к глобальным сетям. Вскоре после своего появления оба протокола были объединены как стек TCP/IP для использования в популярных операционных системах Berkeley UNIX и были встроены в ОС Virtual Memory System (VMS, ныне – OpenVMS) компании DEC и Multiple Virtual Storage (MVS, ныне – OpenMVS) компании IBM.

С момента своего появления в начале 1970-х годов стек TCP/IP широко применялся в сетях в разных странах мира. Он реализован для PC-совместимых компьютеров, рабочих станций UNIX, мини-ЭВМ, компьютеров Macintosh и сетевых устройств, связывающих клиентов и хосты. TCP/IP обеспечивает тысячам открытых и коммерческих сетей подключение к Интернету, которым могут пользоваться миллионы людей.

TCP/IP – это многоуровневый стек протоколов, напоминающих уровни протоколов OSI, но не эквивалентных им. Стек TCP/IP содержит около ста стандартизованных протоколов, позволяющих обеспечить надежную и эффективную передачу данных между системами. Базовыми протоколами в стеке TCP/IP являются следующие:

- Transmission Control Protocol (TCP);
- User Datagram Protocol (UDP);
- Internet Protocol (IP).

Каждый из этих протоколов подробно рассматривается в последующих разделах.

Функционирование протокола TCP

TCP – это транспортный протокол, с помощью которого устанавливаются сеансы передачи данных между процессами прикладных программ, запускаемых клиентами сети. TCP предназначен для надежной доставки данных, для чего осуществляется контроль за правильностью приема фреймов и выполняется управление потоком данных. Для решения этих задач в протоколе предусмотрено упорядочение фреймов и подтверждение их приема.

Два взаимодействующих устройства задают порядковый номер для каждом переданного фрейма, и этот номер записывается в заголовок фрейма TCP Порядковый номер не только показывает местоположение фрейма в потом фреймов, но и указывает на длину данных, содержащихся в этом фрейме. Получив фрейм, принимающий узел проверяет порядковый номер и убеждается в том, что получен правильный фрейм в правильной очередности. Если узел назначения принимает фрейм, он передает подтверждение передающему узлу. Пакет подтверждения не только свидетельствует об успешном приеме фрейма, но и содержит порядковый номер следующего фрейма передачу которого ожидает принимающий узел.

Количество байтов данных, переданных во фрейме, называется *скользящим* окном (sliding window), поскольку это количество может увеличиваться или уменьшаться в процессе обмена информацией по взаимному соглашению между взаимодействующими узлами. Размер скользящего окна определяется, узлами динамически, при этом учитываются два фактора:

- текущий сетевой трафик;
- размер буфера (обычно в памяти), который в данный момент может выделить каждый узел для хранения фреймов, ожидающих обработки данным узлом.

Основные функции протокола TCP аналогичны функциям Транспортами уровня модели OSI. Он должен отслеживать запросы на установление сеансов связи, устанавливать сеансы с другими TCP-узлами, передавать и принимать данные, а также закрывать коммуникационные сеансы. Фрейм 1Я содержит заголовок и полезную нагрузку (рис. 6.1) и называется TCP сегментом.

Заголовок TCP имеет минимальную длину 20 байт и содержит поля, описанные ниже.

- Порт источника (Source Port) – некоторый порт TCP (называемый также сокетом или сеансом в других протоколах), подобный виртуальному каналу между двумя коммуникационными процессами на разных узлах (рис. 6.2). Для обеспечения совместимости некоторым портам TCP (также называемым "хорошо известными портами") назначаются определенные задачи. Назначение портов TCP и их описание можно найти в RFC 1700. Наличие механизма портов TCP означает, что в определенный момент времени в течение одного сеанса связи между двумя взаимодействующими узлами может выполняться обмен данными между несколькими процессами. Например, по одному порту может передаваться; состояние сети, а по другому – сообщения электронной почты или файлы. Порт источника – это порт TCP на передающем устройстве. Некоторые обычно используемые порты TCP перечислены в табл. 6.1.

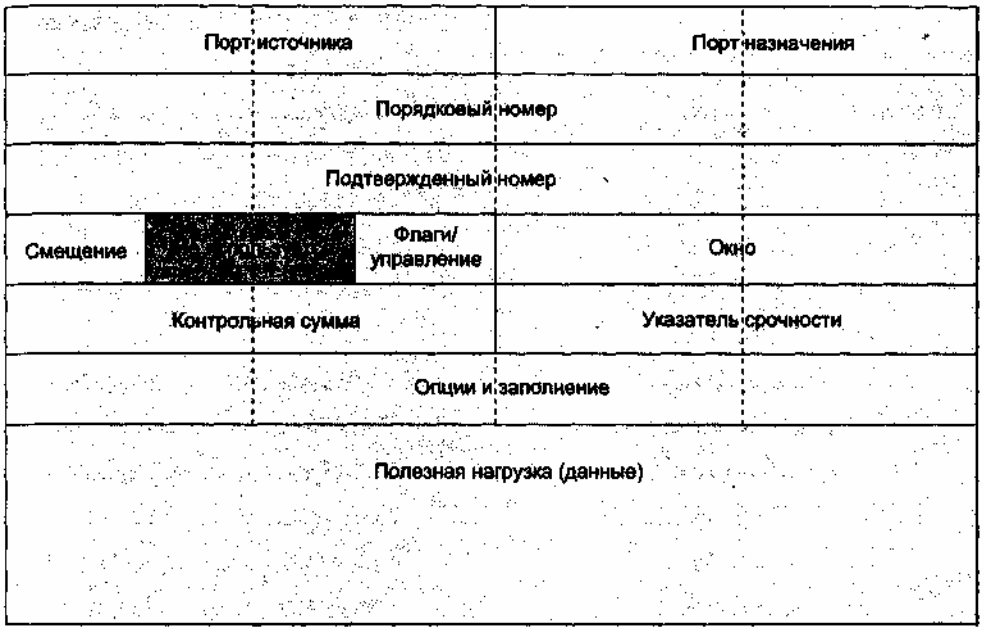


Рис. 6.1. Фрейм TCP

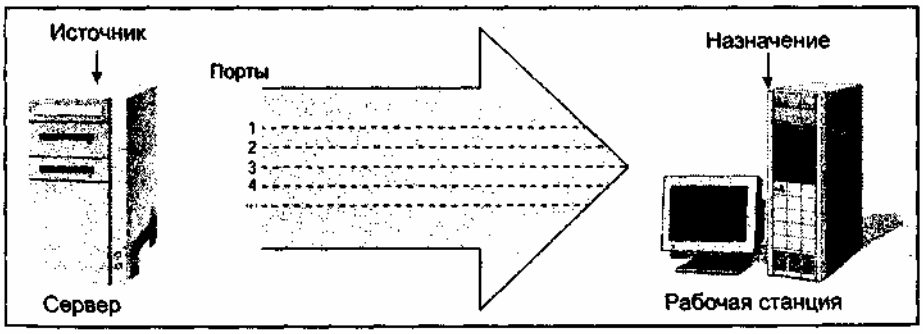


Рис. 6.2. TCP-порты источника и назначения

Таблица 6.1. *Порты TCP*

Номер порта	Назначение	Номер порта	Назначение
1	Мультиплексирование	9	Отвергнутая передача
5	Приложения RJE (remote job entry– дистанционный ввод заданий)	15	Состояние сети
20	Данные FTP	93	Управление устройствами
21	Команды FTP	102	Точка доступа к службе (SAP)
23	Telnet-приложения	103	Стандартные службы электронной почты
25	SMTP-приложения электронной почты	104	Стандартный обмен электронной почтой
37	Транзакции службы времени	119	Передача новостей Usenet
53	Приложения DNS-сервера	139	NetBIOS-приложения
79	Поиск активного пользовательского приложения		

- *Порт назначения* (Destination Port) – некоторый порт TCP на принимающем устройстве (см. рис. 6.2), участвующий в обмене информацией для некоторого прикладного процесса (например, при передаче файлам).

- *Порядковый номер* (Sequence Number) – 32-разрядный последовательный номер, назначаемый каждому фрейму в процессе передачи данных. С его помощью протокол TCP обеспечивает надежность приема всех фреймов. Порядковый номер также используется для обнаружения дубликатов фрейма и для расположения фреймов в нужном порядке после того, как они были переданы по разным сетевым маршрутам или каналам.

- *Подтвержденный номер* (Acknowledgement Number) – число, подтверждающее получение фрейма и передаваемое протоколом TCP исходному узлу после проверки порядкового номера фрейма. Если подтвержденный номер не отправляется обратно, то выполняется повторная передача фрейма.

- *Смещение* (Offset) или *Длина заголовка* (Header Length) – число, определяющее длину заголовка. С его помощью можно быстро определить начало данных, передаваемых во фрейме.

- *Флаги/управление* (Flags/control) – два флага в этом поле используются для обозначения начала (SYN) и конца (FIN) полного потока данных. Другие флаги представляют собой управляющую информацию (например, для сброса соединения или для отображения активности поля указателя

срочности).

- *Окно* (Window) – информация, используемая механизмом управления потоком данных. Окно содержит количество байтов, которые можно передать до того момента, как исходный узел получит подтверждение приема фрейма. По достижении этого числа включается управление потоком, прекращающее передачу до тех пор, пока не будет получено подтверждение. Например, если размер окна равен 64 байтам, то управление потоком включается в тот момент, когда будут переданы 65 байт без подтверждения, посланного передающему узлу. Если скорость сети мала из-за высокого трафика, размер окна может быть увеличен для того, чтобы управление потоком не включалось без необходимости. Размер окна может быть и уменьшен, если принимающий узел отвечает медленно (например, когда на рабочей станции возникает высокая нагрузка на шину или центральный процессор из-за того, что локальное приложение занимает эти ресурсы). Иногда задержки так велики, что выделенное поле окна не может вместить все значение размера окна. Хотя размер окна обычно определяется автоматически взаимодействующими узлами, его может также задать администратор сети, настраивающий оптимальную производительность сети на медленных или быстрых каналах связи. Это можно сделать для уменьшения числа повторных передач от ошибочно работающих программ или при перегрузке сети, а также для исправления ошибок передачи со стороны прикладных программ, плохо работающих в сети.

- *Контрольная сумма* (Checksum) – 16-разрядный циклический код с избыточностью (CRC), вычисляемый путем сложения всех полей заголовка и поля полезной нагрузки (сумма всех полей TCP-сегмента). Сумма вычисляется с использованием логической операции дополнения до единицы, т. е. двоичные разряды каждого поля меняют значение на противоположное (например, двоичный 0 меняется на двоичную 1, а двоичная 1 меняется на двоичный 0). Таким образом, перед сложением двух полей (например, ОНО и 10110110) их значения меняются на обратные (1001 и 01001001), а затем складываются. Общая сумма будет CRC-суммой, которая записывается во фрейм передающим узлом. Принимающий узел также вычисляет контрольную сумму и сравнивает полученное значение со значением, записанным в поле фрейма. Если значения различаются, то фрейм отбрасывается и принимающий узел запрашивает повторную передачу фрейма. В дополнение к значению контрольной суммы используются адреса источника и назначения, которые должны совпадать с теми адресами, которые указаны в IP-заголовке фрейма в качестве подтверждения того, что фрейм послан по заданному адресу.

- *Указатель срочности* (Urgent Pointer) – это поле заголовка, представляющее собой предупреждение для принимающего узла о том, что передаются срочные данные. Оно также указывает на конец срочных данных в последовательности пересылаемых фреймов. Назначение этого поля – заранее дать информацию о том, сколько данных еще будет передано в логически связанной последовательности из нескольких фреймов.

- *Опции* (Options) – поле фрейма, которое может содержать дополнительную информацию о передаваемых данных, а также дополнительные флаги.

- *Заполнение* (Padding) – поле, используемое в тех случаях, когда дополнительные данные отсутствуют или их слишком мало, чтобы обеспечить требуемую длину заголовка, которая должна быть кратна 32.

Примечание

Следует заметить, что данные, фактически передаваемые в TCP-сегментах называются полезной нагрузкой. Она представляет собой исходные данные пересылаемые от передающего узла к принимающему. Также нужно сказать том, что порты TCP и IP поддерживают полудуплексные и дуплексные коммуникации.

Подтверждения протокола TCP могут создать в сети заметный дополнительный трафик, особенно, если средний размер скользящего окна относительно мал. Именно поэтому некоторые типы приложений, для которых не требуется уровень надежности, обеспечиваемый протоколом TCP (с помощью механизмов

упорядочения и подтверждения), используют протокол User Datagram Protocol (UDP).

Функционирование протокола UDP

Для передачи данных стек TCP/IP имеет возможность пересылки информации с помощью потоков без установления соединения, при этом к посылаемым IP-датаграммам практически не добавляется никаких служебных данных (RFC 1240). Алгоритмы, используемые для форматирования, передачи и обратной сборки фреймов, описываются спецификацией протокол *User Datagram Protocol (UDP),* который применяется вместо TCP. Каждый фрейм имеет упрощенный заголовок, за которым следуют данные (рис 6,3) Протокол UDP используется программами мониторинга сети и некоторыми приложениями для передачи файлов, когда не требуется такая степень надежности, которую обеспечивает протокол TCP.

Заголовок UDP содержит следующие поля:

- *порт источника* – порт, используемый некоторым прикладным процессом на передающем узле для обмена информацией с аналогичным процессом на принимающем узле;
- *порт назначения* – порт на принимающем узле, связанный с процессом, с которым обменивается данными передающий узел;
- *длина* – поле, указывающее на длину фрейма;
- *контрольная сумма* – поле, используемое так же, как аналогичное поле в протоколе TCP, служит для сравнения полученного фрейма с переданным.

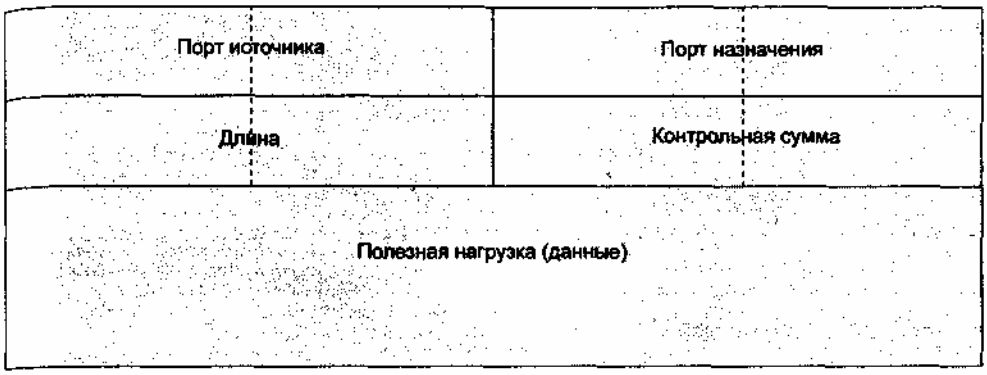


Рис. 6.3. Фрейм UDP

Протокол UDP не обеспечивает такой же уровень надежности и защиты от ошибок, который предлагает протокол TCP, поскольку надежность гарантируется только контрольными суммами фреймов. У протокола UDP отсутствуют механизмы управления потоком, упорядочения и подтверждения. Он функционирует как протокол без установления соединений, позволяя быстрее обрабатывать и передавать данные. Достоинством протокола UDP является то, что он добавляет мало служебной информации в пакеты IP и может использоваться приложениями, выполняющими обработку транзакций, в качестве средства уменьшения нагрузки на сеть. Некоторые прикладные протоколы стека TCP/IP также применяют протокол UDP. Для сетевого администратора он важен тем, что с его помощью осуществляются многие важные операции по управлению сетью и передаются сообщения о состояния сети (например, при использовании описываемых далее протоколов RIP, DNS, SNMP, RMON и BOOTP).

Функционирование протокола IP

Локальная сеть может состоять из нескольких подсетей. Глобальная сеть (например, Интернет) может быть образована из множества самостоятельных сетей (например, SONET, X.25, ISDN и др.). *Internet Protocol (IP)* позволяет передавать пакет в различные подсети локальной сети и разные сети, входящие в глобальную сеть, при соблюдении единственного требования: эти сети должны использовать транспортные механизмы, совместимые со стеком TCP/IP. Такие сети могут соответствовать следующим стандартам:

- Ethernet;
- Token Ring;
- X.25;
- FDDI;
- ISDN;

- DSL;
- сети с ретрансляцией кадров (frame relay);
- ATM (с преобразованием форматов).

Поскольку протокол IP используется очень широко, важно понимать его базовые функций и принципы функционирования в качестве протокола без установления соединения.

Основные функции IP

Базовые функции протокола IP следующие: передача данных, адресация пакетов, маршрутизация пакетов, фрагментация и обнаружение простых ошибок в пакетах. Успешная передача данных и маршрутизация пакетов в нужные сети или подсети делаются возможными благодаря механизму адресации IP. Каждый сетевой узел имеет 32-разрядный адрес, который в сочетании с 48-разрядным MAC-адресом узла обеспечивает осуществление сетевых коммуникаций и успешную доставку пакета в назначенный узел.

> **Примечание**
>
> Протокол IP не совместим с моделью OSI. Он функционирует на уровне, аналогичном Сетевому уровню (Уровню 3) эталонной модели OSI, и обеспечивает возможности маршрутизации, соответствующие Уровню 3.

IP как протокол без установления соединения

IP является протоколом без установления соединения, поскольку его главная задача – обеспечивать межсетевую адресацию и маршрутизацию, а также изменять размер пакетов, если он меняется при переходе от одной сети к другой (например, от Ethernet к FDDI). Задача обеспечения надежности коммуникаций передается от протокола IP к инкапсулированному TCP-сегменту (содержащему заголовок TCP и полезную нагрузку), который следует за заголовком IP и управляет потоком, выполняет упорядочение пакетов и другие проверки, а также подтверждает получение пакетов. Когда к TCP-сегменту добавляется заголовок IP, полученный блок данных называется датаграммой (datagram) или пакетом (рис. 6.4).

Именно адресная информация заголовка IP позволяет проверять маршрут (например, при переадресации IP-пакета). Заголовок пакета IP *(рис.6,5)* содержит поля, описанные ниже.

- *Версия* (Version) – поле, содержащее номер версии IP. В настоящее время в большинстве сетей применяется протокол *IP version 4 (IPv4),* который появился в начале 1980-х годов, а также внедряется стандарт *IP version 6 (IPv6),* ориентированный на Интернет и задачи мультимедиа.

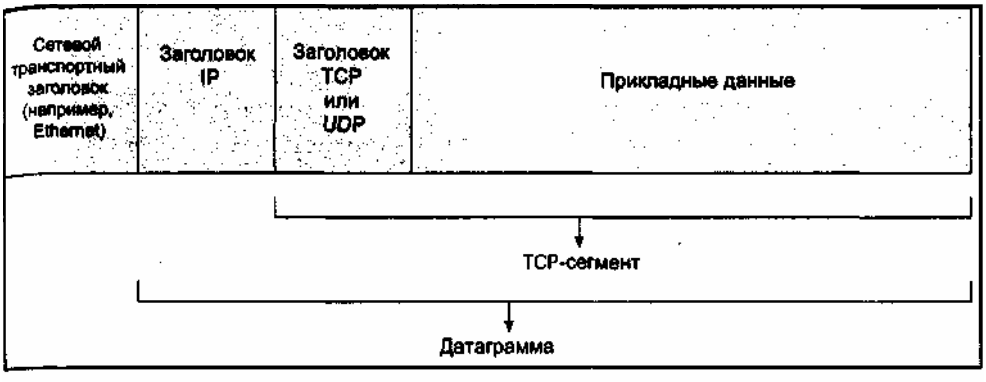


Рис. 6.4. Инкапсуляция пакета TCP/IP

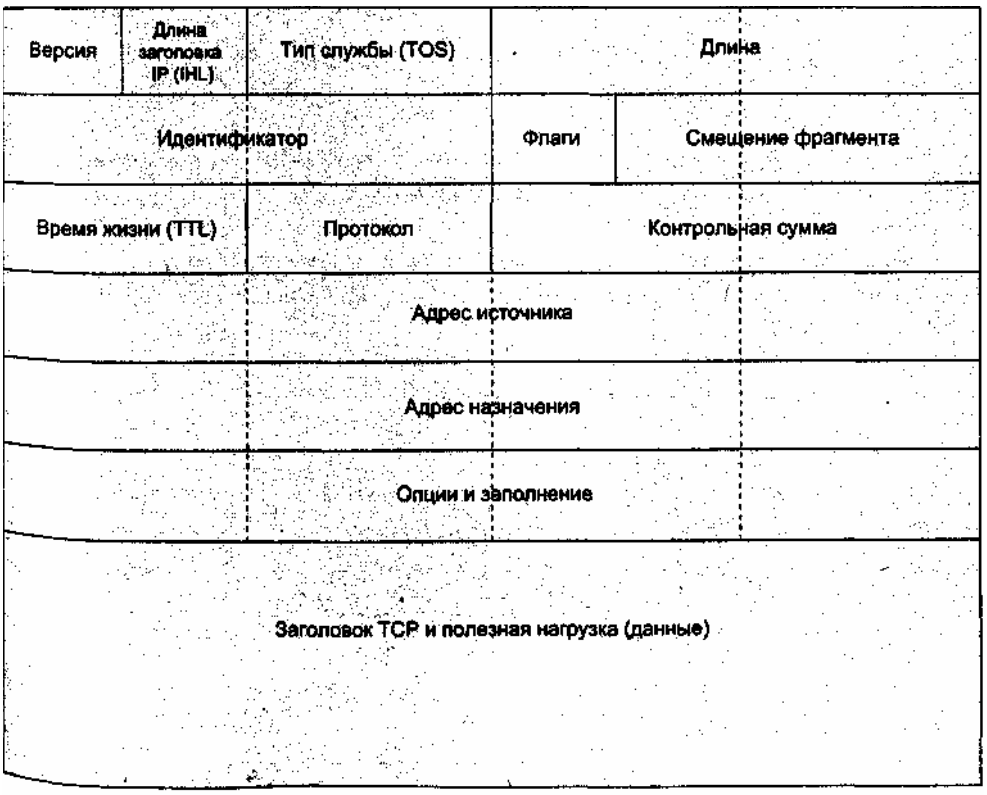


Рис. 6.5. Пакет IP

- *Длина заголовка IP* (IP Header Length, IHL) – указывает размер заголовка IP (минимум 20 байт), который может изменяться в зависимости от размера поля опций
- *Тип службы* (Type of Service, TOS) – поле, указывающее старшинство или приоритет, определенный для содержимого пакета. Оно позволяет протоколам маршрутизации (например, OSPF) определять тип маршрута по которому надо отправлять пакет, используя механизм стоимости маршрута. Например, для обычного пакета данных не нужна такая же скорость передачи, как для пакета мультимедиа-данных. Поле TOS позволяет применять комбинированные уровни приоритета, для чего учитывав значение и положение двоичных разрядов в этом поле. Приоритет может определять следующие параметры канала: нормальный, с малой задет кой, с высокой пропускной способностью, с минимальной стоимостью и с высокой надежностью. Например, если указан нормальный маршрута может быть выбран 10-мегабитный канал, независимо от того, сколько ретрансляций потребуется пакету для достижения целевого узла. Если указаны каналы с минимальной стоимостью и высокой пропускной способностью, то может использоваться 100-мегабитный канал с минимальным количеством маршрутизаторов.
- *Длина* (Length) – полная длина пакета IP, которая может достигать 65 535 байтов.
- *Идентификатор* (Identification). Для разнородных сетей протокол IP может преобразовывать размер пакета. Например, пакет Ethernet может иметь длину от 64 до 1526 байт (включая заголовок), а пакет FDDI может иметь длину до 4472 байт. Длина пакета маркерной сети с частотой 16 Мбит/с может достигать 17 800 байт. Протокол IP может передавать пакеты в сетях различных типов, для чего выполняется фрагментация пакетов (например, один пакет FDDI может быть разбит на несколько частей, удовлетворяющих требованиям максимальной длины, равной 1526 байт, для пакетов Ethernet). Когда протокол IP фрагментирует пакет, он назначает всем фрагментам один групповой номер и помещает этот номер в поле идентификатора для того, чтобы эти фрагменты при сборке не были перепуганы с другими.
- *Флаги* (Flags) – используются вместе с механизмом фрагментации для передачи служебной информации. Например, может быть указано, что фрагментация не должна выполняться для текущего пакета (если пакет пересылается из одной сети Ethernet в другую), или (если пакет фрагментируется) указывается, что был передан последний фрагмент в некоторой последовательности.
- *Смещение фрагмента* (Fragment Offset) – содержит информацию, полагающую восстановить фрагменты, принадлежащие одной группе.
- *Время жизни* (Time-to-Live, TTL) – информация, препятствующая зацикливанию пакета в сети (когда он непрерывно циркулирует внутри некоторой сети). Значение TTL устанавливается

равным максимальному времени (в секундах), в течение которого пакет может передаваться. Это значение проверяется каждым маршрутизатором, через который проходит пакет, и когда значение становится равным нулю, пакет уничтожается. При каждой передаче IP-пакета через маршрутизатор значение TTL уменьшается на некоторую стандартную величину, определяемую самим маршрутизатором или администратором сети.

- *Протокол* (Protocol) – поле, указывающее на то, какой протокол (TCP или UDP) инкапсулирован в IP.
- *Контрольная сумма* (Checksum) – 16-разрядный циклический код с избыточностью (CRC), представляющий собой сумму значений всех полей заголовка IP. Эта контрольная сумма вычисляется так же, как и проверочная сумма для протокола TCP (т. е. с использованием операции дополнения до единицы), однако при вычислениях не учитывается поле полезной нагрузки датаграммы (TCP-сегмент). Полученная сумма используется для проверки правильности приема заголовка IP. Контрольную сумму проверяет каждый маршрутизатор, через который передается пакет, а также принимающий узел. Когда пакет проверяется маршрутизатором, значение контрольной суммы обновляется, что отражает изменения в пакете (например, изменения времени TTL).
- *Адрес источника* (Source Address) – адрес сети и устройства, пославшего пакет.
- *Адрес назначения* (Destination Address) – адрес сети и адрес принимающего узла.
- *Опции* (Options) – некоторые опции, используемые протоколом IP. Например, может быть указано время создания пакета, для ответственных (военных и правительственных) приложений может быть реализован специальный механизм защиты данных.
- *Заполнение* (Padding) –. дополнение поля опций, когда данных недостаточно для того, чтобы общая длина заголовка IP (в битах) была кратна 32.

Полезная нагрузка (данные) в IP-пакете фактически представляет собой заголовок TCP (если используются службы с установлением соединения) или UDP (если используются службы без установления соединения) и прикладные данные.

Совет

Когда в сети отслеживается размер пакетов, пакеты неправильного размера могут указывать на возможный источник сетевых ошибок, которым нередко является неисправный сетевой адаптер. Например, пакет Ethernet короче 64 байтов, но содержащий все обычные поля, может появиться благодаря плохо работающему сетевому адаптеру или из-за проблем в драйвере адаптера. Также это может быть признаком слишком большого количества коллизий в сети, пакет Ethernet длиной от 1526 до 6000 байт называется длинным пакетом и его также может сгенерировать неисправный адаптер или сетевой драйвер. За длинными пакетами иногда может последовать передача пакетов, содержащих символы "A" и "5" и сообщающих другим станциям о том, что сеть активна. Такая ситуация, обусловленная наличием сбойных пакетов, может заметно замедлить работу сети, и это обычно означает необходимость замены передающего сетевого адаптера. Пакет длиной свыше 6000 байтов является гигантским и также указывает на наличие проблем в передающем адаптере.

Принципы адресации IP

Механизм адресации IP служит для идентификации отдельного узла и той сети, в которой он находится. Для правильной доставки пакета очень важно, чтобы IP-адреса были уникальными. Если два или несколько узлов в одной сети пытаются использовать один и тот же IP-адрес, то большинство операционных систем выдают сообщение об ошибке и запрещают таким узлам взаимодействовать с сетью.

Формат IP-адреса использует *десятичное представление с разделительными точками* (dotted decimal notation). Адрес имеет длину 32 разряда и содержит четыре поля, представленные десятичными числами, соответствующими разрядным двоичным кодам. IP-адрес в двоичном виде может выглядеть так: 10000001.00000101.00001010.01100100. В десятичном формате этот адрес соответствует 129.5.10.100. Часть адреса представляет собой идентификатор. (NET_ID), а другая часть – идентификатор хоста (HOST_ID).

Существуют пять классов IP-адресов (с A по E), каждый из которых применяется в сетях различного типа. Классы адресов соответствуют размеру и определяют тип пакетов – однонаправленные или групповые (дополнительная информация по этому вопросу имеется в *главах. 2* и *10).* **Примечание**

Когда приложение, выполняющееся на сетевом узле, использует однонаправленные пакеты (а это самый распространенный тип пакетов), то одна копия каждого пакета в сеансе связи посылается каждому целевому узлу, для которого предназначен пакет. Широковещательные пакеты реже используются прикладными программами, в этом случае исходный узел посылает один пакет множеству целевых узлов, и этот пакет в конце концов доходит до каждого узла назначения.

Классы A, B и C предназначены для однонаправленной адресации, однако каждому классу соответствует свой размер сети. Класс A используется для самых крупных сетей, насчитывающих до 16 777 216 узлов. Для сетей класса A в первой позиции десятичного адреса с разделительными точками допускаются значения от 1 до 126. Идентификатор сети занимает первые 8 разрядов, а идентификатор хоста – остальные 24 разряда. Класс B – это формат однонаправленной адресации для сетей среднего размера, содержащих до 65 536 узлов. Для их идентификации в первом байте используются десятичные числа в диапазоне от 128 по 191. Первые два байта представляют идентификатор сети, а два последних байта содержат идентификатор хоста. Адреса класса C применяются в небольших сетях с однонаправленными коммуникациями и количеством хостов, не превышающем 254. Первый байт таких адресов содержит значения в диапазоне от 192 до 223, при этом идентификатор сети занимает первые 24 разряда, а идентификатор хоста задается последними 8-ю разрядами.

Адреса класса D не связаны с размером сети, они предназначены лишь для групповых рассылок. Четыре байта адреса используются для указания группы адресов, которым предназначены широковещательные пакеты. Эта группа содержит узлы, являющиеся подписчиками таких пакетов *(см. главу 10).* Адреса класса D выбираются из диапазона значений от 224.0.0.0 до 239.255.255.255. Пятый класс адресов, класс E, используется для исследовательских задач и в первом байте содержит значения от 240 до 255.

Помимо классов, существуют некоторые IP-адреса специального назначения (например, адрес 255.255.255.255, который представляет собой широковещательный пакет, посылаемый всем узлам сети). Пакеты, имеющие в первом байте значение 127, используются для тестирования сети. Чтобы указать всю сеть, задается только идентификатор сети, а другие байты содержат нули (например, для некоторой сети класса B можно использовать адрес 132.155.0.0, а для сети класса C – адрес 220.127.110.0).

Примечание

Широковещательным называется пакет, который посылается всем узлам сети.

Роль маски подсети

Адреса TCP/IP требуют указания *маски подсети,* которая используется для Р[e]шения двух задач: для обозначения используемого класса адресов и для деления сети на подсети при управлении сетевым трафиком. Маска подсети позволяет прикладной программе определить, какая часть адреса является идентификатором сети, а какая соответствует идентификатору хоста. Например, [Mac]ка для сети класса A имеет единицы во всех разрядах первого байта и нули – в остальных байтах, т. е. 11111111.00000000.00000000.00000000 (255.0.0.0 в Десятичном представлении). В этом случае единицы указывают на разряды Идентификатора сети (подсети), а нули – на разряды идентификатора хоста.

Создание подсетей

При делении сети на подсети маска содержит идентификатор подсети, определенный администратором и расположенный в диапазоне значений идентификаторов сети и хоста. К примеру, третий байт в адресе класса может быть использован для определения идентификатора подсети, например, 11111111. 11111111. 11111111.00000000 (255.255.255.0). В другом случае для идентификации подсети могут быть задействованы только первые несколько разрядов третьего байта, а остальные три разряда (и последний байт целиком) могут определять идентификатор хоста, т. е. получится значение 11111111. 11111111. 11111000.00000000 (255.255.248.0). (Просмотр и настройка IP-адресов и масок подсетей рассматриваются в практических заданий с 6-1 по 6-4.)

Нужно заметить, что применение маски подсети для деления сети на несколько мелких подсетей позволяет устройствам Класса 3 фактически игнорировать типовые характеристики классов адресов, что создает дополни тельные возможности для сегментирования сетей с использованием множества подсетей и дополнительных сетевых адресов. В этом случае можно преодолеть

ограничения 4-байтовой адресации. Игнорировать классы адресов можно также при помощи *бесклассовой междоменной маршрутизации* (Classless Interdomain Routing, CIDR), когда после десятичного представления адреса с разделительными точками указывается символ косой черты ("/"). CIDR-адресация обеспечивает, в сетях среднего размера дополнительные возможности IP-адресации, поскольку имеется нехватка адресов классов B и C. Эта нехватка объясняется увеличением количества сетей и конечным числом адресов, возможных при использовании базового механизма 4-байтовых адресов. CIDR-адресация позволяет обойти фиксированный размер идентификаторов сети (равный 8, 16 и 24 разрядам для сетей класса A, B и C соответственно) и задействовать неиспользуемые адреса.

Рассмотрим для примера сеть класса C, в которой имеется только 100 узлов (идентификаторов хостов), но адресов в ней достаточно для идентификации 254 узлов. В этом случае теряется 154 возможных идентификатора хостов. При использовании CIDR-адресации число после косой черты представляет собой количество разрядов в адресе, выделяемых для обозначения идентификатора сети. Например, сеть должна иметь идентификаторы для 16 384 (2^{14}) хостов Чтобы определить количество разрядов, необходимых для идентификации сети, нужно вычесть 14 (количество разрядов для идентификаторов хостов) из 32 (общее количество разрядов в IP-адресе): 32 - 14 = 18. Таким образом 18 разрядов требуются для идентификатора сети и 14 – для идентификатора хоста (теперь маска подсети равна 11111111. 11111111. 11000000.00000000, т.е. 255.255.192.0).

IP-адрес для нашего примера может иметь вид 165.100.18.44/18. Если вы хотите с помощью масок подсети разбить сетевой трафик по нескольким небольшим подсетям, заранее спланируйте размещение узлов по сегментам и выберите маски подсетей для этих сегментов. При этом следует учесть перспективы развития сети на ближайшие несколько лет, чтобы при каждом изменении сети не нужно было заново переделывать ее сегменты. При плохом планировании и изменении конфигурации сегментов клиенты должны будут менять IP-адреса своих компьютеров, что создает дополнительные трудности в администрировании сети.

Принципы работы протокола IPv6

В середине 1990-х годов специалисты по сетям осознали тот факт, что протокол IP version 4 (IPv4) имеет некоторые ограничения. Главным из этих ограничений является использование 32-разрядных адресов в то время, когда существуют тысячи сетей и миллионы сетевых пользователей. Фактически адреса для протокола IPv4 были исчерпаны. Кроме того, протокол IPv4 не предусматривает средств для обеспечения сетевой безопасности или реализации сложных схем маршрутизации (например, для создания подсетей на базе уровней качества обслуживания QoS). Также протокол IPv4 имеет недостаточно возможностей (помимо механизмов широковещания и группового вещания) для работы различных приложений мультимедиа (например, для потокового телевидения или видеоконференций).

В ответ на растущие требования к протоколу IP проблемная группа Internet Engineering Task Force (IETF) запустила проект IP Next Generation (IPng). Результатом работы над этим проектом в 1996 году явился новый стандарт – протокол *IP version 6 (IPv6),* описанный в RFC 1883. Назначение этого протокола – обеспечить логический переход от протокола IPv4, чтобы приложения и сетевые устройства могли отвечать новым требованиям по мере их появления. В настоящее время в большинстве сетей во всем мире применяется протокол IPv4, однако начинается переход на IPv6.

Особенности протокола IPv6

Протокол IPv6 имеет следующие новые возможности:

- 128-разрядную адресацию;
- связь одного адреса с несколькими интерфейсами;
- автоматическое назначение адреса и CIDR-адресацию;
- 40-байтный заголовок вместо 20-байтного заголовка протокола IPv4;
- дополнительные заголовки IP, создаваемые для специальных задач, в т. ч. для реализации новых средств маршрутизации и безопасности.

Механизм адресации IPv6 позволяет связывать один идентификатор IP с несколькими интерфейсами, что обеспечивает лучшее управление трафиком мультимедиа-данных. Вместо широковещания и группового вещания сети на базе протокола IPv6, передающие мультимедийные данные, назначают один адрес всем принимающим интерфейсам.

Совет

Протокол IPv6 применяется в некоторых экспериментальных сетях. Если вы имеете доступ к такой сети, то можете сконфигурировать IPv6 для какого-нибудь интерфейса системы Red Hat Linux 7.x. Для этого используется утилита ifconfig с параметром add addr/prefixlen. Протокол IPv6 можно установить в системе Windows XP, для чего следует открыть окно командной строки ввести ipv6 install и нажать клавишу <Enter>. Конфигурирование протокола IPv6 в среде Windows XP описано в справочной системе.

Протокол IPv6 разработан совместимым с CIDR-адресацией (заменившей адресацию на основе классов), благодаря чему имеется множество опций для конфигурирования адресов. Это упрощает маршрутизацию и сегментирование сети на подсети. Кроме того, протокол позволяет создавать признаки, по которым можно различать адреса для сети определенного размера сетевого узла, организации, типа организации, рабочих групп внутри организации и т. д. Механизм адресации IPv6 использует автоматическое назначение адресов, что упрощает сетевому администратору задачу конфигурирования адресов.

IPv6 и автоматическое конфигурирование

Протокол IPv6 поддерживает два механизма автоматического конфигурирования IP-адресов. Первый из них основан на протоколе *Dynamic Host Configuration Protocol (DHCP)* (протокол динамической конфигурации хоста используемом для динамической адресации. При *динамической адресации* IP-адрес автоматически назначается компьютеру при каждом его подключении к сети. При использовании DHCP адрес выделяется (сдается в аренду) компьютеру на некоторое заданное время. Протокол DHCP позволяет серверу, на котором запущены службы DHCP, обнаруживать появление новой рабочей станции, сервера или сетевого устройства и назначать им IP-адрес.

Для использования динамической адресации в сети необходимо разместить службы DHCP на некотором сервере (например, на компьютере под управлением Windows 2000 или UNIX) и сконфигурировать его в качестве **DHCP-**сервера. Этот сервер по-прежнему сможет выполнять свои функции (скажем, файлового сервера), однако у него появится возможность автоматического назначения IP-адресов. DHCP-сервер выдает IP-адреса в аренду на указанное время. Это время может составлять неделю, месяц, год или быть вообще неограниченным (например, для адреса, выданного веб-серверу). Когда срок аренды заканчивается, выданный IP-адрес возвращается в пул имеющихся адресов, который поддерживается на сервере. Применительно к протоколу IPv6 такой способ динамической адресации называется *автоматическим конфигурированием с сохранением состояния* (stateful auto-configuration).

Другим механизмом назначения адресов в IPv6 является *автоматическое конфигурирование без сохранения состояния* (stateless autoconfiguration). В этом случае сетевое устройство само назначает себе IP-адрес, без обращения к серверу. Этот адрес просто создается на основе MAC-адреса сетевого адаптера и адреса подсети, который получается от маршрутизаторов, имеющихся в данной подсети.

Типы пакетов IPv6

Пакеты протокола IPv6 бывают трех типов: однонаправленные, *альтернативные* (anycast) и групповые. Однонаправленный пакет идентифицируется по имеющемуся в нем одному адресу для конкретного интерфейса (сетевого адаптера) и передается в режиме "точка-точка". Альтернативный пакет содержит целевой адрес, ассоциированный с несколькими интерфейсами, которые обычно относятся к разным узлам. Такой пакет передается только ближайшему интерфейсу и перенаправляется другим интерфейсам, имеющим тот же самый адрес. Групповой пакет (как и альтернативный пакет) имеет целевой адрес, связанный с несколькими интерфейсами, однако в отличие от альтернативного пакета он передается каждому интерфейсу с указанным адресом.

Поля заголовка пакета IPv6

Базовый заголовок протокола IPv6 (рис. 6.6) содержит поля, назначение которых описывается ниже.

- *Версия* (Version) – поле идентификатора версии, содержащее число 6.
- *Класс трафика* (Traffic Class) – поле, указывающее на то, содержит ли пакет информацию для управления сетевым трафиком. Пакеты, предназначенные для управления нагрузкой на сеть, могут обеспечивать такие возможности, как фильтрация, автоматическая отправка сообщений

электронной почти или управление через Интернет. Пакеты, не имеющие функций управления, предназначены для передачи данных, и могут быть назначены различные уровни приоритета, указывающие на критичность отбрасывания данного пакета. Например, пакету, передающему аудиосигнал, может быть задан высокий приоритет, указывающий на то, что отбрасывание пакета крайне нежелательно, поскольку из-за этого может возникнуть пауза в непрерывном звучании сигнала.

- *Метка потока данных* (Flow Label) – информация для маршрутизаторов, Указывающая на необходимость особой обработки пакета. Например, групповой пакет может потребовать дополнительных сетевых ресурсов, а для конфиденциального пакета может понадобиться дополнительная защита.

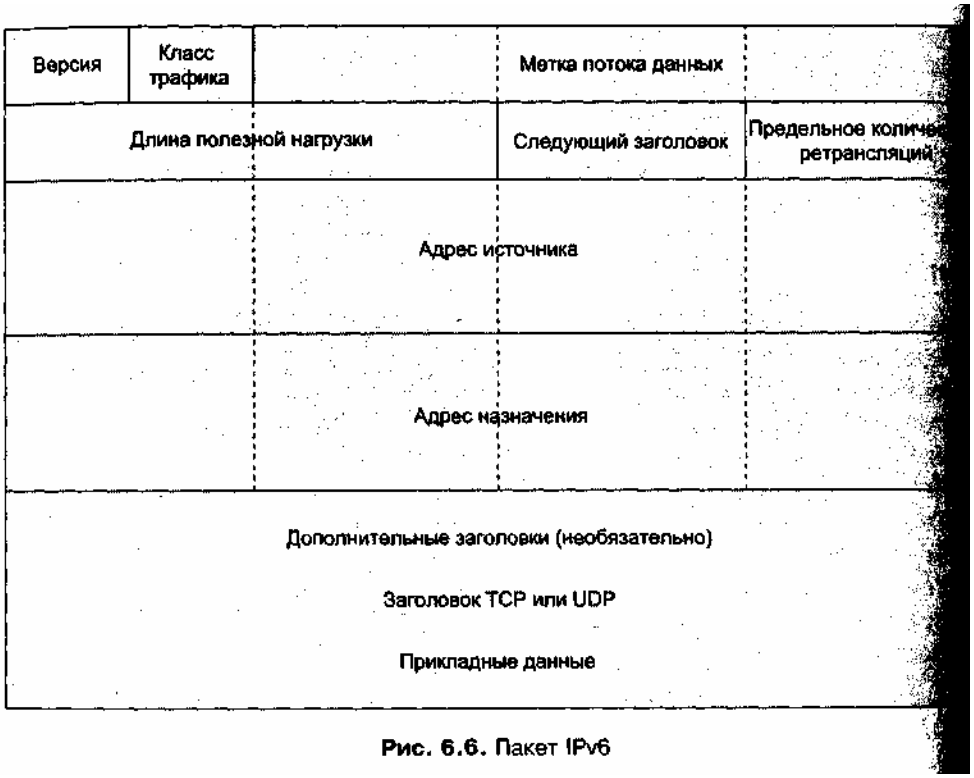


Рис. 6.6. Пакет IPv6

- *Длина полезной нагрузки* (Payload Length) – поле, указывающее размер полезной нагрузки пакета (за исключением заголовка).

- *Следующий заголовок* (Next Header) – поле, указывающее тип заголовка который нужно ждать по окончании базового заголовка, поскольку пакет может иметь дополнительные заголовки. Если дополнительные заголовки отсутствуют, то следующим будет заголовок TCP или UDP.

- *Предельное количество ретрансляций* (Hop Limit) – модифицированное поле TTL протокола IPv4. При создании пакета в это поле заносится максимальное количество ретрансляций пакета через маршрутизаторы, это значение уменьшается на единицу при каждой передаче пакета через устройство Уровня 3. Если такое устройство встречает пакет, у которого количество ретрансляций равно нулю, то оно отбрасывает пакет, благодаря чему пакет не может передаваться в сети бесконечно.

- *Адрес источника* (Source Address) – 128-разрядный адрес передающего устройства.

- *Адрес назначения* (Destination Address) – 128-разрядный адрес устройства, принимающего пакет.

В настоящее время стандарт IPv6 описывает шесть дополнительных заголовков (extension header):

- дополнительный заголовок последовательных (hop-by-hop) ретрансляций;
- дополнительный заголовок маршрутизации;
- дополнительный заголовок фрагмента;
- дополнительный заголовок аутентификации;
- дополнительный заголовок инкапсулированных данных безопасности;

- дополнительный заголовок опций узла назначения.

Основной заголовок IPv6 должен располагаться в пакете раньше, чем любой дополнительный заголовок. Дополнительные заголовки не обязательны и могут использоваться в любом сочетании или вообще отсутствовать. В одном пакете можно указать только один дополнительный заголовок определенного типа. Если используется один или несколько дополнительных заголовков, они должны следовать в том порядке, в котором перечислены в приведенном выше списке. Если, к примеру, используются заголовки маршрутизации, аутентификации и инкапсулированных данных безопасности, они должны следовать в таком порядке (рис. 6.7):

1) основной заголовок IPv6;
2) дополнительный заголовок маршрутизации;
3) дополнительный заголовок аутентификации;
4) дополнительный заголовок инкапсулированных данных безопасности;
5) заголовок TCP или UDP;
6) прикладные данные.

Обратите внимание на то, что первое поле в каждом дополнительном заголовке представляет собой 8-разрядное поле следующего заголовка, указывающее на его тип. В последнем используемом дополнительном заголовке это поле содержит значение 59. В приведенном на рисунке примере поле следующего заголовка в дополнительном заголовке маршрутизации указывает на то, что далее следует дополнительный заголовок аутентификации, а в заголовке аутентификации это поле содержит признак того, что следующим в пакете будет дополнительный заголовок инкапсулированных данных безопасности. В этом заголовке поле следующего заголовка содержит число 59, Указывающее на то, что больше в пакете нет дополнительных заголовков. Во всех дополнительных заголовках (за исключением заголовка фрагмента) за Полем следующего заголовка непосредственно следует 8-разрядное поле Длины дополнительного заголовка, содержащее значение длины текущего заголовка. Длина каждого дополнительного заголовка должна быть кратной 8 байтам

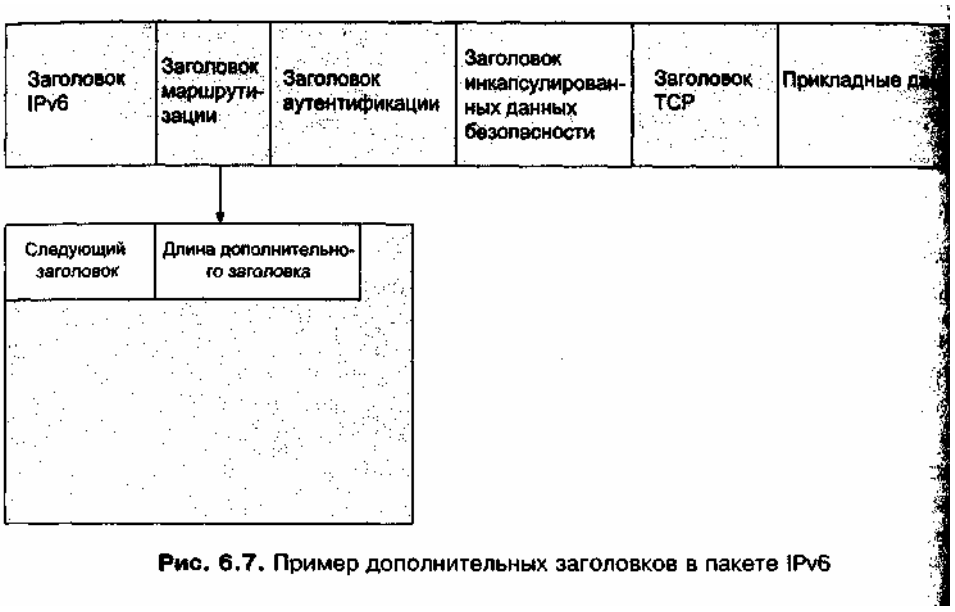


Рис. 6.7. Пример дополнительных заголовков в пакете IPv6

Дополнительный заголовок последовательных ретрансляций используется для передачи данных большого объема (например, пакетов мультимедийных видеосигналов). Благодаря ему поле прикладных данных может содержать от 65 535 до 4 миллионов байт. Заголовок последовательных ретрансляций проверяется каждым маршрутизатором, через который передается пакет, что несколько увеличивает время на его прохождение через маршрутизаторы.

Дополнительный заголовок маршрутизации идентифицирует маршрут для каждого пакета, для чего указывается список адресов маршрутизаторов. Этот заголовок можно сгенерировать так, что пакеты будут следовать по неизменяемому маршруту или маршрут будет зависеть от конкретных условий (например, маршрут может изменяться, если некоторый маршрутизатор в заданном маршруте не работоспособен).

Определение размера пакета

При использовании протокола IPv6 каждый передающий узел может установить минимальный допустимый размер пакета для целевой сети. При этом для обнаружения маршрута для пакета

максимального размера (maximum transmission unit, MTU) используются зондирующие пакеты. В процессе обнаружения маршрута собирается информация о том, работоспособны ли маршрутизаторы и не требует ли целевая сеть пакеты меньшего размера (пакет IPv6 содержит не менее 1280 байт). Если выполняется передача данных некоторому узлу сети, в которой используются пакета размером менее 1280 байт, протокол IPv6 фрагментирует пакеты.

Используя данные, полученные при обнаружении MTU-маршрута, передающий узел фрагментирует пакеты и включает в них дополнительный заголовок фрагмента, сообщающий принимающей стороне о порядке фрагментации пакетов. Возможность фрагментации пакетов важна в тех случаях, когда пакеты передаются из сети Ethernet в сеть с маркерным кольцом или когда пакеты фрагментируются для передачи через сети Fast Ethernet, Gigabit Ethernet и 10 Gigabit Ethernet, в которых имеются особые требования к размеру пакетов. Когда пакет фрагментируется, каждому элементу в группе фрагментов назначается один и тот же идентификатор (уникальный для данной группы), заносимый в 32-разрядное поле идентификатора. Благодаря этому фрагмент из одной группы нельзя перепутать с фрагментами других групп при приеме данных.

Дополнительный заголовок аутентификации используется для проверки целостности датаграммы (заголовка IP, заголовка TCP и данных), т. е. для проверки того, что датаграмма получена в том же виде, в котором была послана. Аутентификация выполняется для каждого поля каждого заголовка, а также для поля полезной, нагрузки. Если значение некоторого поля изменилось в процессе передачи (что всегда верно для поля количества ретрансляций), то это поле при аутентификации получает значение 0. Зачастую заголовок аутентификации и заголовок инкапсулированных данных безопасности используются вместе, т. е. пакет аутентифицируется и шифруется/расшифровывается. Когда присутствуют оба этих заголовка, на принимающем узле выполняются следующие действия:

1- Аутентифицируется заголовок IP, а затем – заголовок TCP (сначала может понадобиться их дешифрация, если в дополнительном заголовке инкапсулированных данных безопасности указано шифрование одного из заголовков – IP или TCP – или обоих заголовков).

2- Дополнительный заголовок аутентификации получает разрешение на дешифрацию полезной нагрузки, для чего снова используются данные заголовка инкапсулированных данных безопасности.

3- После дешифрации поле полезной нагрузки аутентифицируется.

Шифрование и пакеты IP

В сетях, требующих повышенной безопасности, полезная нагрузка пакета IP (или заголовок TCP или UDP и данные) может быть зашифрована с использованием дополнительного заголовка инкапсулированных данных безопасности. Этот заголовок поддерживает методы шифрования, отвечающие требованиям *Data Encryption Standard (DES)* (стандарт шифрования данных).

DES – это сетевой стандарт шифрования с использованием симметричного ключа, разработанный институтами National Institute of Standards and Technology (NIST) (Национальный институт стандартов и технологий) и ANSI. Дополнительный заголовок инкапсулированных данных безопасности вставляется в тех случаях, когда применяется шифрование передаваемых данных, он обеспечивает шифрование при пересылке информации чем Интернет, а также через другие локальные и глобальные сети.

Внимание

Использование дополнительных заголовков аутентификации и инкапсулированных данных безопасности может увеличить задержку при передаче данных. *Задержка* (latency) – это время, необходимое для передачи сетевых данных от передающего устройства к принимающему.

Прикладные протоколы стека TCP/IP

Протоколы TCP/IP предназначены для работы со множеством прикладных протоколов, обеспечивающих передачу электронной почты, эмуляцию терминалов, передачу файлов, маршрутизацию, управление сетью и выполнение других задач. Совокупность этих протоколов называется стеком TCP/IP. Как и протоколы TCP/IP, эти прикладные протоколы обеспечивают коммуникации в полудуплексном и дуплексном режимах. Ниже перечислены некоторые из основных протоколов и прикладных служб, входящих в стек TCP/IP:

- протокол Telnet;

- протоколы File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) и Network File System (NFS);
- Simple Mail Transfer Protocol (SMTP);
- служба имен доменов (DNS);
- Dynamic Host Configuration Protocol (DHCP);
- Address Resolution Protocol (ARP);
- Simple Network Management Protocol (SNMP).

Далее все перечисленные протоколы и приложения рассматриваются пожробно.

Telnet ***Ш***

Telnet – это прикладной протокол стека TCP/IP, обеспечивающий эмуляцию терминалов. *Терминал* – это устройство, состоящее из монитора и клавиатуры и используемое для взаимодействия с хост-компьютерами (обычно мэйнфреймами или мини-компьютерами), на которых выполняются программы. Программы запускаются на хосте, поскольку терминалы, как правило, не имеют собственного процессора.

Примерами терминалов могут служить устройства IBM 3270 или DEC VT220. При *эмуляции терминалов* используются программные средства, с помощью которых некоторый компьютер (например, персональный) может функционировать в качестве терминала. Протокол Telnet позволяет клиенту подключиться к хост-компьютеру, при этом реакция хоста будет такой же, как и при подключении терминала. Например, протокол Telnet с эмулятором устройства IBM 3270 позволяет подключиться к мэйнфрейму IBM и работать с ним так же, как с терминала. Протокол Telnet функционирует на уровне стека TCP/IP, эквивалентном Сеансовому уровню модели OSI, однако с его помощью можно выполнять операции, соответствующие Транспортному уровню.

> **Примечание**
>
> Компьютер под управлением Windows 2000 или Windows Server 2003 можно сконфигурировать как сервер терминалов (Terminal Server) (при этом программы будут выполняться на сервере), однако в этом случае для эмуляции терминалов протокол Telnet не используется. Обычные терминалы могут обращаться к серверу терминалов, и персональные компьютеры могут для эмуляции терминалов использовать фирменное программное обеспечение. Сервер терминалов можно, например, применять в тех случаях, когда прикладные программы и файлы данных должны находиться в безопасном месте и нет возможности их переноса на персональный компьютер.

Протокол Telnet функционирует поверх TCP/IP и имеет две важные особенности, отсутствующие в других эмуляторах: он присутствует практически в каждой реализации стека TCP/IP, а также является открытым стандартом (т. е. каждый производитель или разработчик легко может, реализовать его). Для некоторых реализаций Telnet нужно, чтобы хост был сконфигурирован как Telnet-сервер. Протокол Telnet поддерживается многими рабочими станциями, работающими под управлением MS-DOS, UNIX и любых версий Windows.

Для Telnet-коммуникаций используются специальный заголовок и поле данных, инкапсулированные в поле данных TCP-сегмента как показано на РИС. 6.8. Кроме того, для организации выделенного канала передачи данных Telnet задействует TCP-порт 23 на передающем и принимающем узлах.

Telnet имеет следующие коммуникационные опции:

- совместимость с 7- и 8-разрядными данными;
- возможность использования различных терминальных режимов;
- эхо-отображение символов на передающем и принимающем узлах;
- синхронные коммуникации;
- передача символов в виде потоков или по одному;
- управление потоком данных.

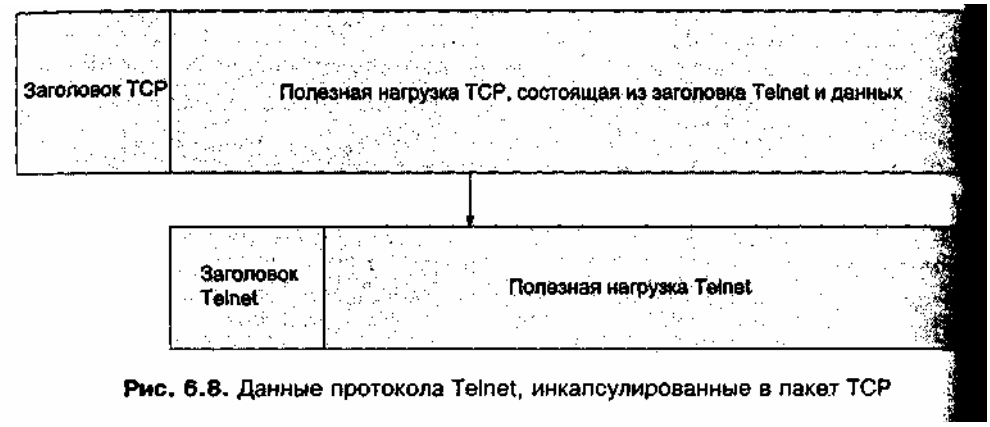


Рис. 6.8. Данные протокола Telnet, инкапсулированные в пакет TCP

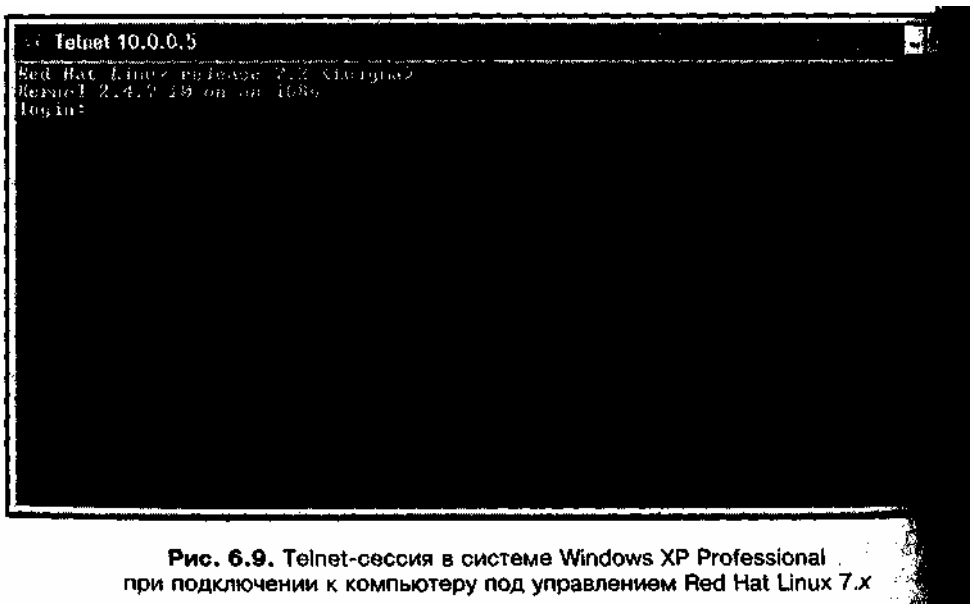


Рис. 6.9. Telnet-сессия в системе Windows XP Professional при подключении к компьютеру под управлением Red Hat Linux 7.*x*

Telnet обеспечивает единственный способ для получения доступа с одного компьютера к другому через сеть или Интернет. Например, программист работающий в системе Windows 2000/XP или Red Hat Linux *7.x,* может с помощью Telnet подключиться через Интернет к некоторому мэйнфрейму. Многие специалисты по мэйнфреймам IBM пользуются Telnet, что позволяет им работать на некотором хосте, расположенном на удалении сотен тысяч километров. Для решения других задач можно применять Telnet в системе Windows/XP для доступа к файлам, находящимся на компьютере UNIX (рис. 6.9), или наоборот. В практическом задании 6-5 рассказывается о том, как с помощью Telnet подключиться к компьютеру UNIX.

Совет

Систему Windows 2000 Server можно настроить для работы в качестве Telnet-сервера, при этом можно с помощью Telnet обращаться к хранящейся на ней информации с любого компьютера. В практическом задании 6-6 показано, как запустить Telnet-сервер в Windows 2000 Server.

File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP) и Network File System (NFS)

Стек TCP/IP содержит три протокола для передачи файлов: *File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP)* и *Network File System (NFS).* Самым распространенным протоколом является FTP, поскольку именно его чаще всего выбирают для передачи файлов пользователи Интернета. С помощью FTP можно, работая на компьютере в одном городе, подключиться к хост-компьютеру, расположенному в другом городе, и скачать один или несколько файлов. (При этом, конечно, нужно знать имя учетной записи и пароль для удаленного хоста.) Пользователи Интернета нередко с помощью FTP скачивают различные файлы (например, сетевые драйверы или обновления системы).

FTP – это приложение, позволяющее с помощью протокола TCP передать данные от одного удаленного устройства к другому. Как и в протоколе Telnet, заголовок FTP и соответствующие

данные инкапсулируются в поле полезной нагрузки пакета TCP. Преимущество FTP по сравнению с протоколами TFTP и NFS заключается в том, что FTP использует два TCP-порта: 20 и 21. Порт 21 – это управляющий порт для команд FTP, которые определяют способ передачи данных. Например, команда get служит для получения файла, а команда put используется для пересылки файла некоторому хосту. FTP поддерживает передачу двоичных или текстовых (ASCII) файлов, Для чего применяются команды binary и ascii. Порт 20 служит только для Передачи данных, задаваемых командами FTP. Некоторые команды FTP перечислены в табл. 6.2.

Таблица 6.2. *Примеры команд FTP*

Команда	Описание
ascii	Передавать файлы в формате ASCII Binary
binary	Передавать файлы в двоичном виде
bye или quit	Завершить сеанс передачи файлов и выйти из режима FTP
close	Завершить сеанс передачи файлов
delete	Удалить файл на другом компьютере
dir или Is	Вывести содержание каталога на другом компьютере
get	Получить файл с другого компьютера
help	Отобразить описание некоторой команды FTP
put	Послать файл на другой компьютер
pwd	Вывести текущее имя каталога другого компьютера
send	Переслать файл на другой компьютер

Примечание

FTP поддерживает передачу файлов в формате ASCII, что позволяет пересылать текстовые файлы, в которых отсутствуют, специальные символы. Для файлов, содержащих специальные или управляющие символы (например, файлы текстовых процессоров или электронных таблиц), используется режим передачи двоичных файлов.

FTP предназначен для передачи файлов целиком, что делает его удобным средством для пересылки через глобальную сеть файлов большого размера FTP не позволяет передать часть файла или некоторые записи внутри файла. Поскольку данные инкапсулированы в пакеты TCP, коммуникации с использованием FTP являются надежными и обеспечиваются механизмом служб с установлением соединения (что подразумевает отправку подтверждения после приема пакета). При FTP-коммуникациях выполняется передача одного потока данных, в конце которого следует признак конца файла (EOF).

Веб-браузеры (такие как Netscape Communication и Microsoft Explorer) позволяют очень легко работать с FTP, т. е. можно подключиться к сайту и пользоваться обычными средствами браузера (например, возможностями перетаскивания значков). Работа с браузером по протоколу FTP рассматривается в практическом задании 6-7.

TFTP – это файловый протокол стека TCP/IP, предназначенный для таких задач, как передача с некоторого сервера файлов, обеспечивающих загрузку бездисковой рабочей станции. Протокол TFTP не устанавливает соединений и ориентирован на пересылку небольших файлов в тех случаях, когда появление коммуникационных ошибок не является критичным и нет особых требований к безопасности. Отсутствие соединений при работе TFTP объясняется тем, что он функционирует поверх протокола UDP (через UDP-порт 69), а не с использованием TCP. Это означает, что в процессе передачи данных отсутствуют подтверждения пакетов или не задействованы службы с установлением соединений, гарантирующие успешную доставку пакетов в пункт назначения.

Распространенной альтернативой FTP являются программные средства Network File System (NFS) (сетевая файловая система), разработанные компанией Sun Microsystems. Для их работы используется предложенная компанией спецификация удаленных вызовов процедур через TCP-порт 111. NFS устанавливается как на передающий, так и на принимающий узлы, и поэтому NFS-программы одного компьютера могут запускать NFS-программы на другом компьютере. Система NFS, часто используемая в UNIX-системах, передает данные в виде потока записей, а не как последовательность целых файлов. Как и FTP, NFS является протоколом с установлением соединения и работает поверх протокола TCP. NFS особенно подходит для компьютеров, обрабатывающих большие объемы транзакций с использованием записей, хранящихся в файлах или базах данных. Также NFS можно применять в тех случаях, когда файлы данных распределены между несколькими серверами.

Simple Mail Transfer Protocol (SMTP)

Протокол *Simple Mail Transfer Protocol (SMTP)* предназначен для передачи сообщений электронной почты между сетевыми системами. С помощью этого протокола системы UNIX, OpenVMS, Windows и Novell NetWare могут пересылать электронную почту поверх протокола TCP.

SMTP можно рассматривать как альтернативу протоколу FTP при передаче файла от одного компьютера к другому. При работе с SMTP не нужно знать имя учетной записи и пароль для удаленной системы. Все, что нужно, – это адрес электронной почты принимающего узла. SMTP может пересылать только текстовые файлы, поэтому файлы в других форматах должны быть конвертированы в текстовый вид, только после этого их можно поместить в SMTP-сообщение.

Сообщения, пересылаемые с помощью SMTP, имеют две части: адресный заголовок и тело сообщения (текст). Адресный заголовок может быть очень Длинным, поскольку он содержит адреса всех SMTP-узлов, через которые передавалось сообщение, а также метку времени для каждого пересылочного Узла. Если принимающий узел недоступен, SMTP ждет некоторое время, а затем пытается переслать сообщение снова. В случае неудачи (если принимающий узел так и не стал доступным в течение заданного периода времени) сообщение возвращается отправителю.

SMTP отвечает стандартам TCP/IP, но не является совместимым с протоколом X.400, описывающим системы электронной почты. SMTP пересылается поверх протокола TCP, который обеспечивает надежность почтовой связи, благодаря наличию служб с установлением соединения. Для развертывания SMTP требуются SMTP-совместимые приложения электронной почты как на передающем, так и на принимающем узлах. SMTP-приложения выбирают некоторый сервер как основной почтовый шлюз, соединяющий рабочие станции и обрабатывающий очередь почтовых сообщений, хранящихся в некотором файловом каталоге или файле спулера печати. Эта очередь служит почтовым отделением, или почтовым доменом, для всех пользователей, подключающихся к данному серверу. Клиенты могут зарегистрироваться на сервере и получить свои сообщения, а сервер может также перенаправлять сообщения другим клиентам (рис. 6.10).

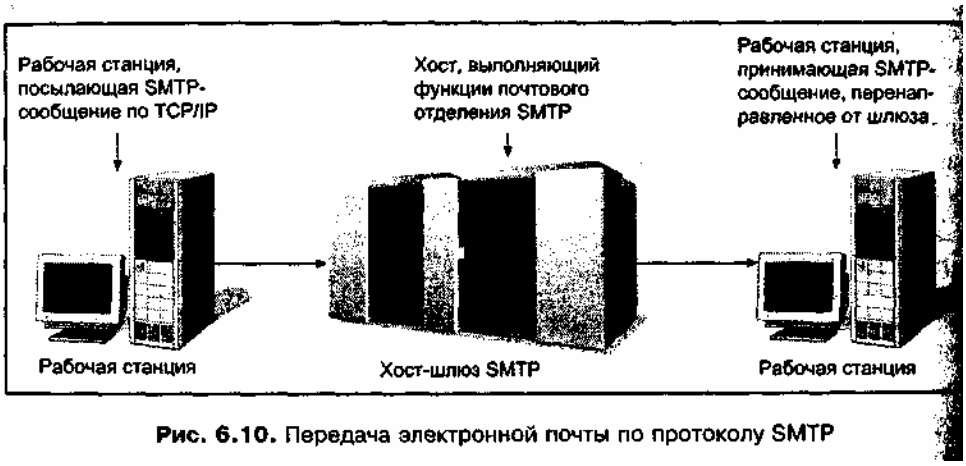


Рис. 6.10. Передача электронной почты по протоколу SMTP

Domain Name System (DNS)

Сетевые компьютеры часто группируются в домены. *Домен* (domain) – это логическое объединение сетевых ресурсов, таких как компьютеры, принтеры и сетевые устройства. Домену дается некоторое имя (например, компания Microsoft имеет домен Microsoft.com). Кроме того, уникальные имена получают все компьютеры в домене, эти имена иногда совпадают с именем пользователя.

В сети TCP/IP, использующей домены, каждый компьютер имеет некоторое доменное имя и IP-адрес. Клиенты сети для обращения к некоторому компьютеру обычно используют доменные имена, поскольку их запоминать легче, чем IP-адреса. Однако нужно заметить, что сама TCP/IP-сеть работает с IP-адресами, а не с именами компьютеров. Следовательно, если клиент хочет обращаться к определенному компьютеру по имени, должен быть не который механизм для преобразования компьютерных имен в соответствующие IP-адреса.

Domain Name System (DNS) (служба имен доменов) представляет собой службу стека TCP/IP, преобразующую имя компьютера или домена в IP-адрес или, наоборот, конвертирующую IP-адрес в компьютерное или доменное имя. Этот процесс называется разрешением (имен или адресов). Пользователям легче запоминать имена, а не IP-адреса в десятичном представлении с

разделительными точками, однако поскольку компьютерам все равно нужны IP-адреса, то должен быть способ преобразования одного способа адресации в другой. Для этого служба DNS использует таблицы просмотра, в которых хранятся пары соответствующих значений.

Примечание

В сетях Windows могут использоваться имена компьютеров и приложения, совместимые с NetBIOS. Для таких сетей помимо DNS-сервера устанавливается сервер службы Windows Internet Naming Service (WINS) (Служба имен Интернета для Windows), с помощью которой выполняется разрешение IP-адресов и NetBIOS-имен компьютеров.

Имя компьютера состоит из двух частей, что напоминает адрес IP-сети и идентификаторы хостов. Одна часть представляет собой имя компьютера или узла, а другая – имя организации, которое является основным доменным именем. Эти две части имени разделяются символом "@" ("коммерческое at", "собака"). Основное доменное имя нередко делится на элементы, разделяемые точкой, что может отражать имя организации, ее тип и страну, в которой эта организация располагается. Например, имя uwyo.edu используется Университетом Вайоминга (University of Wyoming, uwyo), который является образовательной организацией (edu).

Часть имени, соответствующая организации, называется именем домена, это указывает на то, что все частные имена в этой организации находятся в одном компьютерном домене. Крупные организации нередко имеют несколько Доменов. Например, большой университет может иметь домен для студентов (student.uwyo.edu) и домен для преподавателей (faculty) и сотрудников (staff) (fs.uwyo.edu). Интернет-имена доменных хостов состоят из двух или трех частей: доменного имени первого уровня (top-level domain, TLD) (т. е. названия страны или типа организации), необязательного имени субдомена (например, названия университета или компании) и имени хоста (например, имени хост-компьютера). Корневые имена доменов координирует и регистрирует специальная организация – Internet Corporation for Assigned Names and Numbers (ICANN).

В табл. 6.3 перечислены интернет-имена доменов первого уровня (TLD) для Различных типов организаций, а в табл. 6.4 перечислены TLD-имена для Некоторых стран. Табл. 6.5 содержит примеры новых предлагаемых TLD-имен (которые были предложены различными организациями, но еще не утверждены ICANN на момент написания этой книги).

Таблица 6.3. *Доменные имена первого уровня (TLD) для* организуй

Тип организаций	**Принятое доменное имя**
Воздушный транспорт	aero
Фирмы (от мелких до крупных), включая товарищества, частные компании и корпорации	biz
Различные коммерческие организации	com
Коммерческие кооперативы (принадлежащие работающим в них сотрудникам)	coop
Образовательные	edu
Правительственные	gov
Организации, занимающиеся регистрацией доменных имен	info
Организации, созданные согласно международным договорам	int
Музейные	museum
Домены для личного пользования	Name
Поставщики сетевых услуг	net
Некоммерческие	org
Профессиональные (например, объединения врачей, бухгалтеров или юристов)	pro

Таблица 6.4. *Доменные имена ДМШ*

Страна	**Принятое доменное имя**	**Страна**	**Принятое доменное имя**

Страна	Принятое доменное имя	Страна	Принятое доменное имя
Австралия	au	Иордания	jo
Канада	ca	Мозамбик	mz
Чили	cl	Нигерия	ng
Финляндия	fi	Польша	po
Франция	fr	Катар	qa
Венгрия	hu	Самоа	ws
Италия	it	Швеция	se
Япония	jp	Объединенные Арабские Эмираты	ae
Соединенное Королевство Великобритании и Северной Ирландии	uk	Соединенные Штаты Америки	us

Таблица 6.5. *Предлагаемые глобальные доменные имена первого уровня (TLD)*

Тип организаций	Предлагаемое доменное имя
Организации, связанные с искусством	arts
Фирмы, занимающиеся продажей товаров	shop или mail
Организации, связанные с развлечениями и отдыхом	rec
Различные производственные организации и фирмы	firm
Индивидуальные варианты имен для особых организаций	nom
Универсальная идентификация по телефонному номеру	tel
Профсоюзы	union
Здравоохранение	health

Распознаватели имен DNS и пространства имен

Для работы службы DNS необходимы распознаватели доменных имен на каждом клиенте, а также сервер доменных имен, установленный на одном или нескольких хостах. DNS-серверы поддерживают *пространство имен* (namespace) для предприятия и реализуют механизм разрешения имен компьютеров и доменов в IP-адреса, а также и обратное преобразование. Пространство имен представляет собой логическую область сети, содержащую перечень именованных объектов (например, компьютеров) и позволяющую выполнять разрешение имен.

Использование зон

DNS-серверы поддерживают информационные таблицы, с помощью которых имена компьютеров или доменов связаны с IP-адресами. Эти таблицы ассоциируются с разделами DNS-сервера, называемыми *зонами* и содержащими ресурсные записи. Каждая зона представляет собой таблицу (файл зоны или базу данных зоны) ресурсных записей различного типа (например, записей, связывающих серверы домена со службами; которые на этих серверах функционируют). Другие ресурсные записи связывают имена компьютеров и IP-адреса.

Зона, ассоциирующая имена компьютеров с соответствующими JH адресами, называется зоной прямого просмотра (forward lookup zone). Эта зона содержит записи имен хостов, называемые адресными записями. Каждый сервер и клиент IP-сети должен иметь адресную запись, позволяющую найти его с помощью DNS. Например, если DNS-сервер называется NetAdmin и имеет адрес 129.70.10.1, то зона прямого просмотра связывает имя NetAdmin с адресом 129.70.10.1. Для протокола IPv4 запись хоста называется ресурсной записью адреса хоста (типа A) (host address (A) resource record). Для протокола IPv6 такая запись называется ресурсной записью адреса хоста (типа AAAA) (IPv6 host address (AAAA) resource record).

Примечание

При установке службы каталога (например, Active Directory) вы должны иметь в сети хотя бы один

DNS-сервер, поскольку эта служба является частью пространства имен, используемого для хранения информации о сетевых объектах (таких как компьютеры, принтеры и общие ресурсы). Для обновления этой информации служба каталога должна взаимодействовать с DNS-сервером.

В другой зоне, называемой *зоной обратного просмотра* (reverse lookup zone) хранятся *ресурсные записи указателей (типа PTR)* (pointer (PTR) resourse record), которые связывают IP-адреса с именами хостов. Зоны обратного просмотра используются не так часто, как зоны прямого просмотра, однако не следует создавать в тех случаях, когда для обеспечения сетевых коммуникаций требуется связывать IP-адрес с некоторым компьютерным именем (например для мониторинга сети с использованием IP**-адресов**).

Роли DNS-серверов

Обычно DNS-сервер в сети играет одну из двух ролей: он может выступать или в качестве основного DNS-сервера, или выполнять функции дополнительного DNS-сервера. *Основным DNS-сервером* (primary DNS server) считается сервер, отвечающий за некоторую зону и поэтому называющийся авторитетным (authoritative) сервером для этой зоны. Например, если на некотором DNS-сервере первый раз создается зона прямого просмотра ДД домена mybusiness.com, то при этом создается *ресурсная запись начала зоны (SOA)* (start of authority (SOA) resource record), идентифицирующая данный сервер в качестве авторитетного DNS-сервера для домена mvbusiness.com., Это означает, что все изменения зоны (например, создание ресурсных записей адреса хоста (типа A)) должны выполняться на этом сервере.

В средних и крупных сетях обычно устанавливают один или несколько резервных DNS-серверов, называемых (по отношению к основному DNS-се веру) *дополнительными,* или вторичными *DNS-серверами* (secondary DNS server). Дополнительный DNS-сервер содержит копию файла зоны, хранящейся на основном DNS-сервере, при этом данная копия не может использоваться для административных задач. Для обновления копии выполняются пересылки зоны по сети. В процессе пересылки зоны содержимое зоны передается с основного DNS-сервера на дополнительный.

Дополнительные DNS-серверы выполняют три важные задачи. Во-первых, они позволяют получить копию данных основного DNS-сервера в случае отказа этого сервера. Во-вторых, они позволяют распределять нагрузку на службу DNS (позволяя обращаться к общим ресурсным записям) между основным и дополнительными DNS-серверами. Распределение нагрузки означает, что если из-за перегрузки основной DNS-сервер не может выполнить разрешение имени, то повторный запрос на разрешение имени может быть обработан дополнительным DNS-сервером, что ускоряет получение ответов на запросы клиентов. В-третьих, дополнительные DNS-серверы можно разместить в разных областях сети (например, в разных подсетях или на территориально удаленных площадках), в результате чего снижается нагрузка на отдельные участки сети.

Совет

Для обеспечения отказоустойчивости в средних и крупных сетях рекомендуется создать по меньшей мере по одному дополнительному ONS-серверу в каждой подсети, отличной от той подсети, где находится основной DNS-сервер.

Чтобы познакомиться с зонами, ресурсной записью начала зоны (SOA) и другой информацией, хранящейся на DNS-сервере, выполните практическое задание 6-8.

Стандарты DNS

Авторитетные серверы обычно поддерживают два стандарта DNS: ресурсные записи служб и протокол динамического обновления DNS. *Ресурсная запись службы (типа SVR)* (service resource record (SVR RR)) описана в RFC 2052 и представляет собой тип DNS-записи, позволяющей DNS распознавать различные серверы и определять местоположение широко используемых служб TCP/IP, выполняющихся на конкретных серверах. SRV-записи позволяют DNS-серверу генерировать список серверов сети, предоставляющих услуги TCP/IP-сервисов. Также эти записи сообщают о протоколах, поддерживаемых этими серверами, и позволяют определить предпочтительный сервер для некоторой службы. Формат SRV-записи содержит информацию о типе службы, выполняющейся на некотором сервере, имени домена, который обслуживается этим сервером, а также о протоколе, используемом сервером.

Протокол динамического обновления DNS (DNS dynamic update protocol) описан в RFC 2136, с его

помощью можно автоматически обновлять информацию на 1 DNS-сервере. Примером может служить рабочая станция под управлением Windows XP Professional, обновляющая свой IP-адрес, полученный от сервера DHCP. Протокол динамического обновления DNS может сэкономить сетевому администратору массу времени, поскольку ему не понадобится вручную регистрировать каждую новую рабочую станцию или выполнять регистрация компьютера каждый раз по истечении срока арендованного ему 1P-адресзи при получении нового адреса.

Совет

В сети, где работает служба Microsoft Active Directory, SRV-записи позволяют рабочим станциям быстро находить ближайший сервер для аутентификации запросов входа в сеть. Это -позволяет уменьшить ненужный сетевой трафик.

Dynamic Host Configuration Protocol (DHCP)

Протокол *Dynamic Host Configuration Protocol (DHCP)* (Протокол динамически конфигурации хоста) позволяет автоматически назначать в сети 1P-адреса с помощью DHCP-сервера. Когда новый компьютер, настроенный на работу с DHCP, подключается к сети, он обращается к DHCP-серверу, который выделяет (сдает в аренду) компьютеру IP-адрес, передавая его посредством протокола DHCP. Длительность аренды устанавливается на DHCP-сервере сетевым администратором. Например, срок аренды для настольного компьютера может составлять от нескольких дней до нескольких недель (поскольку компьютер постоянно подключен к сети). Срок аренды для портативного компьютера может составлять от нескольких часов до одного дня (поскольку портативный компьютер часто отключается от сети или перемещается на другие участки сети). И, наконец, хост-компьютер или сервер может получить адрес в бессрочную аренду, т. к. их адрес никогда не меняется.

Совет

Чтобы упростить сетевое администрирование, устанавливайте совместимые друг с другом серверы DNS и DHCP, которые поддерживают протокол динамического обновления DNS. Это гарантирует автоматическое обновление DNS зон DHCP-сервером или клиентами DHCP и освобождает администратора от необходимости делать это вручную.

Address Resolution Protocol (ARP)

В большинстве случаев для отправки пакета принимающему узлу отправитель должен знать как IP-адрес, так и MAC-адрес. Например, при групповых передачах используются оба адреса (IP и MAC). Эти адреса не моя совпадать и имеют разные форматы (десятичный с разделительными точками и шестнадцатеричный соответственно).

'Ш

Address Resolution Protocol (ARP) (Протокол разрешения адресов) позволяет передающему узлу получить MAC-адреса выбранного принимающего узла перед отправкой пакетов. Если исходному узлу нужен некоторый MAC-адрес, то он посылает широковещательный ARP-фрейм, содержащий свой собственный MAC-адрес и IP-адрес требуемого принимающего узла. Принимающий узел отправляет обратно пакет ARP-ответа, содержащий свой MAC-адрес.

Вспомогательным протоколом является *Reverse Address Resolution Protocol (RARP)* (Протокол обратного разрешения имен), с помощью которого сетевой узел может определить свой собственный IP-адрес. Например, RARP используется бездисковыми рабочими станциями, которые не могут узнать свои адреса иначе как выполнив RARP-запрос к своему хост-серверу. Кроме того, RARP используется некоторыми приложениями для определения IP-адреса того компьютера, на котором он выполняются.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) (Простой протокол сетевого управления) позволяет администраторам сети непрерывно следить за активностью сети. Протокол SNMP был разработан в 1980-х годах для того, чтобы снабдить стек TCP/IP механизмом, альтернативным стандарту OSI на управление сетями – протоколу *Common Management Interface Protocol (CMIP)* (Протокол общей управляющей информации).

Хотя протокол SNMP был создан для стека TCP/IP, он соответствует эталонной модели OSI. Большинство производителей предпочли использовать SNMP, а не CMIP, что объясняется большой популярностью протоколов TCP/IP, а также простотой SNMP. Протокол SNMP поддерживают многие сотни сетевых устройств, включая файловые серверы, карты сетевых

адаптеров, маршрутизаторы, повторители, мосты, коммутаторы и концентраторы. В сравнении с этим, протокол CMIP применяется компанией IBM в некоторых сетях с маркерным кольцом, однако во многих других сетях он не встречается.

Достоинства SNMP

Важным достоинством SNMP является то, что он работает независимо от сети, т. е. ему не нужно двунаправленное соединение с другими сетевыми объектами на протокольном уровне. Благодаря этому SNMP может анализировать сетевую активность, например, обнаруживать неполные пакеты и отслеживать широковещательные посылки, при этом на его работе не сказывается ошибочная информация, которая может поступить от неисправного Узла. По сравнению с этим, протокол CMIP подключается к сетевым узлам на уровне протокола, и это означает, что его способность обнаруживать проблемы зависит от работоспособности некоторого узла, который может оказаться неисправным.

•*А*

Еще одно достоинство SNMP состоит в том, что контрольные функции выполняются на некоторой станции управления сетью. В этом SNMP отличается от протокола CMIP, для которого функции управления распре делены между отдельными сетевыми узлами, которые одновременно являются и объектами мониторинга. Кроме того, SN.MP требует меньше оперативной памяти, чем CMIP. Для работы CMIP нужно до 1,5 Мбайт памяти на каждом исследуемом узле, а SNMP требует только 64 Кбайт.

Типы узлов, используемых протоколом SNMP

Протоколом SNMP предусмотрены два типа узлов: станция управления сетью (network management station, NMS) и агенты сети (network agents). Станция управления сетью следит за сетевыми устройствами, поддерживающими SNMP. На этих устройствах выполняется агентское программное обеспечение, взаимодействующее со станцией. Большинство устройств, подключаемых к современным сетям, являются агентами. К их числу относятся маршрутизаторы, повторители, концентраторы, коммутаторы, мосты, персональные компьютеры (через свои сетевые адаптеры), серверы печати, серверы доступа и источники бесперебойного питания.

С помощью консоли на станции управления сетью можно посылать команды сетевым устройствам и получать данные о производительности (статистику). Станция управления сетью может построить блок-схему всей сети. Если в сети появляется новое устройство, станция может немедленно его обнаружить. Программные средства станции управления сетью могут обнаружить момент когда агент выключен или работает неверно. Значок такого агента может высвечиваться на блок-схеме другим цветом или может раздаваться предупредительный сигнал. Обычно программы станции управления сетью имеют графический пользовательский интерфейс и с ними очень легко работать.

Многие программные пакеты станций управления сетью могут в графическом виде предоставлять показания счетчиков, отображающих степень использования сети, поток пакетов и другие статистические данные. При возникновении неисправности графические обозначения помогают понять серьезность проблемы и определить тип отказавшего агента. Некоторые пакеты имеют интерфейсы прикладного программирования (API), позволяющие взаимодействовать с программным обеспечением и запрограммировать специфические задачи с использованием простого языка (например, Visual Basic).

Каждый агент сети хранит информационную базу, содержащую количество посланных или полученных пакетов, число пакетных ошибок и другие данные. Такая база называется базой управляющей информации (Management Information Base, MIB). У станции управления сетью имеется множество команд, позволяющих обращаться к данным этой базы и управлять ею. Такие команды передаются с помощью OSI-совместимых модулей данных протокола (PDU) и содержат тип сообщения (например, запрос на получение, запрос на получение следующих данных, ответ на запрос, запрос на присваивание значения и системное прерывание). Получаемые данные позволяют определить, включено ли устройство и имеются ли сетевые проблемы. Станция управления сетью обеспечивает даже удаленную перезагрузку устройства. Сообщения между станцией и агентом передаются поверх протокола UDP, к пакетам которого добавляется заголовок SNMP. Полезная нагрузка SNMP содержит *групповое имя* (community name), представляющее собой некоторый пароль, общий для станции управления сетью и агента.

В базе управляющей информации хранятся сведения о сетевых объектах (таких как рабочие станции, серверы, мосты, маршрутизаторы, концентраторы и повторители). Основной набор

переменных, содержащихся в этой базе, представлен в табл. 6.6. Изначально таблица базы MIB была описана в стандарте Management Information Base-I. Этот стандарт определяет сведения об устройстве и множество соответствующих переменных. Стандарты MIB разрабатываются Проблемной группой проектирования Интернета (IETF).

Таблица 6.6. *Переменные базы управляющей информации (MIB)*

Переменные MIB	Назначение
Address translation group (группа преобразования адресов)	Преобразует сетевые адреса в адреса подсетей или физические адреса
Electronic gateway protocol group (Группа шлюзового протокола электронных устройств)	Обеспечивает сведения об узлах в том же сегменте, в котором находится агент сети
Interfaces group (Группа интерфейсов)	Отслеживает количество сетевых адаптеров и количество подсетей
Internet control message protocol group (Группа протокола управляющих сообщений Интернета)	Собирает данные о количестве. сообщений, посланных агентом и полученных им
Internet protocol group (Группа протокола Интернета)	Отслеживает количество входных принятых датаграмм и количество отвергнутых датаграмм
SNMP group (Группа SNMP)	Собирает данные об обращениях к базе MIB
System group (Системная группа)	Содержит информацию об агенте сети
Transmission control protocol group (Группа протокола управления передачей)	Предоставляет информацию о TCP-соединениях в сети, включая данные об адресах и тайм-аутах
User datagram protocol group (Группа пользовательского протокола данных)	Предоставляет информацию о слушающем агенте, с которым станция управления сетью взаимодействует в данный момент

Новый, более совершенный стандарт MIB-II описывает дополнительные средства безопасности, поддержку сетей с маркерным кольцом и высокоскоростных интерфейсов, а также поддержку для телекоммуникационных интерфейсов. Стандарт MIB-II принят многими производителями сетевого оборудования.

Новые возможности протокола SNMPv2

Первая версия протокола SNMP имела некоторые недостатки, которые были устранены во второй версии, названной SNMPv2. Возможно, главным из недостатков SNMP является отсутствие механизмов защиты. При использовании SNMP групповое имя передается станцией управления сетью без шифрования и в случае перехвата этот пароль можно использовать для получения доступа к важным командам управления сетью. В результате такой утечки злоумышленник может удаленно изменить настройки маршрутизатора или концентратора и дискредитировать безопасность сети.

SNMPv2 позволяет шифровать групповое имя, улучшить обработку ошибок и обеспечить взаимодействие со многими протоколами. Он поддерживает также IPX и AppleTalk. Кроме того, SNMPv2 обеспечивает быструю передачу информации и позволяет одновременно получать больше данных из базы MIB-II.

Мониторинг с использованием протоколов SNMP и SNMPv2

Протоколы SNMP и SNMPv2 можно применять для управления любыми сетями: локальными, глобальными и смешанными. Имеется множество средств и программных пакетов для сетевого мониторинга, которые используют SNMP и SNMPv2. В их число входят программы Sniffer компании Network Associates (см. **www.sniffer.com)** и Network Monitor компании Microsoft (см. www.microsoft.com).

Важным SNMP-совместимым инструментом, используемым для мониторинга локальных сетей, соединенных через глобальные сети, является разработанный в начале 1990-х годов стандарт *Remote Network Monitoring (RMON)* (удаленный мониторинг сети). RMON не только использует протокол SNMP, но также

задействует специальную базу данных для удаленного мониторинга, называемую RMON MIB-II. Эта база позволяет удаленным сетевым узлам собирать сетевую статистику практически в любой точке локальной или глобальной сети. Эти удаленные узлы являются агентами, или зондами. Информация, полученная агентами, может быть передана на некоторую станцию управления, которая заносит ее в базу данных. В настоящее время стандарты RMON MIB-II адаптированы к сетям FDDI, Ethernet и Token Ring.

Другие прикладные протоколы стека TCP/IP

Имеются и другие протоколы или прикладные программы, входящие в стек TCP/IP- Они упрощают работу интернет-служб, передачу данных мультимедиа-приложений, управление сетью и поиск неисправностей. Эти дополнительные протоколы и приложения перечислены в табл. 6.7.

Таблица 6.7. *Приложения и протоколы стека TCP/IP*

Протокол или приложение	Описание
Archie	Приложение, позволяющее пользователю стека TCP/IP находить FTP-сайты, содержащие информацию по определенной тематике
Bootstrap Protocol (BOOTP)	Протокол, используемый бездисковыми рабочими станциями для определения своего IP-адреса и для взаимодействия с сервером, с которого копируются файлы операционной системы, необходимые для загрузки этих станций
Distance Vector Multicast Routing Protocol (DVMRP)	Протокол групповой маршрутизации, используемый вместе с протоколом RIP для определения узлов, подписанных на определенные групповые посылки приложений мультимедиа *(см. главу 10)*
Finger	С помощью данной утилиты сетевой пользователь может определить, какие еще пользователи и хосты активны в сети
Gopher	Приложение, предлагающее список тем, из которых пользователи могут получить доступ к другому меню или текстовым файлам (например, к файлу, содержащему список телефонов). В настоящее время службы Gopher встречаются редко, поскольку, в первую очередь, их заменили веб-серверы
Hypertext Transfer Protocol (HTTP)	Протокол для передачи документов HTML (Hypertext Markup Language) через Интернет по запросам от веб-браузеров; эти документы могут включать в себя аудио- и видеофайлы, а также изображения и графику
Internet Group Management Protocol (IGMP)	Протокол, позволяющий передавать групповые пакеты их получателям и маршрутизаторам. Определяет, какие рабочие станции принадлежат к определенной группе мультивещания *(см. главу 10)*
Multicast Open Shortest Path First Protocol (MOSPF)	Протокол групповой маршрутизации, позволяющий определить кратчайший маршрут от источника к пункту назначения при групповых передачах
Open Shortest Path First Protocol (OSPF)	Протокол, используемый маршрутизаторами для обмена данными таблиц маршрутизации и для оценки сетевых маршрутов при передаче данных с учетом определенных критериев (например, стоимости маршрута)
Ping	Утилита, позволяющая сетевому узлу взаимодействовать с другим узлом, находящимся в той же или в удаленной сети, и определять, имеется ли связь с указанным узлом и отвечает ли тот на запросы. Сетевой администратор может использовать утилиту ping для быстрой проверки соединений с глобальной сетью связываясь с каким-нибудь удаленным узлом

Протокол или приложение	Описание
Real-Time Protocol (RIP)	Этот протокол служит для эффективного управления групповым потоковым мультивещанием, ведущимся в реальном масштабе времени и используемым для организации видеоконференций или для работы аналогичных приложений мультимедиа *(см. главу 10)*
Real-Time Transport Control Protocol (RTCP)	Позволяет управлять сетевым трафиком, упрощая использование приложений мультимедиа, работающих в реальном масштабе времени *(см. главу 10)*
Resource Reservation Protocol (RSVP)	Протокол, позволяющий выделять сетевые ресурсы для определенных приложений (например, резервировать полосу пропускания для приложений мультимедиа) *(см. главу 10)*
Routing Information Protocol (RIP)	С помощью данного протокола маршрутизаторы передают друг другу содержание таблиц маршрутизации и определяют наименьшее количество ретрансляций от одного узла сети к другому
Simple Network Management Protocol (SNMP)	Протокол, обеспечивающий сбор сетевой статистики, хранит эту информацию в базе данных
Traceroute (tracert)	Приложение, позволяющее пользователю определить количество ретрансляций между двумя узлами сети

В практических заданиях 6-9 и 6-10 вы можете попрактиковаться в работе с командой ping, а в заданиях 6-11 и 6-12 вы узнаете, как с помощью команд tracert и ping определить количество ретрансляций от одной точки сети до другой.

Сравнение архитектуры стека TCP/IP и эталонной модели OSI

Как показано на рис. 6.11, компоненты стека TCP/IP, о которых рассказывалось в этой главе, соответствуют уровням эталонной модели OSI. По мере развития стека TCP/IP его компоненты все в большей степени следуют модели OSI. Например, на Физическом и Канальном уровнях стек TCP/IP совместим с сетями Ethernet, Token Ring, FDDI и ATM, а также с шинными сетями с передачей маркера (token bus). На Физическом уровне стек TCP/IP поддерживает коаксиал, витую пару и оптоволокно, а также беспроводные коммуникации. Кроме того, на Канальном уровне стек совместим со стандартом IEEE 802.2 на управление логическим каналом и MAC-адресацию.

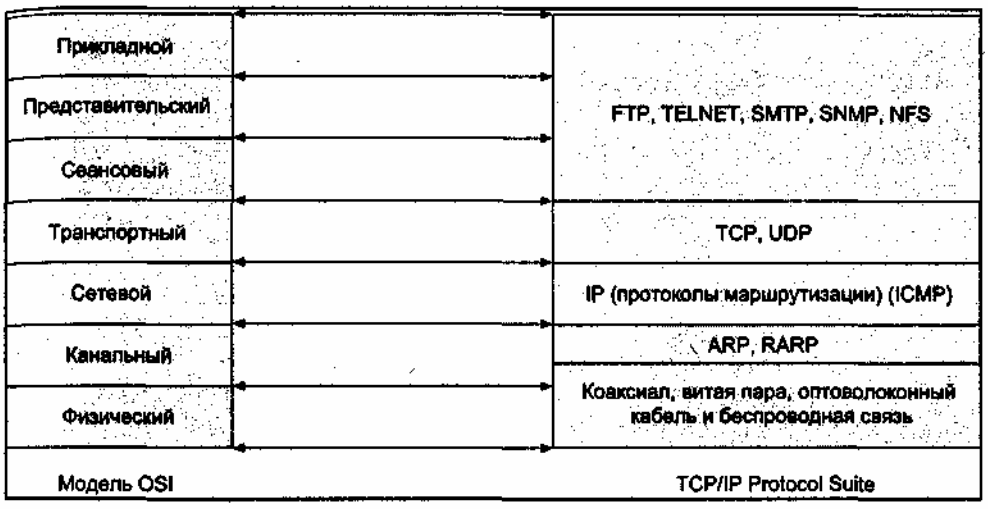


Рис. 6.11. Стек TCP/IP и эталонная модель OSI

Эквивалентом Сетевого уровня в стеке TCP/IP является протокол IP. Следующим уровнем совместимости служит Транспортный уровень, на этом уровне могут работать оба протокола – TCP и UDP. Верхние уровни модели OSI представляются прикладными протоколами TCP/IP. Например, протокол Telnet функционирует на уровне, эквивалентном Сеансовому, а протоколы

SMTP и FTP работают на уровнях, аналогичных Представительскому и Прикладному уровням OSI.

Резюме

- TCP/IP является самым распространенным в мире сетевым протоколом. Он является основой для Интернета и позволяет взаимодействовать между собой миллионам компьютеров и серверов, расположенных по всей планете. Протокол TCP был создан для надежной передачи данных, для чего устанавливаются соединения между узлами и используются сигналы, подтверждающие прием пакетов.
- Протокол UDP является альтернативой TCP. За счет того, что соединения между узлами не устанавливаются, он генерирует меньше служебной информации, но при этом менее надежен, чем TCP. Для передачи пакетов принимающим узлам в локальных и глобальных сетях применяется протокол IP. Он имеет методы адресации для идентификации узда и сети, в которой тот находится. Последней версией IP является протокол IPv6, имеющий расширенный формат адреса, что позволяет охватить большое количество новых адресов сетей и узлов, которые появляются, благодаря быстрому росту Интернета и различных сетей.
- Для надежной доставки пакета необходимо, чтобы каждый IP-адрес был уникальным. Для идентификации конкретного узла и сети, к которой он принадлежит, используются методы адресации IP.
- Важно понимать, что главное назначение протокола IPv6 – обеспечит логический переход от IPv4, чтобы приложения и сетевые устройства могли справляться с новыми требованиями по мере их возникновения
- Фактически TCP/IP является стеком протоколов и приложений, предоставляющих важные возможности. Для подключения рабочих станций к хост-компьютерам используется протокол Telnet (при этом рабочие станции выступают в роли терминалов). FTP – протокол, который миллионы клиентов используют ежедневно для загрузки файлов из Интернета. Протокол SMTP обеспечивает работу почтовых служб, а DNS преобразует имена компьютеров в их IP-адреса. Протокол DHCP автоматически назначает IP-адреса сетевым компьютерам. Протокол SNMP важен для сетей, поскольку может собирать информацию о производительности сети и может использоваться для поиска неисправностей. Протокол ARP позволяет компьютерам или устройствам определять MAC-адрес другого компьютера или устройства.
- Количество интернет-программ, приложений локальных и глобальных сетей, а также их возможности продолжают расти. Протокол TCP/IP сыграл важную роль в развитии сетей, и в будущем его значение сохранится. По мере того как увеличивается число пользователей сетей и сетевых приложений, да к тому же растет пропускная способность сетей, протокол TCP/IP, по всей вероятности, будет существенно модифицироваться особенно когда все большее число клиентов будут использовать Интернет-телевидение, голосовые технологии IP-сетей и средства мультимедиа
- Нужно заметить, что по мере развития протокола TCP/IP некоторые его компоненты стали в большей степени соответствовать эталонной модели OSI.

Глава 7

Методы передачи данных в глобальных сетях

По прочтении этой главы и после выполнения практических заданий вы сможете:

- объяснить основы протокола X.25 и понять, как реализуются подключения к глобальным сетям X.25;
- рассказать о том, как ретрансляция кадров используется в глобальных сетях;
- описать способы применения коммуникаций ISDN для сетей, передающих данные, аудио- и видеосигналы, а также объяснить, как подключиться к сети ISDN;
- объяснить принципы службы SMDS и рассказать о том, как она реализуется;
- описать использование линий DSL в высокоскоростных сетях;
- объяснить, как работает сеть SONET и как она реализована;
- описать региональные Ethernet-сети;
- обсудить дополнительные протоколы глобальных сетей (SLIP, PPP и SS7).

Для быстрого обмена информацией по совместным исследованиям в 1980-х годах ученые имели в своем распоряжении только электронную почту, передаваемую по сети BITNET. В настоящее время исследователи могут в реальном масштабе времени передавать своим коллегам видеоданные о Результатах своих разработок, при этом зрители могут находиться в других странах или на других континентах. Теперь врачи регулярно осваивают новые медицинские технологии с помощью обучающих программ, транслируемых через Интернет. Эти и многие другие формы трансконтинентальных Коммуникаций стали возможными благодаря развитию технологий высокоскоростных глобальных сетей, которые соответствуют общим стандартам, Принятым во всем мире. По мере роста пропускной способности сетей эти технологии предоставляют все новые и новые коммуникационные возможности глобальной связи. В этой главе вы познакомитесь с технологиями глобальных сетей: одни из этих технологий уже существуют многие годы, другие еще только развиваются. Одной из старейших технологий глобальной связи являются сети X.25**,** которые по-прежнему часто применяются вместе с давно существующими локальными сетями. Вы узнаете о сетях с ретрансляцией кадров и ISDN, представляющих собой распространенные технологии глобальных сетей, разработанные в 1970-х и 1980-х годах и достигшие зрелости в 1990-х годах. Также вы познакомитесь с еще более новыми технологиями глобальной связи, в число которых входят служба SMDS, каналы DSL, сети SONET и региональные Ethernet-сети. Эти технологии используются во многих регионах для реализации скоростных глобальных сетей. И, наконец, будут рассмотрены три протокола глобальных сетей – SLIP, PPP и SS7 – часто применяемые во многих глобальных сетях.

СетиX.25I

Протокол *X.25* (также называемый Recommendation X.25) является одним из старейших протоколов глобальных сетей и реализован на основе методов коммутации пакетов, которые были разработаны в 1960-х и 1970-х годах (с коммутацией пакетов вы познакомились в *главе 2).* В 1976 году этот протокол был одобрен Международным консультативным комитетом по телеграфии и телефонии, МККТТ (Consultative Committee on International Telegraph and Telephone, CCITT, ныне International Telecommunications Union, ITU-T), для использования в международных *сетях передачи данных общего пользования* (Public Data Network, PDN). Главным образом протокол X.25 описывает, как данные пересылаются от *терминального оборудования* (Data Terminal Equipment, DTE) (например, от компьютера) к *аппаратуре передачи данных* или *телекоммуникационному оборудованию* (Data Circuit Equipment, DCE) (например, к коммутатору пакетов или устройству доступа к сети общего пользования). Протокол X.25 обеспечивает двухточечные коммуникации с установлением соединения, для чего в состав протокола включены механизмы проверки

целостности соединений глобальной сети и средства, гарантирующие доставку каждого пакета в заданную точку.

При своем появлении коммерческая служба линий X.25 имела максимальную скорость передачи, равную 64 Кбит/с. В 1992 году союз ITU-T обновил стандарты X.25 и включил в него поддержку скоростей до 2048 Мбит/с. X.25 не является протоколом скоростных глобальных сетей, однако он имеет следующие характеристики:

- широкое распространение;
- надежность;
- возможность подключения устаревших локальных сетей к глобальным сетям;
- возможность подключения к глобальной сети устаревших мэйнфреймов и мини-компьютеров.

Примечание

Существует несколько протоколов, которые работают в сочетании с X.25, однако технически не описаны как часть данного интерфейса. В качестве примера можно назвать протокол X.75, описывающий способ соединения между собой отдельных сетей X.25.

X.25 и эталонная модель OSI

Хотя протокол X.25 появился раньше, чем модель OSI, спецификации ITU-T описывают многоуровневые коммуникации между терминальным оборудованием (DTE) и аппаратурой передачи данных (DCE). Эти коммуникации соответствуют первым трем уровням модели OSI, что отображено на рис. 7.1. Уровни X.25 описаны ниже.

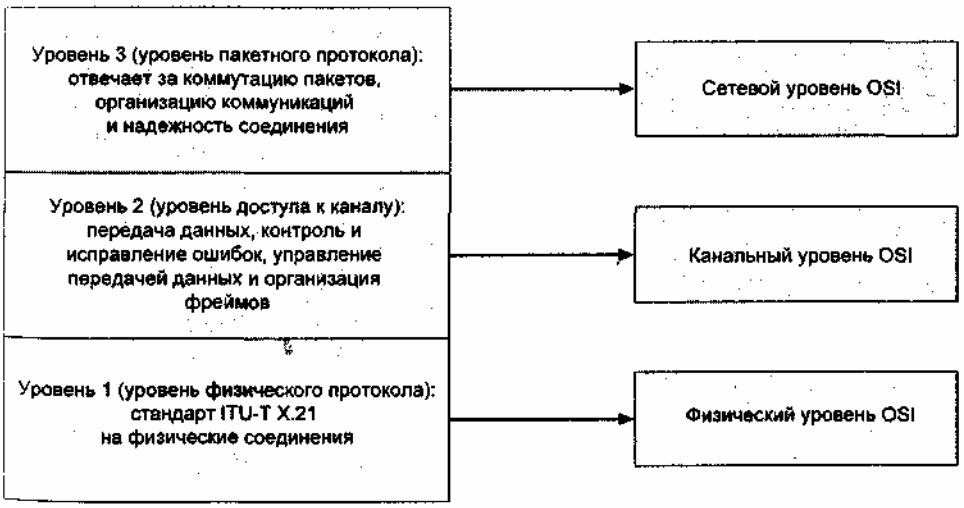


Рис. 7.1. Уровни коммуникаций X.25 в сравнении с эталонной моделью OSI

- Уровень физического протокола X.25 (Уровень 1) – использует интерфейс, определенный стандартом ITU-T X.21. Уровень физического протокола определяет сопряжения физических и электрических параметров коммуникационных адаптеров и передающего кабеля. На этом уровне для передачи фреймов используются синхронные коммуникации и задаются уровни напряжений, форматы представления разрядов данных, а также сигналы синхронизации и управления. Физически интерфейс, определенный стандартом X.21, представляет собой 15-штырьковый разъем. Два провода интерфейса используются для синхронизации, еще два – для передачи управляющей информации и еще два – для передачи данных.
- Уровень доступа к каналу X.25 (Уровень 2) – соответствует подуровню MAC Канального уровня модели OSI. Уровень доступа к каналу управляет передачей данных, адресацией, обнаружением и исправлением ошибок. Также он отвечает за управление каналом и формирование фрейма ИХ.25. В его состав входит протокол Link Access Procedure-Balanced

(LAPB) (Сбалансированные операции доступа к каналу), используемый для установления и разрыва виртуальных соединений через глобальную сеть. Виртуальное соединение представляет собой логическое соединение между двумя точками коммуникационной среды. По одному физическому подключению (или передающему кабелю) можно установить несколько виртуальных соединений X.25. Протокол LAPB также обеспечивает очередность передачи фреймов (чтобы они принимались в том же порядке, в каком были переданы) и проверяет их целостность.

- Уровень пакетного протокола X.25 (Уровень 3) – аналогичен Сетевому уровню модели OSI. Этот уровень упорядочивает процесс обмена информацией и обеспечивает надежность виртуального соединения. По одному физическому соединению одновременно может коммутироваться до 4095 виртуальных соединений. Уровень 3 обеспечивает выполнение следующих важных функций:

- создает два логических канала между терминальным оборудованием (DTE) (таким как хост-компьютер) и аппаратурой передачи данных (DCE) (например, адаптером X.25). Один канал предназначен для отправителя, а другой – для приемника;

- создает виртуальные маршруты из логических Каналов и связанных с ними интерфейсов сетевых устройств;

- мультиплексирует (коммутирует) коммуникационные сеансы при наличии нескольких пользователей сети X.25.

Методы передачи информации в сетях X.25

Пакеты данных в сетях X.25 могут передаваться с помощью одного из трех методов: по коммутируемым виртуальным каналам, по постоянным виртуальным каналам и с помощью датаграмм. Коммутируемый виртуальный канал (switched virtual circuit, SVC) представляет собой двунаправленный канал установленный между узлами через некоторый коммутатор X.25. Канал – это логическое соединение, которое устанавливается только на время передачи данных. По завершении передачи канал может стать доступным для других узлов.

Постоянный виртуальный канал (permanent virtual circuit, PVC) – это логический коммуникационный канал, поддерживаемый постоянно. Соединение не разрывается, даже если передача данных прекращается. Оба типа виртуальных каналов (коммутируемых и постоянных) являются примерами коммутации пакетов.

Датаграмма (datagram) представляет собой упакованные данные, пересылаемые без установки коммуникационного канала. Датаграммы достигают точки назначения при помощи механизма коммутации сообщений. Пакеты адресуются некоторому получателю и могут поступать к нему не одновременно (в зависимости от выбранного маршрута). Датаграммы не применяются в международных сетях, однако включены в спецификации ITU-T для Интернета. Интернет-датаграммы X.25 инкапсулируют уровень IP в пакетах X.25, поэтому устройства сети X.25 не "догадываются" о том, что пакеты содержат данные IP. При этом адрес IP-сети попросту переназначается адресу целевого узла X.25.

Соединения X.25

Для осуществления коммуникаций X.25 используются следующие устройства:

- терминальное оборудование (DTE), представляющее собой терминал или любой хост-компьютер (от персонального до мэйнфрейма);

- аппаратура передачи данных (DTE), являющаяся сетевым оборудованием (например, адаптером X.25, сервером доступа или коммутатором пакетов), применяемым для подключения терминального оборудования к сети X.25;

- *сборщик/разборщик пакетов* (packet assembler/disassembler, PAD) представляющий собой некоторое устройство, преобразующее пакет в формат X.25 и снабжающее его адресом X.25. Также это устройство удаляет адресную информацию формата X.25 из пакета при его доставке в целевую локальную сеть. Программное обеспечение PAD выполняет форматирование данных и обеспечивает исчерпывающую проверку на наличие ошибок.

Любое терминальное оборудование подключается к аппаратуре передачи Данных через PAD-устройство, которое имеет несколько портов, позволяющих ему устанавливать различные виртуальные каналы для каждого подключенного к нему компьютера. Терминальное

оборудование передает данные PAD-устройству, которое преобразует данные в формат X.25 и снабжает их адресной информацией, после чего посылает по каналам коммутации пакетов, которыми управляет аппаратура передачи данных. Эта аппаратура подключена к *пункту коммутации пакетов* (packet-switching exchange, PSE) некоторого поставщика услуг. Пункт коммутации является коммутатором в глобальной сети X.25, расположенным у данного поставщика услуг. Клиентская аппаратура передачи данных подключена к провайдерскому пункту коммутации пакетов при помощи высокоскоростной телекоммуникациой линии, такой как линия T-1 *(см. главу 2)*. После этого пункт коммутации пакетов перенаправляет пакет формата X.25 другому коммутатору глобальной сети X.25 или в целевую сеть (рис. 7.2).

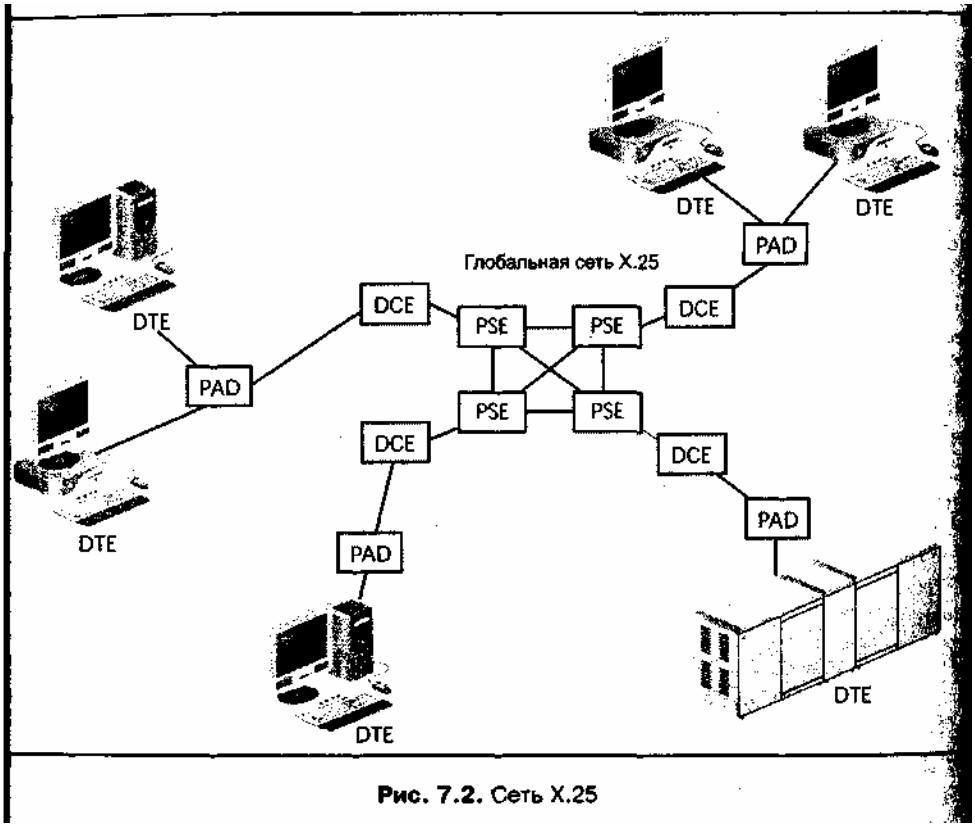


Рис. 7.2. Сеть X.25

Некоторые сетевые операционные системы (такие как Windows 2000 Professional и Server или Windows XP) можно настроить на непосредственное подключение к сети X.25, для чего в компьютере устанавливается интеллектуальная карта X.25 или адаптер PAD, подключаемый к PAO-устройству сети X.25. *Интеллектуальная карта* (смарт-карта, smart card) по размеру почти равна кредитной карточке и может вставляться в компьютер. Достоинством смарт-карты является то, что она имеет цифровую подпись, ключи доступа, доступ с применением пароля и персональный идентификационный номер (PIN) для управления процессами входа в сеть и доступа к файлам и данным.

Смарт-карта является важным средством, обеспечивающим защиту удаленного доступа (такого, как через сети X.25). Например, после того как вы согласно инструкциям производителя установите смарт-карту на сервер Windows 2000, можно создать подключение к частной сети X.25. В практических заданиях 7-1 и 7-2 рассказывается о том, как настроить системы Windows 2000 или Windows XP для удаленного подключения к глобальной сети X.25.

Следующие четыре протокола особенно важны для работы сети X.25:

- *X.3* – определяет методы, с помощью которых PAD-устройство преобразует передаваемый пакет в формат X.25 и извлекает информацию стандарта X.25 из пакета, доставленного в целевую сеть;
- *X.20* – определяет начало и окончание коммуникаций между терминальным оборудованием и аппаратурой передачи данных;
- *X.28* – описывает интерфейс между терминальным оборудованием и PAO-устройством;
- *X.29* – определяет способы передачи управляющей информации между терминальным

оборудованием и РАО-устройством, а также формат, в котором эта информация пересылается.

Данная технология коммутации пакетов предусматривает передачу сообщений с использованием промежуточного хранения. Терминальное оборудование (DTE) упаковывает сообщения, содержащие данные, в пакеты и передает их РАО-устройству. РАО-устройство может по одному кабелю пересылать данные от нескольких терминальных устройств к узлу коммутации пакетов (ОСЕ). Аппаратура ОСЕ представляет собой коммутатор, физически связанный с несколькими другими DCE-устройствами. В сети X.25 коммутатор ОСЕ может передавать данные по нескольким логическим каналам, образованным с помощью протокола X.25. Этот коммутатор принимает переданные пакеты и хранит их в буфере до тех пор, пока не освободится нужный передающий канал. Затем пакеты перенаправляются в точку назначения, где другой коммутатор ОСЕ передает пакеты РАО-устройству, которое разбирает пакеты и возвращает их в исходный вид. Поскольку сеть X.25 поддерживает множество каналов, несколько терминальных устройств может одновременно работать на передачу. Коммутатор последовательно переключается с одного канала на другой, передавая данные от каждого терминального устройства.

Сети X.25 не были предназначены для взаимодействия с другими типами сетей, однако необходимость.в этом появилась после того, как были созданы Другие глобальные сети. Союз ITU-T разработал протокол X.75 (также называемый шлюзовым протоколом) для связи сетей X.25 с другими сетями коммутации пакетов (например, с обсуждаемыми ниже сетями frame relay). Еще один протокол, X.121, обеспечивает единую адресацию в тех случаях, когда глобальная сеть X.25 подключается к другой глобальной сети. Этот протокол предусматривает методы адресации для коммутаторов, регионов и стран.

Структура фрейма X.25

Фрейм X.25 имеет следующие поля (рис. 7.3):

- *флаг* (Flag) – указывает на начало фрейма;
- *уровень фрейма и управляющий адрес* (Frame Level и Control Address) – содержат LAPB-поля Уровня 2;
- *данные* (Data) – содержит поля Уровня 3;
- *контрольная последовательность кадра* (Frame Check Sequence, FCS) – используется для проверки с помощью CRC-суммы;
- *флаг* (Flag) – указывает на конец фрейма.

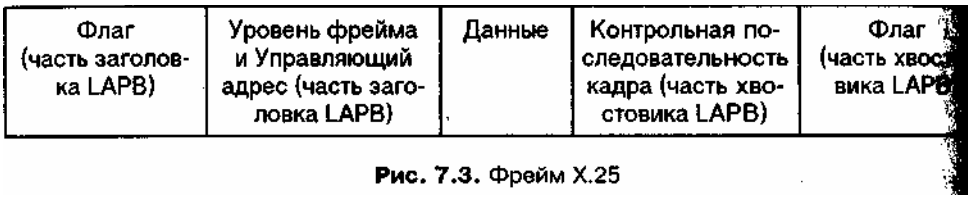


Рис. 7.3. Фрейм X.25

Вокруг полей фрейма, соответствующих Уровню 3, располагаются поля протокола LAPB: поля заголовка LAPB (флаг начала фрейма, поле управления фреймом и адресная информация) и поля хвостовика LAPB (поле контрольной суммы и флаг конца фрейма). Адресные данные LAPB определяют точку назначения фрейма, а поле управления указывает на то, является ли сообщение командой или ответом. Также оно содержит порядковый номер фрейма.

Поля Уровня 3, содержащиеся в области данных фрейма X.25 (см. рис. 7,3) состоят из заголовка и инкапсулированного пакета, полученного из передающей сети (рис. 7.4).

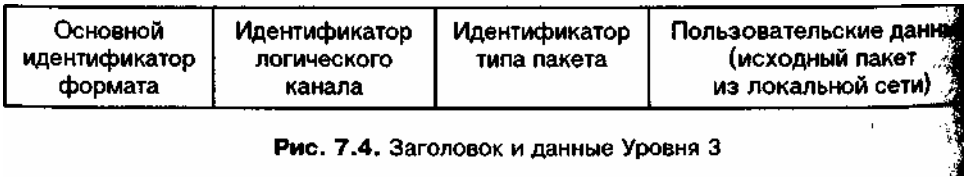


Рис. 7.4. Заголовок и данные Уровня 3

Этот заголовок содержит следующие поля:

- *основной идентификатор формата* (General Format Identifier, GFI) – определяет способ форматирования заголовка пакета;
- *идентификатор логического канала* (Logical Channel Identifier, LCI) – содержит некоторое число, идентифицирующее виртуальный канал, используемый для передачи фрейма;
- *идентификатор типа пакета* (Packet Type Identifier, PTI) – определяет тип передаваемого пакета X.25.

После того как виртуальный канал установлен, протокол X.25 в каждый фрейм помещает некоторый порядковый номер. Этот номер помещается в поле управления той части фрейма, которая относится к протоколу LAPB. Кроме этого, при установлении соединения определяется максимальное количество фреймов, посылаемых без дополнительного запроса со стороны принимающего терминального оборудования (DTE). Обычно это предельное значение зависит от установленного времени подписки (для сетей общего пользования).

Использование сетей X.25

Сети X.25 распространены потому, что они обеспечивают глобальные связи между локальными Сетями и их архитектура предусматривает освобождение неиспользуемой полосы пропускания при отсутствии коммуникаций между узлами. Начиная с 1970-х годов и до сего дня сети X.25 играли важную роль в организации глобальных сетей, однако в настоящее время они заменяются более скоростными технологиями (такими как frame relay, SMDS, SONET и Optical Ethernet).

Сети с ретрансляцией кадров (frame relay)

Стандарты ITU-T для *сетей с ретрансляцией кадров* (frame relay) были предложены в 1984 году как средство организации глобальных сетей с большой полосой пропускания для передачи значительных объемов данных. Затем, по мере роста требований к таким сетям были приняты дополнительные стандарты. Сети frame relay описываются стандартами ITU-T I.451/Q.931 и Q.922 и являются распространенным средством организации глобальных сетей, принятым многими компаниями, входящими в рейтинг Fortune 1000. Первоначально типовые реализации сетей frame relay предусматривали скорость передачи 56 Кбит/с и 2 Мбит/с, однако в настоящее время сети такого типа обеспечивают скорость до 45 Мбит/с по линиям DS-3 (эти линии описывались в *главе 2)*. Среди протоколов, которые можно передавать по сети frame relay, можно назвать следующие:

- IP;
- IPX;
- AppleTalk;
- PPP (инкапсулирующий протоколы TCP/IP, IPX/SPX и NetBEUI);
- SLIP (инкапсулирующий протокол TCP/IP).

Сети frame relay имеют элементы, общие с сетями X.25. Например, в сетях обоих типов используется коммутация пакетов по виртуальным каналам (называемым в сетях frame relay виртуальными соединениями). Как и в сетях X.25, виртуальные соединения в сетях frame relay могут быть коммутируемыми (SVC) или постоянными (PVC). В сетях frame relay терминальное оборудование (DTE) может быть маршрутизатором, коммутатором, коммуникационным контроллером мэйнфрейма или компьютером, подключенным к аппаратуре передачи данных (DCE), представляющей собой некоторое сетевое устройство, соединенное с глобальной сетью frame relay как показано на рис. 7.5.

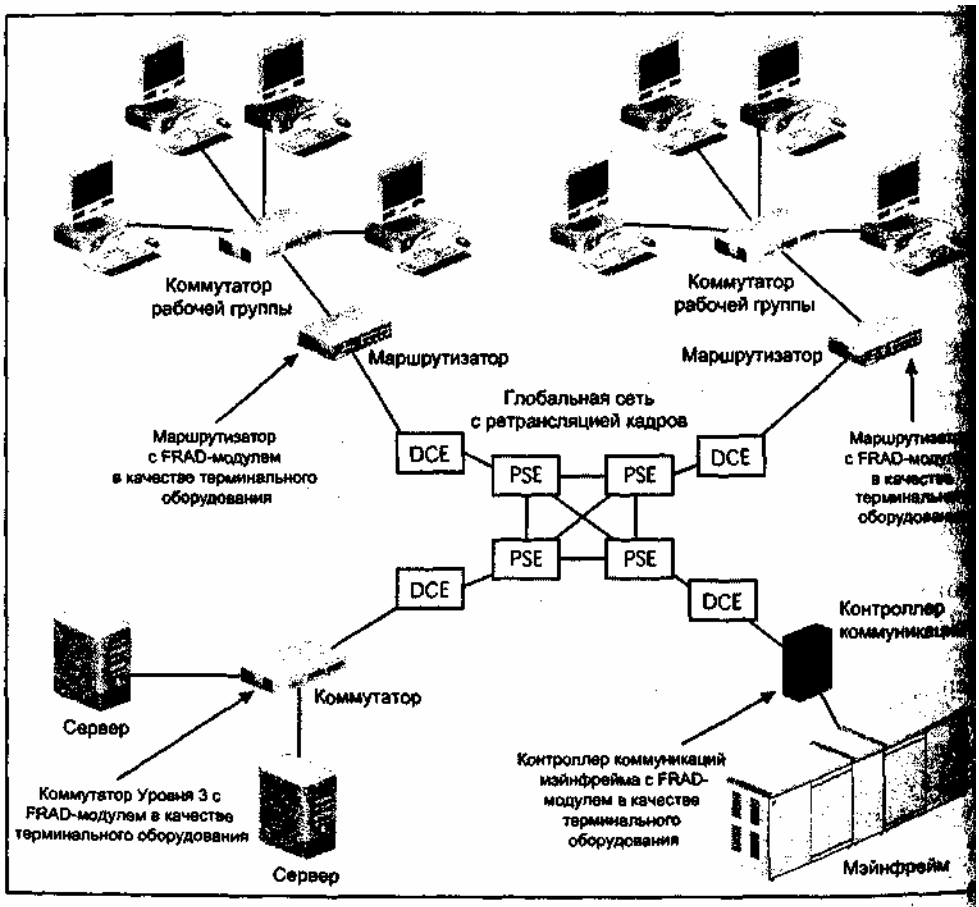


Рис. 7.5. Глобальная сеть с ретрансляцией кадров (frame relay)

В отличие от PAD-устройств, используемых *в* сетях X.25 для преобразования пакетов, в сетях frame relay применяются устройства, называемые *frame relay assembler/disassembler, FRAD* (ассемблер/дизассемблер ретрансляции кадров). Обычно эти устройства представляют собой модуль в маршрутизаторе, коммутаторе или стоечном концентраторе. FRAD-модуль – это устройство, соединяющее пользовательскую локальную сеть с сетью frame relay и отвечающее за инкапсуляцию (ассемблирование, сборку) пакетов локальной сети, благодаря чему эти пакеты могут передаваться по глобальной сети frame relay. Кроме того, FRAD-модуль распаковывает (дизассемблирует) данные, форматированные для сети frame relay, и переводит их в формат, пригодный для передачи в локальную сеть.

В отличие от сетей X.25, сети frame relay могут взаимодействовать с современными сетями, имеющими собственные механизмы обнаружения ошибок. Сети frame relay позволяют достигнуть высоких скоростей передачи данных, при этом предполагается, что новые сетевые технологии имеют средства обнаружения ошибок на промежуточных узлах и, следовательно, в самих сетях frame relay серьезные проверки на наличие ошибок не производятся (т. е. эти сети являются службами без установления соединения). Коммутация кадров часто используется в TCP/IP-сетях и иногда даже с более старыми IPX-сетями, где названные протоколы обеспечивают надежность связи между узлами. При коммутации кадров не анализируются цепочки плохих кадров. Если обнаруживаются ошибки, не замеченные промежуточными узлами, то плохие пакеты попросту отбрасываются. Также пакеты отбрасываются при возникновении перегрузки сети. Этот недостаток следует учитывать при оценке перспектив использования данной технологии.

Многоуровневые коммуникации в сетях frame relay

Еще одно различие между сетями frame relay и X.25 состоит в том, что в сетях frame relay используются только два коммуникационных уровня: Физический и *Link Access Protocol for Frame Mode Bearer Services (LAPP)* (Протокол доступа к каналу для служб, обеспечивающих передачу фреймов). Их соответствие Физическому и Канальному уровням эталонной модели OSI показано на рис. 7.6.

Физический уровень образует интерфейсы, аналогичные тем, которые используются в сетях

X.25 (например, интерфейс типа EIA-232C/D для подключения к сети frame relay) и телекоммуникационные канала (например, Т-линии) для передачи данных по проводам. Уровень 2 (LAPF) предназначен для скоростных коммуникационных служб, не создающих дополнительную нагрузку на X.25. В нем также имеется необязательный подуровень для тех случаев, когда требуется высокая надежность.

Во всех сетях frame relay реализуется базовый протокол LAPF, который управляет основными коммуникационными службами. Этот протокол осуществляет форматирование и коммутацию кадров, проверяет их длину (чтобы она не превышала допустимое значение) и обнаруживает ошибки передачи и перегрузку линии. Кроме того, необязательный управляющий протокол LAPF может использоваться для слежения за потоками (flow control) в виртуальных соединениях, этот протокол контролируется принимающим узлом.

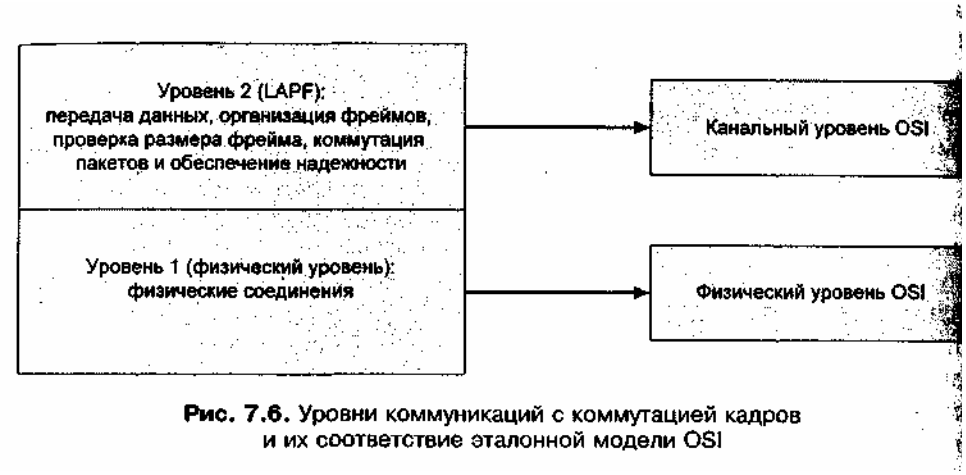


Рис. 7.6. Уровни коммуникаций с коммутацией кадров и их соответствие эталонной модели OSI

Совет

Управление каналом намеренно исключено из числа функций Уровня 2 для того, чтобы уменьшить нагрузку на скоростные службы (т. е. службы работают медленнее, если реализован необязательный управляющий протокол LAPF).

Коммутация и виртуальные каналы

В сетях frame relay в одном несущем кабеле может быть создано несколько виртуальных соединений. Каждое такое соединение обеспечивает передачу данных между двумя коммуникационными узлами. Как и в сетях X.25, виртуальные соединения являются логическими, а не физическими. При коммутации кадров возможны два типа виртуальных соединений: постоянные и коммутируемые.

Постоянные виртуальные соединения были предложены в 1984 году в составе первоначального стандарта на коммутацию кадров. Такие соединения представляют собой постоянно доступный маршрут между двумя узлами, который имеет некоторый идентификатор, указываемый в каждом передаваемом пакете. Установленное соединение остается всегда открытым, поэтому коммуникации могут осуществляться в любой момент. Отдельные передачи данных обрабатываются на Физическом уровне, а виртуальные соединения являются частью уровня LAPF. Один передающий кабель может поддерживать несколько виртуальных соединений с различными целевыми сетями.

Коммутируемые виртуальные соединения включены в стандарт на коммутацию кадров в 1993 году. Для них требуется установление сеанса связи. Чтобы начался обмен данными, между двумя узлами передается управляющий сигнал вызова. По окончании коммуникаций этот сигнал сопровождается командой на отключение обоих узлов. Коммутируемые виртуальные соединения служат для того, чтобы позволить сети или поставщику Т-линии определять скорость передачи данных. Скорость может выбираться в соответствии с требованиями приложения и в зависимости от имеющегося в данный момент сетевого трафика. Между двумя точками по одному кабелю может проходить множество коммутируемых виртуальных соединений. В сетях frame relay коммутируемые виртуальные соединения являются более новой технологией, чем постоянные виртуальные соединения.

Формат фрейма

Формат фрейма в сетях frame relay (рис. 7.7) напоминает формат, используемый в сетях X.25 (но без управляющего поля уровня фрейма), и содержит следующие поля, определенные стандартом ITU-T Q.922:

- *флаг* (Flag) – указывает на начало фрейма;
- *адрес* (Address) – может иметь длину от 2 до 4 байтов;
- *данные* (Data) – содержит пользовательские данные, передаваемые по сети frame relay;
- *контрольная последовательность кадра* (Frame Check Sequence, FCS) – для базового механизма обнаружения ошибок;
- *флаг* (Flag) – указывает на конец фрейма.

Рис. 7.7. Формат фреймов сетей frame relay

Совет

Дополнительную информацию о формате фрейма и сетях frame relay можно найти на веб-странице Frame Relay Forum по адресу **www.frforum.com.**

Поле адреса содержит *идентификатор подключения к каналу* (data link connection identifier, DLCI), с помощью которого идентифицируется виртуальное соединение, по которому передается фрейм. Поле DLCI в сетях frame relay выполняет те же функции, что и поле идентификатора логического канала (LCI) в LAPB-заголовке сети X.25. Например, одно виртуальное соединение может в поле DLCI иметь значение 810, для другого соединения поле будет содержать значение 820, для третьего – 830 и т. Поля DLCI позволяют сети frame relay различать сообщения, отправляемые одновременно по одной линии от разных источников (например, от четырех рабочих станций или серверов к четырем различным принимающим узлам), как показано на рис. 7.8.

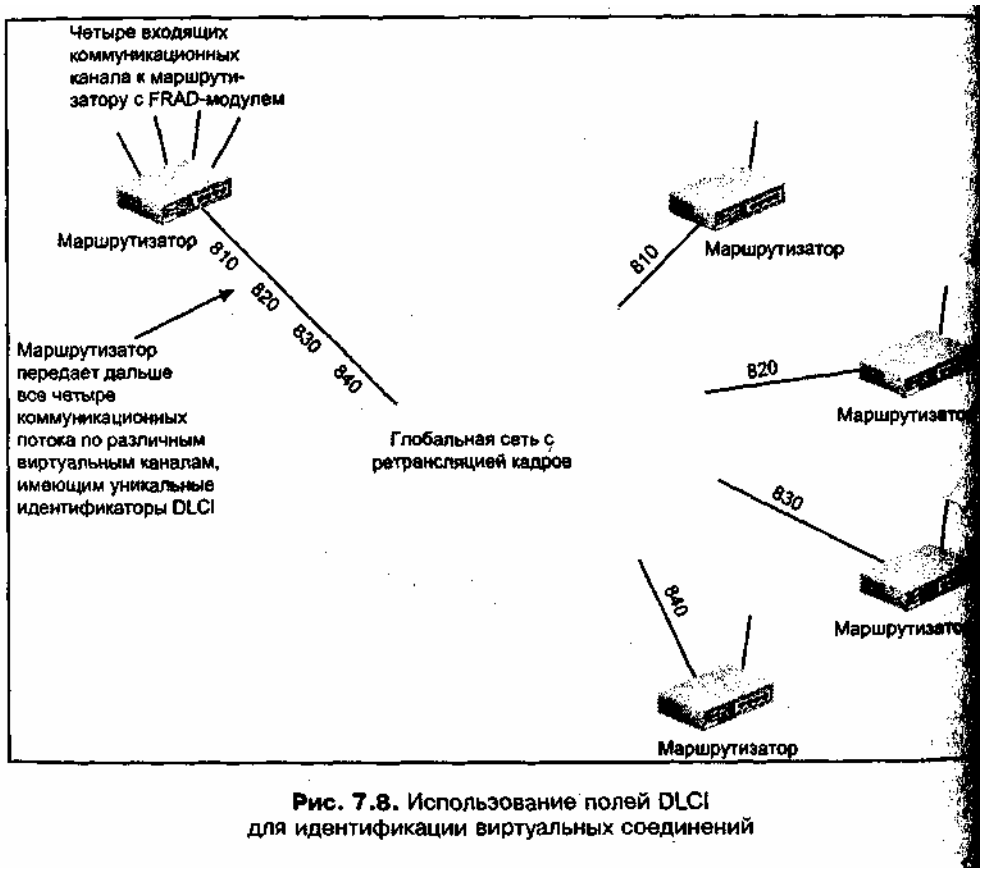


Рис. 7.8. Использование полей DLCI для идентификации виртуальных соединений

Примечание

Обычно каждое поле DLCI назначается поставщиком услуг сети frame relay с использованием глобальной адресации, при которой уникальное значение этого поля задается для каждого порта сети в рамках всей сети frame relay.

Обычно для передачи служебных сигналов в сетях frame relay используется протокол *Local Management Interface (LM1)* (Локальный управляющий интерфейс), с помощью которого определяются моменты создания нового виртуального соединения и удаления ненужного соединения, а также указывается на неисправность некоторого виртуального соединения. Помимо базовой информации имеются *LMI-расширения* (LMI extension), которые могут быть включены в качестве заголовков в поле данных фрейма. Когда используются постоянные виртуальные соединения (PVC), в каждый фрейм добавляется LMI-расширение для сообщений о состоянии виртуального соединения. Это расширение позволяет синхронизировать коммуникации между терминальным оборудованием (DTE) и аппаратурой передачи данных (DCE), а также убедиться в существовании соединения перед посылкой данных.

Имеется необязательное LMI-расширение для приложений мультимедиа, требующих группового вещания (когда один фрейм отправляется нескольким целевым узлам). Такое расширение используется совместно с протоколами маршрутизации данных мультимедиа. Еще одно LMI-расширение служит для глобальной адресации, с помощью которой разрешение имен во всей глобальной сети может выполняться так, будто все узлы располагаются в локальной сети. То есть при разрешении имен в IP-адреса (и наоборот) имена компьютеров и доменов, а также интернет-имена рассматриваются такими, будто они находятся в одной локальной сети. Имеется еще одно LMI-расширение, с помощью которого реализуется *управление потоком данных по принципу "включено/выключено"* (XON/XOFF flow control), между устройствами, связанными через глобальную сеть. Этот способ управления является давно существующим механизмом управления потоком, при котором клавиши <Ctrl>+<S> используются для приостановки передачи, а клавиши <Ctrl>+<Q> – для возобновления.

LMI – это протокол передачи служебных сигналов, разработанный совместно компаниями Northern Telecom, Digital Equipment Corporation, Cisco и StrataCom и часто используемый в устройствах этих производителей. Другой аналогичный протокол описан в стандарте ANSI T1.617, а еще один протокол для сетей frame relay определяется стандартом ITU-T Q.933.

Между протоколом LMI и двумя другими протоколами передачи служебных сигналов имеются два общих различия. Во-первых, при использовании LMI поле DLCI всегда равно 1023, при этом согласно стандартам T1.617 и Q.933 это поле всегда содержит 0. Во-вторых, при использовании LMI можно создавать до 992 виртуальных каналов, а стандарты T1.617 и Q.933 допускают создание 976 виртуальных каналов.

Передача голоса по сетям с ретрансляцией кадров (VoFR)

Сети frame relay имеют опцию, называемую *передачей голоса по сетям с Ретрансляцией кадров* (voice over frame relay, VoFR). С ее помощью речевые сигналы можно передавать по сети, что позволяет сократить расходы на междугородные телефонные разговоры, при этом используются две технологии: сжатие речевого сигнала и подавление пауз. Обе технологии предназначены для увеличения пропускной способности сети при передаче данных и речи.

При *сжатии речевого сигнала* (voice compression) используются следующие технологии: *импульсно-кодовая модуляция (ИКМ)* (pulse code modulation, PCM), *адаптивная дифференциальная импульсно-кодовая модуляция* (adaptive differential pulse code modulation, ADPCM) и *адаптивная дифференциальная импульсно-кодовая модуляция в частичном диапазоне* (sub-band adaptive differential pulse code modulation, SB-ADPCM). ИКМ – это технология речевых коммуникаций, при которой аналоговый аудиосигнал преобразуется в 8-разрядный цифровой сигнал. Он также применяется для передачи речи через Интернет. ADPCM – это разновидность ИКМ, позволяющая передавать голос со скоростью в два-четыре раза меньше, чем при обычных ИКМ-коммуникациях. SB-ADPCM представляет собой модификацию ADPCM для работы в сетях ISDN и frame relay. Все перечисленные методы сжатия речевого сигнала предусматривают передачу аудиофайлов, которые создаются на передающем конце и воспроизводятся на принимающем. Каждый из этих методов

рассматривается подробнее в *главе 10.*

Подавление пауз (silence suppression) – это технология для обнаружения пауз между словами или при переключении диалога от одного говорящего к другому. Сеть frame relay передает данные в течение обнаруженных пауз. Качество речи в сети frame relay при подавлении пауз обычно хуже, чем при сжатии речевого сигнала, особенно в тех случаях, когда в сети имеется высокий трафик.

Технология передачи голоса по сетям с ретрансляцией кадров (а также возможность передачи факсов) очень привлекательна для корпоративных пользователей, поскольку она позволяет существенно экономить средства при совместной передаче данных и речи, что в значительной мере делает ненужными платные телекоммуникационные услуги.

Службы поставщиков сетевых услуг

Поставщики сетей frame relay (региональные телефонные компании или телекоммуникационные компании дальней связи) обычно предоставляют услуги трех типов (и их комбинации): Л

- *согласованная скорость передачи информации* (committed information rate? CIR) – гарантированная минимальная скорость передачи данных (например, частная или полная линия T-1, линия T-3). Сложность при использовании этой услуги заключается в том, что мониторинг каналов выполняется нерегулярно, поэтому клиенту сложно проверить, всегда ли обеспечивается заявленная скорость;
- *постоянное виртуальное соединение* (PVC) – постоянно существующее выделенное соединение с некоторой точкой. Эти услуги, пожалуй, наиболее ценны, поскольку предусматривают установление непрерывного коммуникационного маршрута;
- *порт* – приобретение доступа к определенному порту (или нескольким портам) (например, к порту 56 Кбит/с или порту линии T-1), расположенному на коммуникационном коммутаторе поставщика услуг.

Совет

Сетевой администратор должен разбираться в типах услуг для того, чтобы обсуждать реализацию конкретной сети frame relay.

Сети ISDN

Цифровые сети связи с комплексными услугами (Integrated Services Digital Network, ISDN) появились в 1970-х годах для передачи в цифровом виде речевых сигналов, данных, графики и видеосигналов. В 1984 и 1988 годах они были стандартизованы союзом ITU-T (в то время называющимся Международным консультативным комитетом по телеграфии и телефонии, МККТТ – Consultative Committee on International Telegraph and Telephone, CCITT). Эти стандарты описывали узкополосные сети ISDN (N-ISDN) и при своем появлении явились заметным шагом вперед по сравнению с коммуникациями на скорости 9,6 Кбит/с, широко используемыми в то время для организации телекоммуникационных глобальных сетей. ISDN – это стандарт цифровых телекоммуникаций, который в настоящее время предусматривает передачу пользовательских данных на скорости до 1,536 Мбит/с и имеет теоретический предел в 622 Мбит/с. Клиенты, которым нужно получить услуги ISDN для связи с некоторой точкой, могут получить цифровую ISDN-линию с одноканальным обслуживанием от своей региональной телефонной компании. Одноканальная служба позволяет конечному пользователю подключать к линии несколько устройств (например, факс, компьютер и цифровой телефон). Некоторые компании позволяют подключать до восьми устройств (максимум для данного типа ISDN-служб). Организации, которые через глобальную ISDN-сеть соединяют между собой локальные сети, обычно используют для этого T-линии. Сети ISDN предоставляют различные услуги, среди которых следующие:

- обеспечение связи между локальными сетями;
- обеспечение работы домашних офисов и надомных работников;
- удаленная архивация и восстановление настольных компьютерных систем;
- подключение частной телефонной системы к региональной телефонной компании;
- передача больших файлов изображений и данных;

- обеспечение работы видео- и мультимедиа-приложений, работающих в нескольких локальных сетях.

«I»-серии стандартов ISDN включают в себя следующие наборы стандартов:

- 1.100 – введение в ISDN и глоссарий (список терминов);
- 1.200 – перечень возможностей, имеющихся для пользователей, в том числе:
- полная и гарантированная совместимость между оконечными узлами;
- стандартные терминалы и процедуры;
- список абонентов ISDN в международном каталоге;
- стандартные процедуры тестирования и сопровождения;
- правила тарификации и учета;
- 1.300 – стандарты, ориентированные на сетевые вопросы (такие как нумерация и адресация);
- 1.400 – стандарты, описывающие сетевой интерфейс (такие вопросы, как конфигурации оборудования, скорости передачи и спецификации протоколов);
- 1.500 – стандарты, определяющие интерфейс между сетями ISDN и другими типами сетей;
- 1.600 – здесь описываются установка абонентов, серверы доступа и общие вопросы архитектуры.

Реализация сетей ISDN оказалась дорогой для компаний дальней связи. Поскольку эти сети полностью цифровые, необходимо было заменить устаревшие аналоговые и электромеханические коммутаторы. В США компании дальней связи, такие как AT&T, MCI и Sprint, а также многие региональные телефонные компании предоставляют услуги ISDN для личного пользования, домашних офисов и организаций. Сети ISDN имеют следующие достоинства:

- возможность передачи по одной сети речевых сигналов, данных и видео информации;
- наличие многоуровневого стека протоколов, совместимых с эталонной моделью OSI;
- коммуникационные каналы со скоростями, кратными 64, 384 и 1536 Кбит/с;
- наличие служб коммутируемых и некоммутируемых соединений;
- широкополосные средства ISDN, обеспечивающие скорость 155 Мбит/с и выше. 1

Сетевые службы 1.200

Раздел 1.200 спецификаций ITU-T для сетей ISDN описывает различные сетевые средства, которые делятся на передающие службы, телекоммуникационные службы и вспомогательные службы. Передающие службы имеют сетевые опции и опции пакетов. Сетевые опции перечислены в табл. 7.1. В столбце "Канал" приведены имена коммуникационных ISDN-каналов, используемых для обеспечения работы службы. Опции пакетов передающих служб включают в себя каналы виртуального вызова и постоянные каналы виртуального вызова, которые выполнены по аналогии с коммутируемыми и постоянными виртуальными каналами сетей X.25.

Таблица 7.1. *Сетевые опции ISDN*

Скорость передачи информации	**Канал**	**Приложения**
64 Кбит/с	B (несущий)	Универсальные коммуникации с частотой 8 кГц
64 Кбит/с	B	Оцифрованная речь с частотой 8 кГц
64 Кбит/с	B	Аудиосигналы с частотой 8 кГц
64 Кбит/с	B	Альтернативная передачи речи с частотой 8 кГц
16 или 64 Кбит/с	D (данные)	Передача сигналов с частотой 8 кГц, коммутация пакетов и верификация кредитных карт
384 Кбит/с	H0 (шесть B-	•Передача видеосигналов с частотой 8

Скорость передачи информации	Канал	Приложения
	каналов)	кГц и связь с частными телефонными системами •Быстрая передача факсов •Передача компьютерных изображений • Высокоскоростная передача данных •Связь между локальными сетями
1,472 Мбит/с	H10 (эквивалентен 23 североамериканским каналам 64 Кбит/с)	• Видеоконференции • Связь между локальными сетями • Передача компьютерных изображений • Высокоскоростная передача данных
1 ,536 Мбит/с	H11 (эквивалентен 23 североамериканским B-каналам 64 Кбит/с плюс один D-канал 64 Кбит/с)	• Видеоконференции • Связь между локальными сетями • Передача компьютерных изображений • Высокоскоростная передача данных
1,984 Мбит/с	H12 (эквивалентен 30 европейским B-каналам 64 Кбит/с)	Обеспечивает скорость передачи, равную 1 ,920 Мбит/с, что соответствует 30 европейским B-каналам 64 Кбит/с плюс один D-канал 64 Кбит/с)
155 Мбит/с	H4X	Высокоскоростная передача данных, речевых и видеосигналов

Телекоммуникационные службы предназначены для речевых коммуникации с частотой 3,1 кГц. К ним также относятся службы телекса для интерактивного обмена текстовыми сообщениями, а также службы факса и видеотекс (видеографии), обеспечивающие получение цифровой почтовой информации (включая тексты и графику). Вспомогательные службы в первую очередь предназначены для поддержки речевых коммуникаций. Сюда относятся определение идентификатора вызывающей стороны (caller ID) и групповой вызов.

Цифровые коммуникационные службы

Узкополосная ISDN-сеть (N-ISDN) поддерживает интерфейсы двух типов: интерфейс базового уровня (basic rate interface, BRI) и интерфейс основного уровня (primary rate interface, PRI).

В ISDN-сети с *интерфейсом базового уровня* (BRI) используется разновидность множественного доступа с уплотнением каналов (также называемого мультиплексированием с разделением времени – см. *главу 2)*. Такая сеть имеет общую пропускную способность, равную 144 Кбит/с. Интерфейс базового уровня состоит из трех каналов: двух несущих (bearer, B) каналов для передачи данных, речи и графики со скоростью 64 Кбит/с и третьего – D-канала (Delta, иногда называемого Demand (запрос)), обеспечивающего скорость 16 Кбит/с и используемого для передачи сигналов управления коммуникациями, коммутации пакетов и верификации кредитных карт. Главная задача D-канала – обеспечить прохождение и снятие ISDN-вызова, а также начало и окончание сеанса передачи данных. Интерфейс базового уровня применяется для выполнения следующих задач:

- обеспечение связи локальных сетей;
- проведение видеоконференций;
- подключение к поставщику услуг Интернета;
- высокоскоростной обмен данными с надомными работниками и домашними офисами.

Несколько BRI-каналов можно связать между собой (сгруппировать) для обеспечения

коммуникаций с еще более высокой скоростью. Например, два 64-килобитных B-канала в одной BRI-линии можно сгруппировать и получить соединение с реальной скоростью передачи, равной 128 Кбит/с. При добавлении 16-килобитного D-канала плюс 48 Кбит/с для сопровождения и синхронизации можно получить общую скорость в 192 Кбит/с. Можно сгруппировать три BRI-линии, содержащие 64-килобитных B-канала, и получить общую реальную скорость передачи данных, равную 384 Кбит/с.

Совет

Windows 2000, Windows XP и многие системы UNIX поддерживают группировку ISDN-линий с помощью механизма многоканальных PPP-подключений (multilink PPP). Кроме того, если вы хотите стать абонентом сети BRI ISDN, поищите телекоммуникационные компании, реализующие возможность загрузки данных по D-каналу, что на 16 Кбит/с увеличивает скорость нисходящих коммуникаций (от поставщика услуг к клиенту). В практическом задании 7-3 рассказывается о том, как включить режим многоканальных PPP-подключений в системе Windows 2000 Server.

Клиенты подключаются к ISDN-сетям с интерфейсом базового уровня (BRI) при помощи 4-проводного телефонного кабеля на основе витой пары, при этом обычно имеются три способа подключения.

Во-первых, можно просто установить на компьютер терминальный адаптер (описывался в *главе 4),* который также имеет терминатор сетевого терминала (NT1). Линия подключается к такому компьютеру при помощи коннектора RJ-45.

Во-вторых, можно использовать внешний терминальный адаптер, оборудованный U-интерфейсом, к которому подключается ISDN-линия. U-интерфейс обеспечивает дуплексную связь между терминальным адаптером и коммутатором ISDN, расположенным у поставщика услуг. Терминальный адаптер может иметь последовательный порт RS-232 для подключения к компьютеру и телефонный порт для связи с обычной телефонной линией с помощью коннекторов RJ-11.

В-третьих, ISDN-линию можно подключить к сетевому устройству, называемому *оконечным комплектом сети* (network termination unit, NTU). NTU имеет U-интерфейс, подключаемый к ISDN-линии через коннектор RJ-45. С помощью S/T-интерфейсов, имеющихся в NTU, можно подключить несколько устройств (до восьми), в том числе компьютеры, факсы и телефоны. На рис. 7.9 показано, как к сети ISDN подключаются компьютеры с ISDN-совместимыми сетевыми адаптерами, факсимильные аппараты и телефоны, разработанные для связи с ISDN.

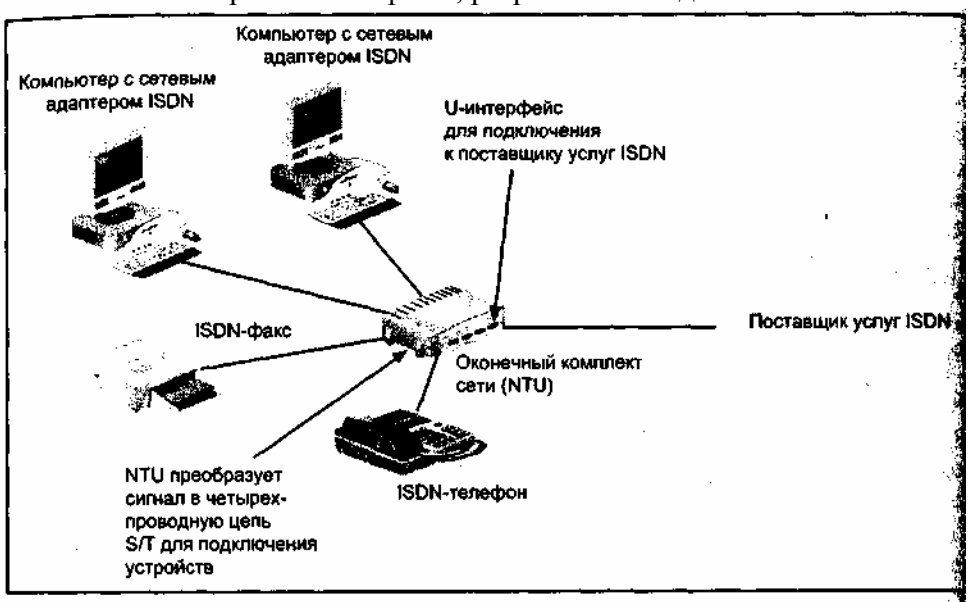


Рис. 7.9. Подключение с помощью оконечного комплекта сети (NTU)

Совет

Если терминальный адаптер устанавливается непосредственно на компьютер, работающий под управлением Windows 2000 или Windows XP, то этот адаптер необходимо настроить, указав тип ISDN-коммутатора, применяемого региональной телефонной компанией (например, коммутатор

фирм AT&T (ATT) или North Telecom (NTI)). В большинстве случаев при установке терминального адаптера системы Windows 2000 и Windows XP распознают его и конфигурируют автоматически. После установки адаптера в системе Windows 2000 выберите значок **My Computer** (Мой компьютер) и щелкните правой кнопкой мыши; в системе Windows XP в меню **Start** (Пуск) выберите пункт **My Computer (**Мой компьютер) и щелкните правой кнопкой мыши. В появившемся контекстном меню выберите команду **Manage** (Управление). В дереве объектов выберите узел **Device Manager** (Диспетчер устройств). В правой половине окна выберите название терминального адаптера и дважды щелкните по нему, чтобы настроить тип коммутатора. Если адаптер не виден в этом окне, дважды щелкните по узлу **Modems** (Модемы) и выберите терминальный адаптер в этой ветке дерева устройств.

ISDN-сети с *интерфейсом основного уровня* (PRI) обеспечивают более высокую по сравнению с BRI ISDN скорость передачи данных, при этом суммарная полоса пропускания коммутируемых данных достигает 1,536 Мбит/с. В США и Японии интерфейс основного уровня состоит из 23 64-килобитных B-каналов и одного 64-килобитного D-канала для передачи служебных сигналов и коммутации пакетов. Европейские сети PRI ISDN имеют 30 64-килобитных B-каналов и один 64-килобитный канал для служебных сигналов или коммутации. PRI-интерфейсы используются для связи локальных сетей и поставщиков услуг Интернета, а также для проведения видеоконференций и (в корпоративных сетях) для подключения надомных работников, имеющих ISDN-доступ.

Для подключения клиентов к PRI-интерфейсу используется мультиплексор (как показано на рис. 7.10) или частная телефонная система, а также группа из 24 каналов, называемая транком (магистралью). Мультиплексор обычно применяется тогда, когда PRI ISDN обеспечивает связь между локальными сетями, для поставщика услуг Интернета он может представлять собой внешнее устройство или модуль в маршрутизаторе. Частная телефонная система используется для организации видеоконференций и центров обработки телефонных вызовов, имеющих базы абонентских номеров, связанных с пользовательскими службами. Такая телефонная система должна иметь возможность подключения к PRI ISDN. В одной точке можно использовать несколько PRI-магистралей, и в этом случае количество D-каналов, применяемых для передачи служебных сигналов, можно сократить. Например, если компания имеет пять PRI-магистралей для решения коммуникационных задач, то она может приобрести только один или два D-канала (второй D-канал может использоваться в качестве резервного в случае отказа первого канала). В практическом задании 7-4 рассказано о том, как узнать о имеющихся в вашем регионе ISDN-сетях, предоставляющих BRI- и PRI-интерфейсы.

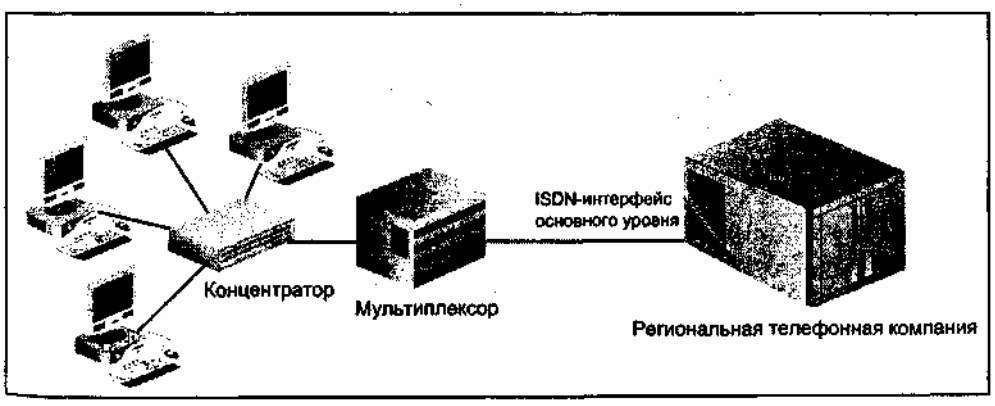


Рис. 7.10. Подключение к ISDN-интерфейсу основного уровня

Широкополосные сети ISDN

Развитие высокоскоростных сетей привело к появлению *широкополосных ISDN-сетей* (broadband ISDN, B-ISDN). Эта развивающаяся технология предназначена для обеспечения совместимости с сетями ATM и SONET (рассматриваемыми в следующих главах). Широкополосные ISDN-сети предназначены для коммуникаций со скоростями от 155 Мбит/с до 1 Гбит/с (и выше) по оптоволоконному кабелю. В них применяется не коммутация пакетов, а

коммутация ячеек. На момент написания книги эта технология еще не стала распространенной по причине отдельных успехов в области сетей ATM (в которых используются некоторые элементы, изначально описанные в спецификациях сетей B-ISDN) и SONET.

Принципы работы ISDN-сетей

Сети ISDN совместимы со многими существующими цифровыми сетями телекоммуникационными технологиями, среди которых ATM, X.25, SMDS и линии T-1. Как было показано в табл. 7.1, сеть ISDN образуется из 64-килобитных каналов: каналов B, C, D, НЮ, НИ, H12 (применяемых в Европе) и H4X (широкополосных).

Для передачи по сети цифровых сигналов используются два метода. Первый из них называется *уплотнением с временной компрессией* (time-compression multiplexing), когда 16- или 24-разрядные блоки данных передаются в виде повторяющихся цифровых пакетов. Между пакетами имеется пауза, позволяющая линии подготовиться к передаче следующего пакета. Следовательно, после передачи пакета в одном направлении следует пауза, после которой пересылается пакет в обратном направлении. Скорость передачи пакета равна 288 Кбит/с. Из-за переключения направлений фактическая скорость передачи данных составляет 144 Кбит/с. Пакетами данных управляет центральное устройство синхронизации.

Второй метод передачи – *эхоподавление* (echo cancellation). В этом случае данные одновременно передаются в обоих направлениях. Для подключения трансивера (приемопередатчика) к абонентской линии используется устройство, называемое гибридным (hybrid). При осуществлении одновременных двунаправленных коммуникаций часто возникает отражение (эхо) передаваемого сигнала. Отраженный сигнал в линии может в три раза превышать по мощности истинные сигналы, из-за чего данные трудно распознать. Для борьбы с отраженными сигналами в ISDN-сетях применяется эхоподавитель, который определяет амплитуду этих сигналов и вычитает ее из амплитуды входящих сигналов. Поскольку мощность эхосигналов может варьироваться, в эхоподавителе используется цепь обратной связи, позволяющая непрерывно измерять амплитуду отраженного сигнала.

ISDN и многоуровневые коммуникации OSI

В ISDN-сетях используются многоуровневые коммуникации, соответствующие Физическому, Канальному, Сетевому и Транспортному уровням эталонной модели OSI (рис. 7.11). Уровень 1 сети ISDN обеспечивает передачу сигналов и обнаружение конфликтов (что необходимо, т. к. два узла могут начать передачу одновременно). Для обнаружения коллизий и определения очередности циклов передачи используется эхоразряд. Передаваемой информации Уровень 1 дает наивысший приоритет. При наличии конфликта между речевыми сигналами и данными более высокий приоритет получает речевая (телефонная) связь. Уровень 2 управляет служебными данными и обеспечивает самое строгое обнаружение коммуникационных ошибок, что позволяет добиться высокой надежности при передаче информации. Уровень 3 управляет установлением и снятием запросов, а также обеспечивает связь между соединениями с коммутацией каналов и соединениями с коммутацией пакетов. Уровень 4 гарантирует надежность коммуникационного маршрута после того, как тот установлен.

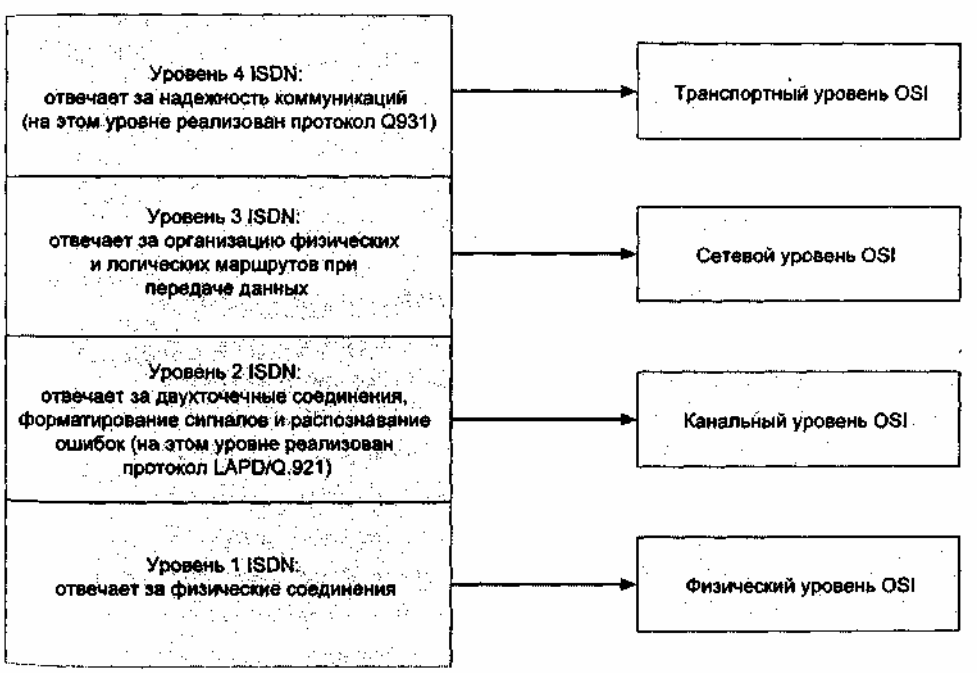


Рис. 7.11. Многоуровневые коммуникации ISDN в сравнении с эталонной моделью OSI

Формат фрейма LAPD

На Уровне 2 ISDN, называемом *Link Access Procedure D channel (LAPD)* (D-канал операций доступа к каналу) используется формат фрейма, показанный на рис. 7.12. По структуре он напоминает LAPB-формат сетей X.25. LAPD также называется протоколом Q.921.

Фрейм содержит следующие поля:

- флаг (Flag) – указывает на начало фрейма;
- адрес (Address) – содержит адрес конечного узла (или узлов – поскольку один фрейм может предназначаться нескольким пунктам назначения);
- управление (Control) – содержит данные, управляющие процессом передачи, в том числе идентификатор используемого канала и тип пересылаемого пакета;
- данные (Data) – содержит заголовок пакета и полезную нагрузку, передаваемую по сети ISDN;
- контрольная последовательность кадра (Frame Check Sequence, FCS) используется для обнаружения ошибок;
- флаг (Flag) – указывает на конец фрейма.

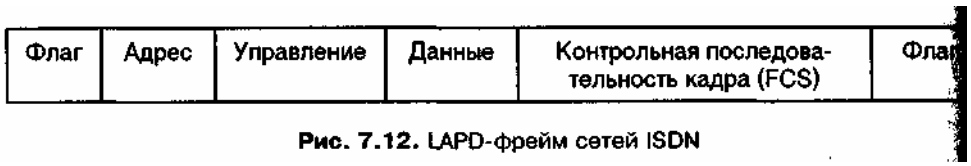


Рис. 7.12. LAPD-фрейм сетей ISDN

Протокол управления соединениями Q.931

На Уровне 4 ISDN используется протокол Q.931, обеспечивающий управление соединением по D-каналу и отвечающий за установление и разрыв соединения. Блоки управляющей информации, передаваемой этим протоколом, называются информационными элементами. Например, информационные элементы протокола Q.931 могут содержать следующие команды:

- Setup – запрос соединения;
- Call Proceeding – обработка запроса на соединение;
- Connect – окончание обработки запроса на соединение;
- Connect Acknowledgement – проверка соединения;
- Suspend – временная приостановка процесса передачи информации, при этом могут осуществляться другие коммуникации;
- Resume – возобновление приостановленного процесса передачи информации;

- Disconnect – запрос на окончание коммуникационного сеанса;
- Release – процесс завершения коммуникационного сеанса;
- Release Complete – окончание процесса завершения коммуникационного сеанса.

Особенности подключения к сетям ISDN

Ответ на вопрос "имеются ли сети ISDN в моем регионе?" зависит от того, какие услуги предоставляет ваша телефонная компания и модернизировано ли телекоммуникационное оборудование в вашем городе для работы с ISDN. При знакомстве со службами ISDN уточните, какой протокол используется вашим поставщиком услуг. Самыми распространенными являются протоколы National ISDN-1 (N1-1) и National ISDN-2 (N1-2). Знать, какой протокол применяется, нужно для того, чтобы настроить телекоммуникационное оборудование на площадке клиента. Протокол N1-1 обычно выбирается региональными телефонными компаниями и операторами дальней связи, а некоторые из них используют протокол N1-2, являющийся последней версией ISDN-протокола.

Подключение к ISDN-сети может обеспечить кабель на основе витых медных пар или оптоволоконный кабель. Лучше применять оптоволокно, поскольку оно обеспечивает наилучшие коммуникационные параметры и высокую скорость (в особенности для сетей PRI ISDN и B-ISDN). При использовании витой пары следует учитывать три момента. Во-первых, длина линии между поставщиком услуг и абонентом не должна превышать 5,5 км (если отсутствуют повторители для увеличения этого расстояния). Во-вторых, следует применять высококачественные кабели, при этом нужно минимизировать факторы, влияющие на уменьшение амплитуды сигнала (например, несогласованные телефонные кабели или большое количество кросс-соединений в монтажном шкафу). В-третьих, нужно убрать существующие фильтры и устройства подавления шумов в аналоговых сигналах, поскольку они вносят искажения в цифровые сигналы

Подключение к сети ISDN через T-линию

Если вы подключаетесь к сети ISDN не по специально выделенной линии (а, например, по T-линии), то поставщик услуг, вероятнее всего, предложит вам канальные службы, пакетные службы или службы обоих типов. *Канальные службы* (службы канального режима) предоставляют коммуникационный канал на время сеанса передачи пользовательских данных и используются монопольно двумя соединенными устройствами до тех пор, пока канал не будет разорван. Чаще всего такие службы применяются для передачи речи. *Пакетные службы* (службы пакетного режима), предназначенные для передачи данных, предусматривают возможность использования нескольких каналов в течение одного сеанса передачи данных, при этом в начале сеанса каждому подключенному устройству назначается адрес и номер последовательности, благодаря которым обеспечивается доставка данных в указанный пункт назначения. Преимуществом пакетных служб является то, что они максимально используют имеющуюся полосу пропускания сети.

Служба SMDS

Служба *Switched Multimegabit Data Service (SMDS),* разработанная компанией Bell Communications, впервые была продемонстрирована в 1990 году в качестве системы на основе телекоммуникационных каналов, предназначенной для объединения сетей FDDI в региональную сеть. В настоящее время эта служба может также связывать сети Ethernet и Token Ring. Служба SMDS представляет собой технологию передачи данных с использованием ячеек, она обеспечивает скорость передачи до 155 Мбит/с по T-линиям и широко применяется в Европе.

С самого начала служба SMDS была совместимой с сетями B-ISDN, что обеспечило возможность очень быстрой передачи ячеек SMDS на большие расстояния. Эти ячейки обрабатываются SMDS-коммутаторами, которые связываются между собой с помощью высокоскоростных каналов DS-1, ISDN и SONET (рассматриваются в этой главе позже). SMDS – это транспортный механизм без установления соединения, позволяющий уменьшить издержки за счет того, что задача обнаружения ошибок передается интеллектуальным оконечным устройствам (таким как коммутаторы и маршрутизаторы).

Примечание

В США службы SMDS впервые применялись региональными телефонными компаниями

(такими как Verizon и SBC Pacific Bell). Многие из этих компаний в настоящее время переключили свое внимание на сети SONET, обеспечивающие более высокие скоростные показатели.

Служба SMDS была разработана для передачи данных в высокоскоростных региональных сетях, она должна обеспечить выполнение следующих задач:

- предоставление высокоскоростных каналов связи для региональных сетей;
- передача больших графических файлов (например, рентгеновских снимков);
- передача архитектурных чертежей и файлов систем автоматизированного проектирования (САПР);
- быстрый доступ к библиотечным хранилищам и электронным каталогам.

Архитектура SMDS масштабируемая и предусматривает использование Яличных коммуникационных скоростей, поэтому служба SMDS может легко интегрироваться как в региональные сети (для которых она и была первоначально разработана), так и в глобальные сети. Другим достоинством службы SMDS является то, что она совместима со множеством протоколов, включая TCP/IP, SNA, IPX/SPX, DECnet и AppleTalk. Поскольку для передачи данных служба SMDS использует ячейки, при работе в глобальных сетях о может пропускать очень большие фреймы, не фрагментируя их на более мелкие блоки.

Архитектура SMDS

Интерфейс службы SMDS носит название *Distributed Queue Dual Bus (DQDB)* (двойная шина распределенных запросов) и образуется двумя оптоволоконными кабелями с общим доступом. С одного конца оба кабеля подключаются к оборудованию клиента, а с другой – к коммутатору, установленному у поставщика услуг (рис. 7.13). Данные по каждому кабелю передаются только в одну сторону: по одному кабелю информация поступает от клиента к поставщику, а по другому – в обратном направлении. Наличие двух независимых однонаправленных шин устраняет вероятность возникновения конфликтов.

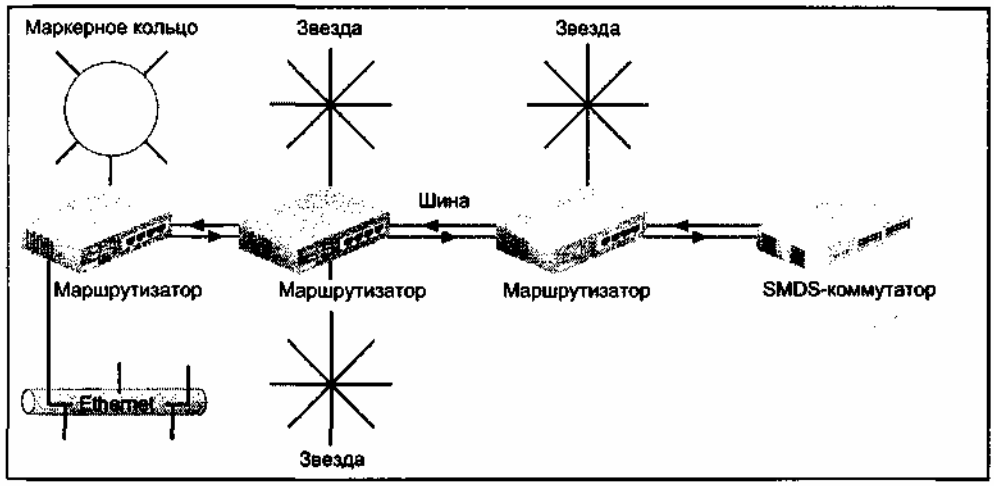


Рис. 7.13. Глобальная сеть на основе службы SMDS

В DQDB-интерфейсе информационный поток по каждой шине квантуется по времени, при этом используется разновидность множественного доступа с временным разделением (TOMA). Любое подключенное устройство может в любой момент получить доступ к шине за исключением тех случаев, когда по шине передаются данные. Тактируемый доступ осуществляется посредством распределения квантов времени между устройствами, так что ни одно устройство не может получить выделенный квант полностью. К SMDS-шине можно подключить до 512 устройств, при этом ее общая длина может составить до 160 километров.

Для организации SMDS-шины обычно используются Т-линии. Скорость передачи данных по ним будет, однако, меньше общей пропускной способности, поскольку часть полосы пропускания выделяется для управляющих и служебных сигналов. Например, линия Т-1 имеет скорость 1,544 Мбит/с, а служба SMDS сможет передавать данные по этой линии только со

скоростью 1,17 Мбит/с. При использовании линии Т-3 с уровнем доступа DS-3 служба SMDS делит линию на несколько классов обслуживания, пропускная способность которых образуется как комбинация скоростей 4, 10, 16, 25и 34 Мбит/с.

Примечание

Некоторые телекоммуникационные компании предлагают услуги SMDS по частным линиям Т-1, которые имеют скорость передачи 56 Кбит/с (а не полную скорость частной линии Т-1, которая составляет 64 Кбит/с).

Служба SMDS, которая в первую очередь предназначена для передачи данных, преобразует фреймы, полученные из локальных сетей, в ячейки. Исключение составляют фреймы маршрутизации и сетевых функций, которые должны конвертироваться и которые обрабатываются интерфейсом SMDS Data Exchange Interface (SMDS-DXI). Этот интерфейс вместо ячеек использует фреймы в формате High-level Data Link Control (HDLC), который напоминает форматы протоколов X.25 LAPB и ISDN LAPD. I

Многоуровневые коммуникации SMDS и структура ячейки

Служба SMDS реализует коммуникационные уровни, соответствующие Физическому, Канальному и Сетевому уровням эталонной модели OSI (рис. 7.14)

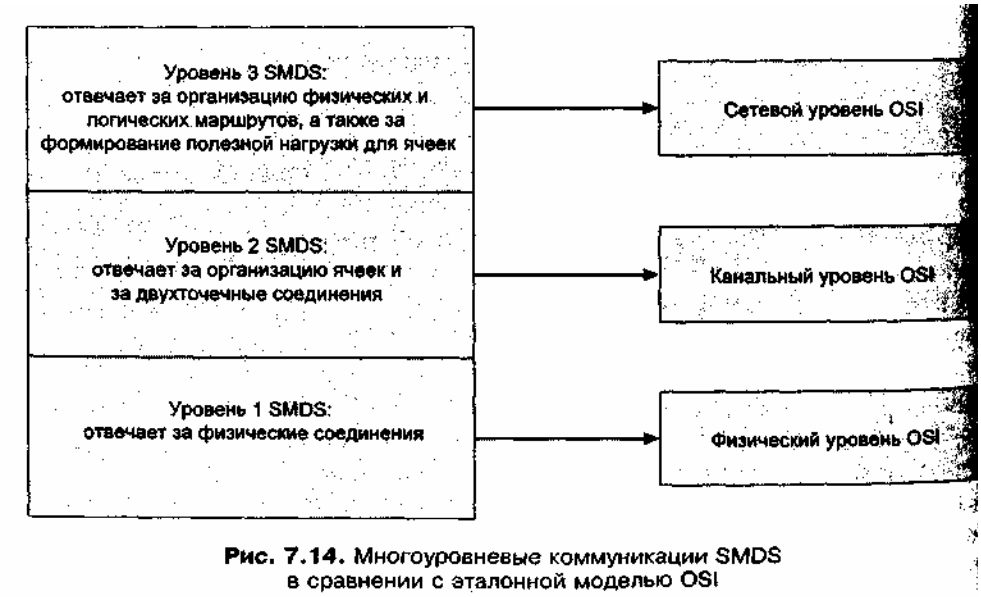


Рис. 7.14. Многоуровневые коммуникации SMDS в сравнении с эталонной моделью OSI

На Физическом уровне используется стандарт IEEE 802.6 на передачу данных в региональных сетях, а на Канальном уровне коммуникации осуществляются на подуровне LLC. Сетевой уровень образуют коммуникационные маршруты, служащие для передачи данных.

Ячейка SMDS имеет фиксированную длину, равную 53 байтам, и состоит из заголовка, модуля сегментации и хвостовика (рис. 7.15). В состав заголовка входят следующие поля:

- *Управление доступом* (Access Control) – содержит информацию, указывающую на то, откуда была отправлена ячейка: либо от клиентского оборудования (например, от маршрутизатора), либо от SMDS-коммутатора, расположенного у поставщика услуг;
- *Управление сетью* (Network Control) – указывает, например, тип содержимого ячейки: либо это управляющая информация, либо данные;
- *Тип сегмента* (Segment Type) – указывает, содержит ли ячейка начало, середину или окончание последовательности сегментов сообщения, или же все сообщение располагается в ячейке целиком;
- *Идентификатор сообщения* (Message ID) – содержит уникальный номер, присваиваемый всем ячейкам в последовательности сегментов сообщения и указывающий на то, что все эти ячейки должны обрабатываться как единое целое.

Управление доступом	Управление сетью	Тип сегмента	Идентификатор сообщения	Модуль сегментации	Длина полезной нагрузки	Контрольная (CRC) сумма для полезной нагрузки

Рис. 7.15. Ячейка SMDS

Модуль сегментации в ячейке содержит полезную нагрузку, которая представляет собой пользовательские данные, передаваемые по сети SMDS. Хвостовик ячейки состоит из двух полей: поля длины полезной нагрузки и контрольной (CRC) суммы для полезной нагрузки. Первое из этих полей указывает, какую часть, модуля сегментации составляет полезная нагрузка, а какая часть модуля пустая. Если полезная нагрузка отсутствует, поле длины полезной нагрузки содержит нули. Поле контрольной (CRC) суммы Для полезной нагрузки позволяет принимающему узлу убедиться в том, что информация, содержащаяся в полях типа сегмента, идентификатора сообщения, модуля сегментации и в поле длины полезной нагрузки, не исказилась в процессе пересылки. Все перечисленные поля содержат информацию, определяющую правильность приема и интерпретации полезной нагрузки. Контрольная сумма представляет собой число, полученное от сложения всех полей.

Особенности подключения к сетям SMDS

Помимо того, что сети SMDS обеспечивают высокую скорость передачи данных и совместимы с технологиями B-ISDN, SONET и ATM, а также Т-линиями, эти сети предоставляют пользователям надежные средства безопасности. Например, доступ к сети со стороны узла можно ограничить и разрешить его только группам адресов или отдельным адресам. Кроме того, для передачи особо важной информации можно организовать частные сети. Клиенты могут оплачивать сетевые услуги с учетом степени использования SMDS-служб. Слабым местом сетей SMDS является их недостаточная доступность (по сравнению с сетями X.25, frame relay и ISDN). Кроме того, сети SMDS предназначены только для передачи данных.

Линии DSL

Digital Subscriber Line (DSL или *XDSL)* (Цифровая абонентская линия) – эта технология, использующая усовершенствованные методы модуляции в существующих телекоммуникационных сетях и обеспечивающая высокие скорое передачи данных между абонентом и региональной телефонной или телекоммуникационной компанией. Технология DSL позволяет передавать данные, речь и видео, а также файлы мультимедийных приложений. Первоначально она предназначалась надомным работникам и мелким фирмам, однако ее все чаще используют средние и крупные компании в качестве средства "последней мили", соединяющей площадки клиента и телекоммуникационной компании. Телекоммуникационный акт (Telecommunications Act), принятый в 1996 году, особенно повлиял на развитие DSL, поскольку способствовал тому, что поставщики услуг телекоммуникаций и кабельного телевидения стали развивать средства интерактивных коммуникаций на основе существующих телефонных сетей.

Ниже перечислены области применения технологии DSL, в которых она особенно эффективна:

- создание линий связи для надомных работников;
- доступ к Интернету (особенно передача файлов к клиенту и в обратном направлении);
- сетевой доступ к средствам мультимедиа, в том числе к новинкам музыкальной и киноиндустрии;
- быстрая передача больших графических файлов (например, карт) между различными узлами;
- проведение интерактивных учетных занятий или семинаров;
- реализация распределенных клиент-серверных приложений для географически удаленных пользователей.

Совет)

Дополнительную информацию о Телекоммуникационном акте 1996 года можно получить в Интернете по адресу **www.fcc.gov/telecom.html.**

Основные понятия DSL

DSL – это цифровая технология на основе медных проводов, проложенных и используемых телефонными службами. Для работы с этой технологией в устройство, подключаемое к сети DSL, необходимо установить интеллектуальный адаптер. Таким устройством, к примеру, может быть компьютер, сервер доступа или маршрутизатор. Для компьютера подобный адаптер может выглядеть как внутренняя плата модема, а для маршрутизатора он может представлять собой сменный модуль.

На рис. 7.16 показано соединение, использующее маршрутизатор, оборудованный модулем адаптера DSL. Для небольшой офисной сети адаптер DSL и маршрутизатор могут быть объединены в одно устройство, имеющее размер небольшого коммутатора или концентратора. Адаптер является полностью цифровым, т. е. он не преобразует цифровой сигнал терминального оборудования (компьютера или сетевого устройства) в аналоговый сигнал, а передает цифровой сигнал непосредственно в телефонную линию.

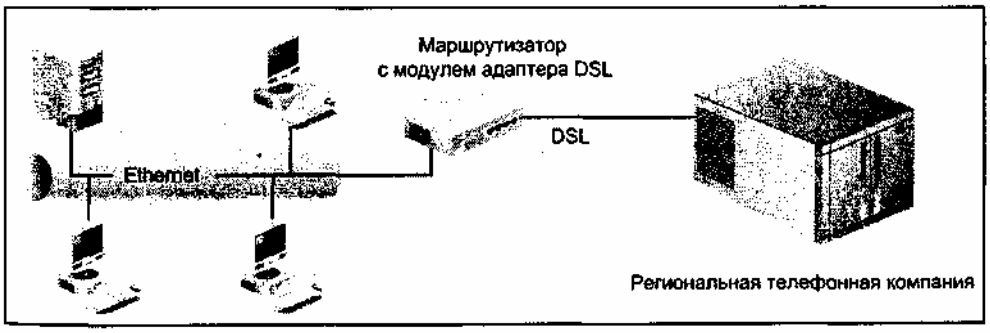


Рис. 7.16. Подключение сети к DSL-линии

Обычно адаптер подключается к телефонной розетке с помощью двух пар проводов. Для большинства версий DSL коммуникации по медному проводу являются симплексными (односторонними), т. е. одна пара проводов используется для передачи данных от абонента, а другая пара – для приема информации к абоненту. Таким образом реализуется поток восходящих данных к телекоммуникационной компании и поток нисходящих данных к абоненту. Максимальная скорость восходящего потока составляет 2,3 Мбит/с, а для нисходящего потока скорость может достигать 55 Мбит/с. Максимальное расстояние между абонентом и поставщиком услуг (без повторителя) для большинства версий DSL составляет 5,5 км (почти как для сетей ISDN)

Примечание

Реальная скорость передачи данных определяется несколькими факторами том числе типом используемой службы DSL, состоянием кабеля, расстоянием до поставщика услуг и скоростью шины в пользовательском оборудовании (например, в компьютере).

Если соединение осуществляется с помощью платы в пользовательском компьютере, адаптер DSL напоминает кабельный модем в том смысле, что он обеспечивает передачу данных с высокой скоростью. Однако по сравнению с кабельным модемом адаптер имеет несколько преимуществ. Например, кабельный модем работает с линией, которая совместно используется несколькими абонентами, т. е. передаваемый сигнал может быть перехвачен и прочитан другим абонентом. DSL-линия выделяется конкретному пользователю, что уменьшает вероятность перехвата сигнала без ведома телекоммуникационной компании. Кроме того, абонент DSL использует всю полосу пропускания своей линии (в отличие от пользователя кабельного модема, который делит полосу пропускания с другими пользователями и, следовательно, может сталкиваться с задержками в работе при большом трафике). Недостатком технологии DSL является то, что она не настолько распространена, как доступ с помощью кабельного модема.

Типы служб DSL

Существуют восемь основных типов служб DSL:

- Asymmetric Digital Subscriber Line (ADSL);
- G.lite Asymmetric Digital Subscriber Line (G.lite ADSL);
- Integrated Services Digital Network Digital Subscriber Line (IDSL);

- Rate Adaptive Asymmetric Digital Subscriber Line (RADSL);
- High-Bit-Rate Digital Subscriber Line (HDSL);
- Symmetric High-Bit-Rate Digital Subscriber Line (SHDSL);
- Very High-Bit-Rate Digital Subscriber Line (VDSL);
- Symmetric Digital Subscriber Line (SDSL).

Примечание

Имеются также и другие, частные версии (модификации) DSL, которые не рассматриваются в этой книге по причине ограниченного распространения и отсутствия стандартов. Среди таких версий можно упомянуть следующие технологии: Etherloop от фирмы Nortel Networks, Consumer Digital Subscriber Line (CDSL) от фирмы Rockwell International и Consumer Installable Digital Subscriber Line (CiDSL) от компании Globespan.

Asymmetric Digital Subscriber Line (ADSL)

Появление технологии *Asymmetric Digital Subscriber Line (ADSL)* (Асимметричная цифровая абонентская линия) стало возможным тогда, когда Федеральная комиссия связи США (FCC) разрешила телекоммуникационным компаниям передавать телевизионные сигналы домашним пользователям. В настоящее время ADSL является самой распространенной модификацией DSL. Помимо передачи данных и файлов мультимедийных приложений, эта технология может эффективно применяться для интерактивного мультимедиа и дистанционного обучения.

Перед тем как передавать данные, аппаратура ADSL проверяет телефонную линию на наличие шума и отсутствие ошибок. Этот процесс называется прямым исправлением ошибок (forward error correction). При своем появлении технология ADSL обеспечивала скорость восходящего потока, равную 64 Кбит/с, а нисходящие данные передавались со скоростью 1,544 Мбит/с (как в линии T-1). В настоящее время эти скорости составляют 576–640 Кбит/с и 6 Мбит/с (максимум) соответственно. Также в ADSL может использоваться третий коммуникационный канал для передачи речи с частотой 4 кГц, причем это осуществляется одновременно с передачей данных.

Совет

Если ADSL будет использоваться одновременно для цифровой и телефонной связи, между ADSL-линией, идущей от телекоммуникационной компании, и телефоном необходимо поместить недорогое фильтрующее устройство. Этот фильтр, имеющий с двух сторон гнезда для разъемов обычного телефонного шнура, служит для устранения шума в линии, который может ухудшить качество телефонных разговоров. Однако не следует устанавливать такой фильтр между входящей линией и цифровым адаптером DSL.

Для работы ADSL используется один из двух отличающихся методов передачи сигналов: амплитудная модуляция без несущей частоты (carrierless amplitude modulation, CAP) и дискретные мультиканалы (discrete multitone, DMT). CAP-модуляция объединяет амплитудную и фазовую модуляции, позволяя достичь скорости передачи одного сигнала, равной 1,544 Мбит/с, при этом применяются те же методы, что реализованы в кабельном телевидении. DMT поддерживается институтом ANSI и является более новой технологией, которая разделяет всю полосу пропускания на 256 каналов с частотой 4 кГц. Передаваемые данные фрагментируются, каждому фрагменту назначается уникальный идентификатор, после чего фрагменты распределяются между всеми каналами. На принимающей стороне данные восстанавливают исходный вид, при этом используются идентификаторы фрагментов.

Одним из наиболее обещающих проектов, связанных с ADSL, является разработка интерфейса связи с сетями ATM. В этом случае ADSL сможет конкурировать с технологией SONET при объединении локальных ATM-сетей.

G.lite Asymmetric Digital Subscriber Line (G.lite ADSL)

G.lite Asymmetric Digital Subscriber Line (G.lite ADSL) (Асимметричная шифровая абонентская линия G.lite) – это разновидность ADSL, созданная для совместимости с технологией *Plug-and-Play (PnP),* с помощью которой компьютерные операционные системы могут автоматически конфигурировать новые установленные аппаратные средства. Линия G.lite ADSL позволяв передавать восходящие

данные со скоростью 500 Кбит/с и нисходящие – Я скоростью 1,5 Мбит/с.

Integrated Services Digital Network Digital Subscriber Line (IDSL)

Во многих новых жилых и деловых районах распространено устройство телефонной сети, называемое Digital Loop Carrier (Цифровой контурный канал) и предназначенное для совершенствования методов разводки телефонного кабеля, а также для реализации услуг DSL. Для использования DSL в таких районах была разработана технология *Integrated Services Digital Network Digital Subscriber Line (IDSL)* (Цифровая абонентская линия ISDN). Линия IDSL позволяет передавать восходящие и нисходящие данные со скоростью до 144 Кбит/с. Другим достоинством линий IDSL является то, что они совместимы с существующими терминальными адаптерами ISDN.

Rate Adaptive Asymmetric Digital Subscriber Line (RADSL)

Технология *Rate Adaptive Asymmetric Digital Subscriber Line (RADSL)* (Асимметричная цифровая абонентская линия с адаптивной скоростью), базирующаяся на принципах ADSL, первоначально была разработана для передачи видео по запросу. В отличие от ADSL, она позволяет менять скорость передачи, информации в зависимости от того, передаются ли данные, файлы мультимедиа или речь. Для определения скорости обмена имеются два способа. Во-первых, телекоммуникационная компания может установить определенную скорость для каждой абонентской линии в зависимости от того, для чего эта линия будет использоваться. Во-вторых, поставщик услуг может разрешить адаптивную настройку скорости в зависимости от типа информации, передаваемой по линии.

Для абонентов технология RADSL имеет преимущества, поскольку они будут оплачивать только ту часть полосы пропускания, которая им требуется. Для телекоммуникационной компании важным достоинством линии RADSL является то, что она сможет выделять неиспользуемую полосу пропускания другим абонентам. Немаловажно и то, что в случае неполного использования полосы пропускания линия RADSL может быть длиннее, т. е. к ней смогут подключиться абоненты, находящиеся на расстоянии свыше 5,5 км (от поставщика услуг). RADSL обеспечивает скорость восходящего потока (от абонента) до 1 Мбит/с и скорость нисходящего потока (к абоненту) до 7 Мбит/с.

High Bit-Rate Digital Subscriber Line (HDSL)

Первоначально технология *High Bit-Rate Digital Subscriber Line (HDSL)* (Высокоскоростная цифровая абонентская линия) разрабатывалась для осуществления дуплексных коммуникаций по двум парам медных телефонных проводов с фиксированной скоростью приема и передачи, равной 1,544 Мбит/с или 2,3 Мбит/с, для расстояний не свыше 3,6 км. Другой вариант HDSL был создан для использования только одной из двух пар телефонных проводов, при этом скорость дуплексных коммуникаций равнялась 768 Кбит/с. Ограничением технологии HDSL является то, что в отличие от ADSL и RADSL она не поддерживает передачу речи. Такая ситуация объясняется тем, что для этого нужны специализированные конвертеры и адаптеры. Однако технология HDSL представляет собой альтернативу линиям T-1, поскольку она может работать с существующими телефонными линиями и требует меньших затрат на реализацию. Поэтому она особенно полезна для компаний, которым требуется объединять локальные сети.

Новая версия, названная HDSL2, позволяет по одному медному кабелю передавать восходящий и нисходящий потоки, содержащие данные сетей ATM или frame relay, со скоростью 1,544 Мбит/с. В настоящее время технология HDSL2 не поддерживает речевых коммуникаций.

Symmetric High-Bit-Rate Digital Subscriber Line (SHDSL)

Технология *Symmetric High-Bit-Rate Digital Subscriber Line (SHDSL)* (Высокоскоростная симметричная цифровая абонентская линия, также называемая G.shdsl, позволяющая передавать данные по одному или двум кабелям. При использовании двух кабелей максимальное расстояние составляет 6,4 км, что превышает аналогичный показатель для старых версий DSL, равный 5,5 км. Выигрыш достигается за счет дополнительного поглощения отраженного сигналы в линии. Скорость восходящего и нисходящего потоков может меняться от 192 Кбит/с до 2,3 Мбит/с. Одним из ограничений технологии SHDSL является то, что она предназначена для пересылки данных и не обеспечивает одновременную передачу данных и речи.

Very High-Bit-Rate Digital Subscriber Line (VDSL)

Технология *Very High Bit-Rate Digital Subscriber Line (VDSL)* (Сверхскоростная цифровая абонентская линия) создавалась как альтернатива сетям на основе коаксиального или оптоволоконного кабеля. Она позволяет для передачи нисходящего потока (к абоненту) достичь скорости 51–55 Мбит/с, а для восходящего потока (от абонента) – 1,6–2,3 Мбит/с. Хотя данная технология обеспечивает очень высокую пропускную способность, длина линий VDSL относительно невелика и равняется 300–1800 м, что уменьшает их ценность а качестве средства построения глобальных сетей. Линии VDSL работают подобно линиям RADSL в том смысле, что их полоса пропускания может выбираться автоматически в соответствии с типом передаваемой информации, также они напоминают линии ADSL с дискретными мультиканалами (DMT), поскольку в них создается множество каналов (в кабелях на основе витой шары) и они позволяют одновременно передавать речь и данные.

Symmetric Digital Subscriber Line (SDSL)

Линия *Symmetric Digital Subscriber Line (SDSL)* (Симметричная цифровая абонентская линия) напоминает ADSL-линию, однако скорость передачи как для восходящего, так и для нисходящего потока данных в ней составляет 384 Кбит/с. Линии SDSL особенно эффективны для организации видеоконференций и дистанционного обучения, поскольку скорость передачи информации одинакова в обоих направлениях.

Разновидности линий DSL перечислены в табл. 7.2. Выполните практическое задание 7-5, в котором сравниваются услуги DSL, предлагаемые различными региональными телефонными компаниями.

Таблица 7.2. *Разновидности DSL*

Технология DSL	**Скорость восходящего (upstream) потока данных**	**Скорость нисходящего (downstream) потока данных**
Asymmetric Digital Subscriber Line (ADSL)	576–640 Кбит/с	До 6 Мбит/с
G.lite Asymmetric Digital Subscriber Line (G.lite ADSL)	До 500 Кбит/с	До 1 ,5 Мбит/с
Integrated Services Digital Network Digital Subscriber Line (IDSL)	До 144 Кбит/с	До 144 Кбит/с
Rate Adaptive Asymmetric Digital Subscriber Line (RADSL)	До 1 Мбит/с	До 7 Мбит/с
High-Bit-Rate Digital Subscriber Line (HDSL)	Фиксированные скорости 1 ,544 Мбит/с и 2,3 Мбит/с	Фиксированные скорости 1 ,544 Мбит/с и 2,3 Мбит/с
Symmetric High-Bit-Rate Digital Subscriber Line(SHDSL)	192 Кбит/с -2,3 Мбит/с	192 Кбит/с -2,3 Мбит/с
Very High-Bit-Rate Digital Subscriber Line (VDSL)	1,6-2,3 Мбит/с	51-55 Мбит/с
Symmetric Digital Subscriber Line (SDSL)	384 Кбит/с	384 Кбит/с

Сети SONET

Synchronous optical network (SONET) (Синхронная оптическая сеть) – это оптоволоконная технология, позволяющая передавать данные быстрее, чем 1 Гбит/с: Она быстро развивается, и все больше и больше телефонных компаний предлагают соответствующие услуги. Компании Bellcore и Alliance for Telecommunications Industry Solutions (AXIS) создали стандарт, который в

1984 году был предложен комитету ANSI в качестве стандарта открытых, гибких и доступных коммуникаций с использованием оптоволокна. В 1986 году союз ITU-T начал разработку аналогичных рекомендаций (определяющих методы и скорости передачи), которые, однако, воплотились в стандарт, названный Synchronous Digital Hierarchy (SDH) и используемый преимущественно в Европе. В настоящее время скорость передачи данных в сетях SONET достигает 9,953 Гбит/с, и в перспективе достижима скорость, равная 13,271 Гбит/с.

Одним из достоинств технологии SONET является то, что она стандартизована, поэтому оконечное сетевое оборудование можно приобрести у многих производителей. Для создания сверхскоростных коммуникационных каналов сеть SONET может подключаться к интерфейсам для ATM, ISDN, маршрутизаторов и другого оборудования. Другое достоинство технологии SONET состоит в том, что с ее помощью высокоскоростные коммуникации можно осуществлять на очень больших расстояниях (например, между городами или странами).

Ниже перечислены области применения технологии SONET, в которых она особенно эффективна:

- создание сверхскоростных каналов передачи данных между удаленными сетями (например, между кампусами колледжа и исследовательскими центрами, спонсируемыми частными компаниями);
- проведение видеоконференций между удаленными площадками;
- дистанционное обучение;
- высококачественная передача музыки и видео;
- высокоскоростная передача сложных графических изображений (например, топографических карт) и фотографий, полученных со спутников.

Коммуникационная среда и характеристики

Для высокоскоростной передачи данных в сетях SONET используются одномодовый оптоволоконный кабель и Т-линии (начиная с линий Т-3). Основной транспортный механизм реализован на Физическом уровне модели OSI, что позволяет передавать через сеть SONET пакеты других коммуникационных технологий (таких как FDD1, SMDS и ATM). Наибольшая совместимость сетей SONET достигается с технологиями, использующими ячейки фиксированной длины (в частности, с сетями ATM и SMDS), несколько хуже совместимость *с* технологиями, где применяются фреймы переменив длины.

Сеть SONET функционирует на базовом уровне со скоростью передачи 51,84 Мбит/с (optical carrier level 1, OC-1), а электрический эквивалент называется Synchronous Transport Signal Level 1 (STS-1). Начиная с этого уровня, скорость сигнала может постепенно увеличиваться за счет коммутации каналов и достигать значения, необходимого для конкретного типа службы. В табл. 7.3 приведен имеющийся в настоящее время набор скоростей. Ожидается, что в будущем скорости передачи данных в сетях SONET достигнут уровня STS level 256, что соответствует 13,271 Гбит/с. В настоящее время чаще всего предлагаются услуги уровней OC-3, OC-12, OC-48 и OC-192. Выполните практическое задание 7-6, в котором вы познакомитесь с услугами SONET, предлагаемыми региональными телефонными компаниями.

Таблица 7.3. *Скорости передачи данных для сетей SONET*

Уровень оптического канала (OC)	Уровень STS	Коммуникационная скорость в Мбит/с
OC-1	STS-1	51 ,84
OC-3	STS-3	155,52
OC-9	STS-9	466,56
OC-1 2	STS-12	622,08
OC-1 8	STS-18	933,12
OC-24	STS-24	1244,16

Уровень оптического канала (ОС)	Уровень STS	Коммуникационная скорость в Мбит/с
ОС-36	STS-36	1866,24
ОС-48	**STS-48**	**2488,32**
ОС-96	**STS-96**	**4976,64**
ОС- 192	**STS-192**	**9953,28**

Примечание

Электрический эквивалентный уровень STS определяет количество каналов, которые сеть SONET использует для передачи данных. Например, уровень STS-1 указывает на то, что задействован один канал, а уровню STS-12 соответствует 12 каналов.

Стандарт ITU-T Synchronous Digital Hierarchy (SDH) аналогичен SONET, однако базовая скорость SDH равна 155,52 Мбит/с (а не 51,84 Мбит/с), что соответствует уровню, называемому Synchronous Transport Model Level 1 (STM-1). Скорости оптических коммуникаций SDH перечислены в табл. 7.4.

Таблица 7.4. *Уровни SDH в сравнении с уровнями SONET*

Уровень SDH	Эквивалентный уровень SONET	Коммуникационная скорость в Мбит/с
STM-1	ОС-3	155,52
STM-3	ОС-9	466,56
STM-4	ОС-12	622,08
STM-6	00-1 8	933,12
STM-8	ОС-24	1244,16
STM-12	ОС-36	1866,24
STM-16	ОС-48	2488,32
STM-32	ОС-96	4976,64
STM-64	ОС-192	9953,28

Сети SONET описаны в стандартах ANSI T1.105 и ANSI T1.119, а спецификация SDH закреплена в следующих стандартах: ITU-T G.707, ITU-T G.781, ITU-T G.782, ITU-T G.783 и ITU-T G.803.

Топология сети SONET и обнаружение отказов

Для организации сети SONET используется кольцевая топология, а для восстановления в случае отказа имеются три возможных способа (выбор реализуемого способа зависит от архитектуры, используемой поставщиком услуг глобальной сети): переключение однонаправленного маршрута, автоматическое защитное переключение и переключение двунаправленной линии.

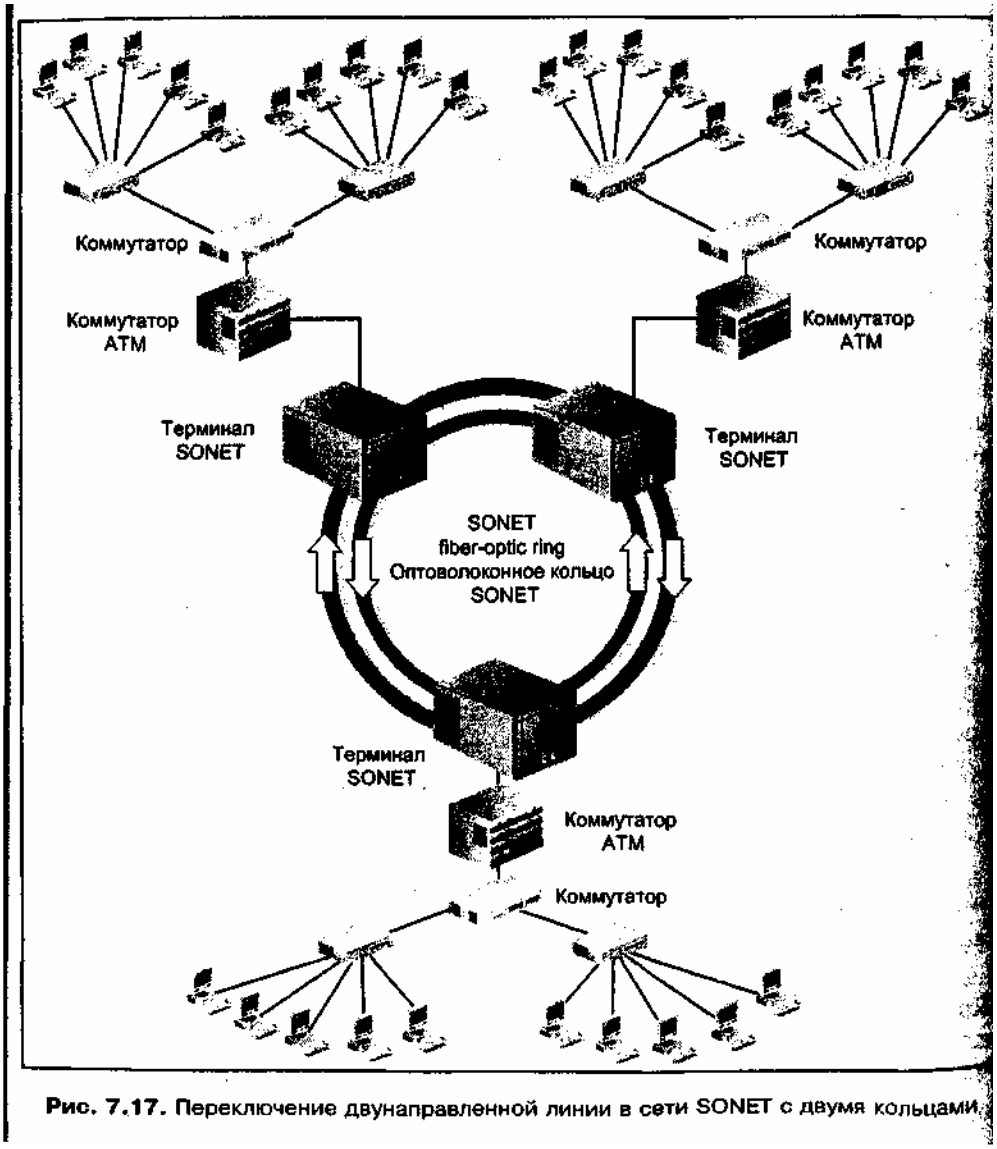


Рис. 7.17. Переключение двунаправленной линии в сети SONET с двумя кольцами

При переключении однонаправленного маршрута используется только одно оптоволоконное кольцо. Данные передаются по этому кольцу в обоих направлениях. Принимающий узел сам определяет, какой сигнал принимать. Если один маршрут становится недоступным, сигнал все равно может достигнуть пункта назначения по альтернативному пути. Данные, посланные по альтернативному маршруту, предупреждают принимающий узел о том, что доступен только один маршрут.

При автоматическом защитном переключении, если обнаруживается неисправность в некоторой точке сети SONET, данные отправляются альтернативному коммутирующему узлу, который перенаправляет их в указанный пункт назначения.

Самый высокий уровень избыточности (до 99%) обеспечивает третий способ восстановления – переключение двунаправленной линии. В этом случае используется двойное кольцо, при этом к каждому узлу всегда имеются два маршрута. Переключение двунаправленной линии показано на рис. 7.17. Данные одновременно посылаются по обоим кольцам, однако в противоположных направлениях. Если один из маршрутов становится недоступным, данные все равно смогут передаваться по второму маршруту.

Уровни SONET и эталонная модель OSI

Как показано на рис. 7.18, в сетях SONET используются четыре уровня протоколов, однако только нижний уровень действительно соответствует модели OSI. Этот уровень, аналогичный Физическому уровню модели OSI, называется Световым (Photonic). Он управляет передачей и преобразованием информационных сигналов. Передаваемые электрические сигналы трансформируются в световые сигналы, которые передаются в оптоволоконный кабель, а принимаемые световые сигналы преобразуются обратно в электрические. Также этот уровень контролирует передачу сигналов, в том числе проверяет форму светового импульса, уровни

передаваемой мощности и длину волны переданного сигнала.

Второй уровень называется Сегментирующим (Section). Этот уровень инкапсулирует данные, гарантирует их отправку в нужном порядке, обеспечивает синхронизацию каждого фрейма, а также обнаруживает коммуникационные ошибки.

Далее следует Канальный (Line) уровень, который обнаруживает неисправности (если таковые появляются) и выполняет аварийное переключение. Кроме того, он отвечает за синхронизацию и переключение сигналов, а также гарантирует доставку всего фрейма в заданный пункт назначения.

Верхний, Маршрутный (Path) уровень, обеспечивает выбор коммуникационного канала для сигнала. Например, сигналу ATM он может назначить один канал, а сигналу ISDN – другой. Также он обеспечивает надежность канала от источника к целевому узлу.

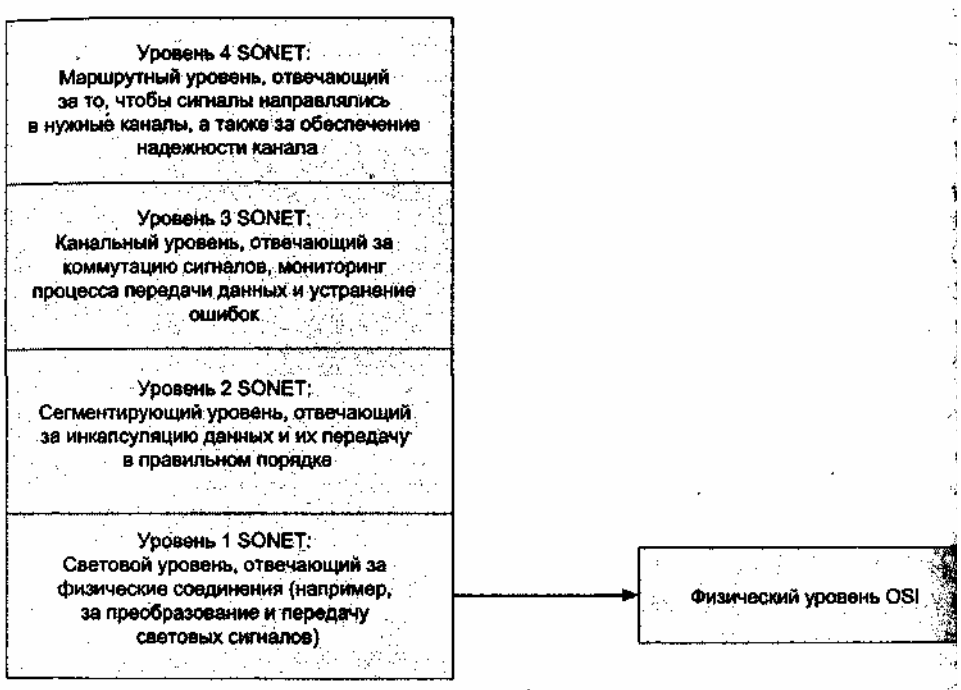


Рис. 7.18. Многоуровневые коммуникации SONET в сравнении с эталонной моделью OSI

Фрейм SONET

Фрейм STS-1 представляет собой базовый модуль для построения фрейма SONET, он показан на рис. 7.19. Длина фрейма STS-1 равна 90 байтам. Фрейм состоит из *виртуальных блоков* (virtual tributary), причем тип используемого блока определяется потребностями конкретного приложения. Виртуальный блок представляет собой отдельный конверт данных, он указывает, как передаваемый сигнал отображается во фрейме SONET. Например, определены виртуальные блоки для коммуникаций по линиям T-1 (VT1.5) и T-6 (VT6). Механизм виртуальных блоков позволяет передавать по сети SONET как асинхронные, так и синхронные сигналы.

Помимо того, что фрейм STS-1 передает несколько виртуальных блоков, он также содержит вводную часть со служебными данными. Сюда входят разряды, используемые для обнаружения ошибок и выполнения других транспортных задач.

Служебные разряды для управления сегментацией и транспортировкой	Служебные разряды для управления маршрутами	VT1.5	VT1.5	VT1.5	VT1.5	VT6	VT6

Рис. 7.19. Фрейм STS-1 сети SONET

Передача протокола PPP по сетям SONET

В настоящее время ведутся работы по реализации стандарта RFC 2615, в котором описаны методы непосредственной передачи протокола *Point-to-Point Protocol (PPP)* по сетям SONET и SDH. Эти работы инициировали компания Ascend Communications и Проблемная группа проектирования Интернета (IETF). Протокол PPP применяется для того, чтобы инкапсулировать и передавать по глобальным сетям обычные протоколы локальных сетей. Если вы для подключения к Интернету используете модем, то, скорее всего, работаете с протоколом PPP. Стандарт RFC 2615 предполагает, что протоколы TCP/IP, NetBEUI или IPX/SPX могут инкапсулироваться в PPP и затем пересылаться по сети SONET. Дополнительная информация о протоколе PPP содержится в этой главе ниже.

Совет

Копию стандарта RFC 2615 можно получить по адресу **ftp://ftp.isi.edu/in-notes/ rfc2615.txt.**

Региональные Ethernet-сети (Optical Ethernet)

Высокоскоростные технологии *Optical Ethernet* начинают конкурировать с сетями SONET и frame relay в региональных сетях Ethernet, реализованных на базе оптоволоконного кабеля. Несколько компаний поставляют решения на основе Optical Ethernet для развертывания региональных сетей. В состав таких сетей обычно входят следующие компоненты:

- магистраль Gigabit Ethernet или 10 Gigabit Ethernet;
- подключения по многомодовому оптоволоконному кабелю, имеющие длину до 9,6 км;
- подключения по одномодовому оптоволоконному кабелю, имеющие длину до 71 км.

На рис. 7.20 представлена стандартная конфигурация сети Optical Ethernet, основной задачей которой является подключение локальных сетей на базе Fast Ethernet или Gigabit Ethernet к региональной сети Optical Ethernet, построенной на основе Gigabit Ethernet или 10 Gigabit Ethernet.

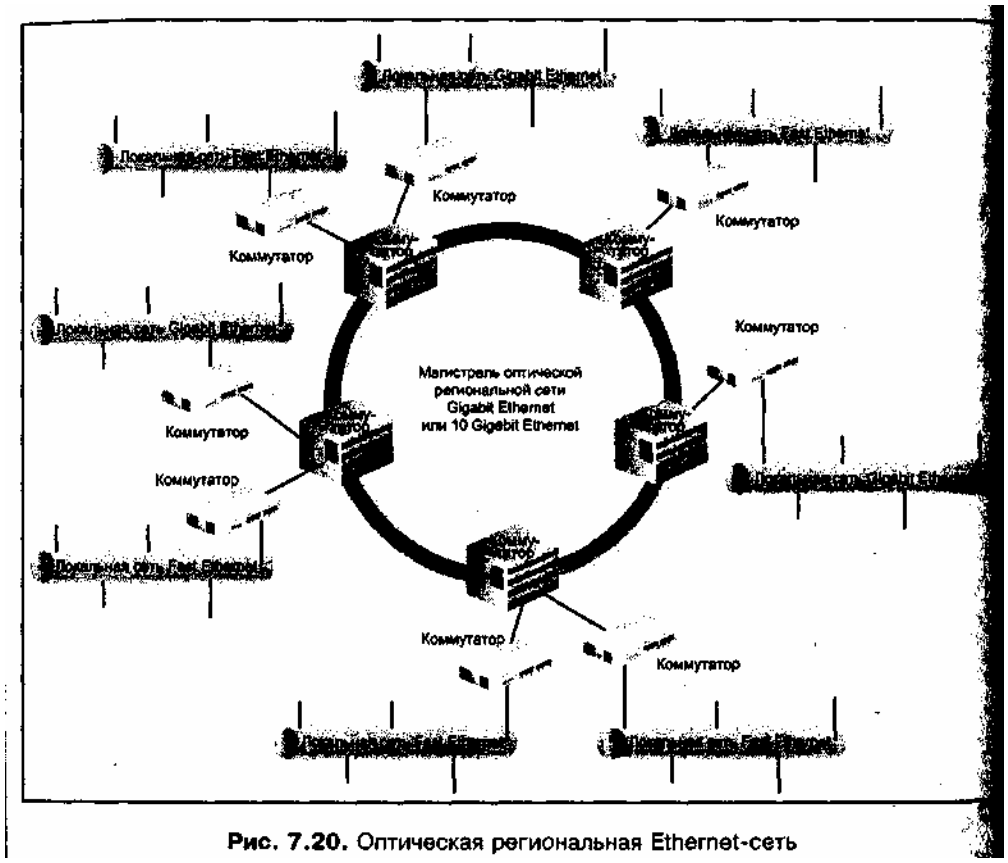


Рис. 7.20. Оптическая региональная Ethernet-сеть

Каждой локальной сети, подключенной к магистрали Optical Ethernet, назначается класс обслуживания в соответствии с условиями контракта, заключенного пользователем. Согласно более дорогим контрактам предоставляются классы обслуживания, дающие клиенту более высокий приоритет и большую полосу пропускания. При уменьшении стоимости контракта пользовательский трафик будет иметь низкий приоритет и меньшую полосу пропускания. Классы обслуживания

устанавливаются на базе стандарта IETF Defferentiated Services (DifTServ), который изначально был разработан для коммуникаций Интернета. Дополнительную информацию о стандарте DiffServ можно найти в RFC 2475, «An Architecture for Differentiated Services», по адресу **ftp://ftp.isi.edu/in-notes/rfc2475.txt.**

Выполнив практическое задание 7-7, вы узнаете, как технологии глобальных сетей, рассматриваемые в этой главе, используются в бизнесе.

Дополнительные протоколы глобальных сетей

Перед тем как закончить обсуждение методов передачи данных в глобальных сетях, следует познакомиться с тремя протоколами глобальных сетей, которые используются для удаленных коммуникаций, осуществляемых в этих сетях. Два из этих протоколов (Serial Line Internet Protocol, SLIP и Point-to-Point Protocol, PPP) служат для инкапсуляции одного или нескольких протоколов локальных сетей (например, TCP/IP) при их передаче по каналам глобальной сети. Третий протокол (Signaling System 7, SS7) предназначен для определения самых быстрых маршрутов в телекоммуникационных сетях.

SLIP

Протокол *Serial Line Internet Protocol (SLIP)* (Межсетевой протокол для последовательного канала) изначально предназначался для UNIX-систем и служит для осуществления двухточечных коммуникаций между компьютерами, серверами и хостами, работающими с TCP/IP. Например, SLIP применяется в том случае, когда пользователь может передавать данные между удаленным домашним компьютером и UNIX-системой, находящейся в офисной локальной сети (рис. 7.21). Для подключения к UNIX-компьютеру может использоваться коммутируемая телефонная линия, а коммуникации ведутся с помощью пакетов TCP/IP, инкапсулированных в SLIP.

Для хоста SLIP является протоколом глобальной сети, координирующим сеансы связи по телефонной линии с использованием модемов. После того как протокольная информация (содержащая полезную нагрузку) достигает пункта назначения, заголовок и хвостовик SLIP удаляются и пакет TCP/IP остается в "чистом виде".

Нужно заметить, что SLIP является достаточно старым протоколом удаленных коммуникаций и содержит больше служебной информации, чем протокол PPP (обсуждаемый в следующем разделе). Новой модификацией SLIP является протокол *Compressed Serial Line Internet Protocol (CSLIP)* (Межсетевой протокол для сжатого последовательного канала), который сжимает заголовок каждого пакета, передаваемого по каналу удаленной связи. CSLIP уменьшает объем служебной информации SLIP-подключения благодаря тому, что он уменьшает размер заголовка, в результате чего скорость коммуникаций увеличивается. Однако на принимающем узле заголовок, нужно распаковать.

Оба протокола (SLIP и CSLIP) имеют общий недостаток: они не поддерживают аутентификацию сетевого подключения, препятствующую перехвату передаваемых данных. Кроме этого, они не позволяют ускорить передачу данных по соединению, автоматически организуя сетевые коммуникации на нескольких уровнях модели OSI. Еще одним минусом обоих протоколов является то, что они предназначены для асинхронной передачи данных, осуществляемой, например, при модемном соединении. Синхронные коммуникации (например, создание подключения через Интернет) эти протоколы не поддерживают. SLIP нельзя также использовать в том случае, когда сетевой администратор хочет в удаленном режиме (через Интернет) создать новую учетную запись в системах Windows NT Server или Windows 2000 Server с помощью средств удаленного администрирования. Систему Windows NT Server можно настроить на работу с протоколом SLIP, установив службы Remote Access Services (RAS), хотя это и не рекомендуется. RAS-сервер позволяет пользователям удаленно подключаться к этому серверу или через этот сервер входить в локальную сеть.

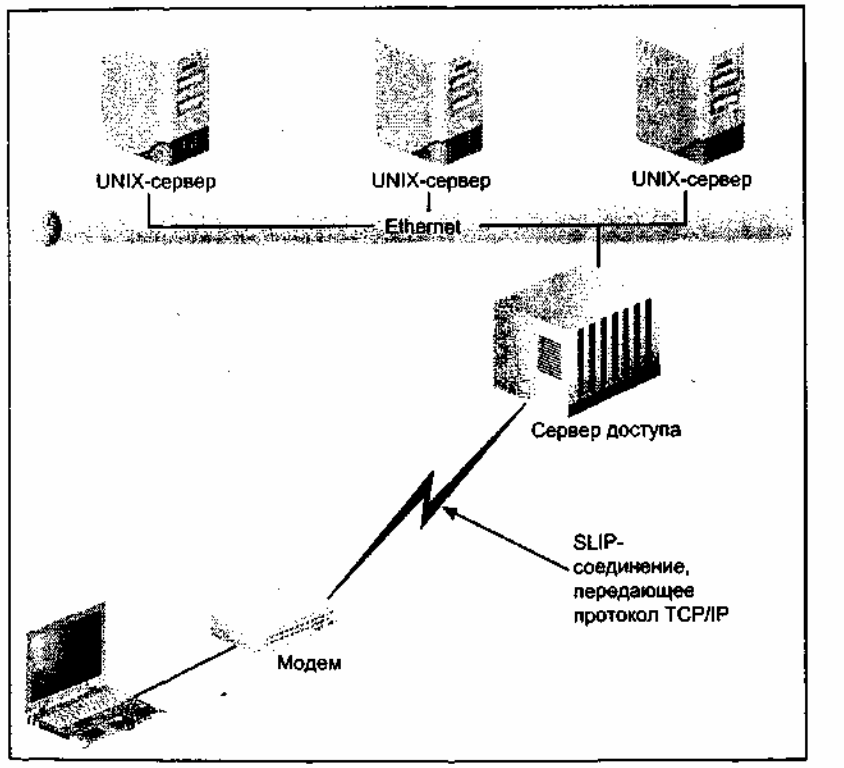


Рис. 7.21. Использование протокола SLIP
для организации удаленного соединения глобальной сети

Совет

Многие службы коммутируемого доступа не поддерживают SLIP и CSLIP, поскольку эти протоколы не обеспечивают аутентификации. Из-за отсутствия у протокола SLIP средств безопасности применяйте его только тогда, когда конфигурируемая операционная система компьютера не поддерживает протокол PPP.

PPP

Протокол *Point-to-Point Protocol (PPP)* (Протокол двухточечного соединения) применяется для удаленных коммуникаций чаще, чем SLIP или CSLIP, поскольку он использует меньше служебной информации, имеет больше возможностей и обеспечивает хорошую защиту. PPP поддерживает больше сетевых протоколов, чем SLIP, в их число входят протоколы IPX/SPX, NetBEUI и TCP/IP. PPP может автоматически организовывать и осуществлять одновременно коммуникации, соответствующие нескольким уровням модели OSI. Кроме того, он обеспечивает безопасность, аутентифицируя и шифруя соединения.

В дополнение к PPP имеется более новый протокол *Point-to-Point Tunneling Protocol (PPTP)* (Протокол туннелированного двухточечного соединения), который позволяет использовать Интернет для удаленного подключения к сетям, а также организовывать частные виртуальные сети (VPN). С помощью PPTP менеджер компании может, например, из дома подключиться к Интернету по коммутируемой линии и получить доступ к документам, хранящимся в корпоративной сети или VPN-сети. Скорее всего, вы уже пользуетесь протоколом PPP, если работаете в системах Windows 2000, Windows XP или Red Hat Linux *7.x* (выполните практические задания 7-8 и 7-9 для того, чтобы узнать, как протокол PPP конфигурируется в этих системах).

Оба протокола (PPP и PPTP) поддерживают синхронные и асинхронные коммуникации, позволяя передавать данные через модемы, коммутируемые телефонные линии, выделенные линии, сети ISDN, X.25 и SONET. Протокол PPP имеется в системах Windows 95/98, Windows NT, Windows 2000 и Windows XP. Например, если сервер Windows 2000 сконфигурирован как сервер удаленного доступа (RAS-сервер), то его можно настроить на прием удаленных подключений с использованием PPP.

Протокол PPP рекомендуется для тех сетей, где пользователи работают с несколькими

протоколами (например, с IPX/SPX и TCP/IP). Протоколы PPP и SLIP сравниваются в табл. 7.5.

Таблица 7.5. *Сравнение протоколов PPP и SLIP*

Возможность	PPP	SLIP
Поддерживаемые сетевые протоколы	TCP/IP, IPX/SPX и NetBEUI	TCP/IP
Поддержка асинхронных коммуникаций	Имеется	Имеется
Поддержка синхронных коммуникаций	Имеется	Отсутствует
Одновременная настройка сетевой конфигурации и автоматическое подключение, при котором коммуникации между узлами возможны на многих уровнях модели OSI	Имеется	Отсутствует
Аутентификация соединения для защиты от подслушиваний	Имеется	Отсутствует

При использовании PPP или PPTP многие системы – Windows, UNIX и Mac OS – позволяют выполнять аутентификацию паролей и шифрование данных (эти функции отсутствуют у протоколов SLIP или CSLIP). Например, протоколы PPP и PPTP поддерживают протокол *Password Authentication Protocol (PAP)* (Протокол аутентификации паролей), который используется для проверки паролей, введенных при доступе к какому-нибудь серверу через глобальную сеть.

Протокол PAP сам по себе может аутентифицировать пароли, но не может их шифровать. В сочетании с PAP можно применять протокол *Challenge Handshake Authentication Protocol (CHAP)* (Протокол аутентификации с предварительным согласованием вызова), шифрующий пароли, что затрудняет злоумышленникам их перехват и дешифрацию. CHAP предназначен для UNIX-систем, однако компания Microsoft разработала протокол MS-CHAP, который может применяться с компьютерами, работающими под управлением операционных систем Windows. Системы Windows 95/98, Windows NT, Windows 2000 и Windows XP, настроенные на работу с PPP или PPTP, могут также шифровать данные, пересылаемые по глобальной сети между рабочей станцией и удаленной сетью.

Совет

Для реализации глобальных коммуникаций наличие у протокола PPP средств безопасности (таких как PAP и CHAP) делает его намного привлекательнее, чем протокол SLIP.

Signaling System 7 (SS7)

Signaling System 7 (SS7) – это протокол глобальных сетей, утвержденный союзом ITU-T и предназначенный для определения самых быстрых коммуникационных маршрутов между разнообразными глобальными сетями, построенными на основе телекоммуникационных каналов: например, между каналами локального доступа и местной связи (local access and transport area, LATA) и каналами дальней связи или каналами информационного обмена (interexchange carrier, IXC) (каналы LATA и IXC рассматривались в *главе 2)*. В настоящее время протокол SS7 применяется в речевых коммуникациях для реализации таких служб, как роуминг вызовов в системах сотовой связи, голосовая почта и перенаправление вызовов служб 800. Протокол SS7 может эффективно маршрутизировать трафик между глобальными сетями и адаптирован для быстрой маршрутизации в глобальных сетях на основе T-линий и ATM.

Протокол SS7 может обеспечить скоростные коммуникации, благодаря следующим факторам:

- он поддерживает информационные базы маршрутов в различных опорных точках глобальной сети;
- он может перехватить запрос к центральному узлу (запрос на поиск кратчайшего маршрута для некоторого вызова) и быстро перенаправить тому узлу, который содержит соответствующую информацию о маршрутах;

- он отслеживает все телекоммуникационные вызовы, определяя кратчайший маршрут для этих вызовов, после чего обновляет соответствующую информационную базу.

Для реализации функций, выполняемых протоколом SS7, используются следующие средства:

- *пункты управления службами* (service control point), представляющие собой узлы глобальной сети, содержащие информационные базы маршрутизации (например, сведения о том, как можно некоторое соединение быстро перенаправить определенному оператору связи);
- *пункты переключения служб* (service switching point), расположенные в главных узлах глобальной сети и используемые для того, чтобы определить, какую базу данных пункта управления службами следует выбрать при поиске маршрута для определенных коммуникаций;
- *пункты передачи сигналов* (signal transfer point), работающие подобно маршрутизаторам и с максимальной скоростью соединяющие некоторый пункт переключения служб с соответствующим пунктом управления службами.

Резюме

- Технологии глобальных сетей достигли зрелости, и в настоящее время имеется множество типов сетей, начиная с X.25 и заканчивая Optical Ethernet. Тридцать лет назад первые глобальные сети на основе X.25 обеспечивали скорость передачи 65 Кбит/с. В настоящее время скорость передачи данных может достигать 10 Гбит/с и более.
- X.25 – это одна из первых технологий глобальной связи, разработанная в 1970-х годах. В ней используется коммутация пакетов. Сети X.25 имеют полосу пропускания до 2,048 Мбит/с и доступны во многих регионах, в особенности в Европе.
- В сетях frame relay используются некоторые принципы, примененные в сетях X.25, однако сети с ретрансляцией кадров являются действительно высокоскоростными глобальными сетями, обеспечивающими скорости до 45 Мбит/с. Многие корпоративные клиенты пользуются сетями frame relay для подключения своих удаленных площадок. Технология передачи голоса по сетям frame relay (voice over frame relay) позволяет компаниям уменьшить затраты на междугородные телефонные разговоры.
- Сети ISDN представляют собой технологию глобальной связи для передачи речи, видео и данных, которую региональные телефонные компании в США реализовали во многих регионах для развертывания телефонных и цифровых служб. Чаще всего применяются узкополосные сети ISDN (N-ISDN), которые в настоящее время имеют фактическую скорость передачи данных, соответствующую полосе пропускания линии T-1. Развиваются широкополосные сети ISDN (B-ISDN), являющиеся технологией глобальной связи, совместимой с другими высокоскоростными сетями (такими как ATM и SONET).
- SMDS – это высокоскоростная технология глобальных сетей, для реализации которой часто используются T-линии. Она представляет собой скоростную шину с полосой пропускания до 155 Мбит/с. Данная технология совместима со многими протоколами локальных сетей и широко используется в Европе для построения глобальных сетей.
- DSL-линии существуют во множестве модификаций и привлекают внимание сетевых администраторов благодаря тому, что с их помощью можно имеющийся телефонный провод на основе витой пары превратить в средство построения высокоскоростной глобальной сети, обеспечивающей скорость до 55 Мбит/с (при передаче данных к абоненту). В настоящее время наиболее распространенной версией DSL-линий является ADSL
- Услуги глобальной сети SONET предоставляют многие телефонные и телекоммуникационные компании, поскольку эта сверхскоростная сеть обеспечивает скорость передачи данных свыше 1 Гбит/с и, кроме того, она является хорошим средством для объединения высокоскоростных локальных сетей (включая сети ATM), не снижающим полосу пропускания между ними. Ожидается, что быстродействие сетей SONET достигнет 13,271 Гбит/с.
- Технология Optical Ethernet стала эффективным средством для построения региональных

сетей. Обычно для ее реализации используется оптоволоконная магистраль на базе Gigabit Ethernet или 10 Gigabit Ethernet. Для подключения имеющихся локальных сетей к региональной сети Optical Ethernet клиенты могут приобретать услуги различных классов.

- Многие глобальные сети строятся на базе трех протоколов удаленного доступа. Первым был разработан протокол SLIP, используемый UNIX-системами для инкапсуляции протокола TCP/IP при его передаче по сети. Существенным недостатком этого протокола является отсутствие механизмов безопасности. Протокол удаленного доступа PPP может инкапсулировать TCP/IP, NetBEUI и IPX/SPX. Важным достоинством протокола PPP является то, что он совместим с такими средствами безопасности, как протоколы PAP и CHAP. SS7 – это телекоммуникационный протокол, применяемый в тех случаях, когда в телекоммуникационной сети нужно найти самые эффективные маршруты.

Глава 8

Технологии ATM

По прочтении этой главы и после выполнения практических заданий вы сможете:

- перечислить основные характеристики ATM;
- объяснить многоуровневые коммуникации ATM;
- описать структуру ячейки ATM;
- рассказать о том, как работают сети ATM;
- обсудить вопросы проектирования сетей ATM;
- рассказать об использовании ATM в локальных и глобальных сетях;
- обсудить виртуальные локальные сети и их связь с ATM;
- обсудить вопросы-управления локальными и глобальными ATM-сетями.

Технология ATM (Asynchronous Transfer Mode – асинхронный режим передачи) была создана на базе принципов работы широкополосных ISDN-сетей (B-ISDN), поскольку первоначально рассматривалась в качестве основного средства быстрой передачи данных при организации коммуникаций в сетях B-ISDN. По мере развития эта сетевая технология заняла свою нишу в локальных и глобальных сетях, не считая сетей B-ISDN. Операторы дальней связи и региональные телефонные компании предлагают ATM для реализации глобальных коммуникаций, и зачастую эти услуги идут в одном пакете с возможностями SONET, frame relay и другими услугами глобальной связи.

Технология ATM имеет множество достоинств. Она легко масштабируется, поэтому скорость передачи данных в локальных или глобальных сетях может увеличиваться по мере их роста или при перерастании локальной сети в глобальную. С ее помощью можно решать проблемы перегруженности сети, сегментировать сети и даже обеспечивать высокоскоростное подключение настольных систем. Крупные банки и университеты используют ATM для организации глобальных коммуникаций между удаленными площадками, правительственные организации применяют ATM для связи отделений в пределах одного города, а в кинематографической промышленности технологии ATM используются для передачи фильмов.

Несмотря на достаточно широкое распространение, в настоящее время технологии ATM во многих локальных сетях начинают уступать свои позиций технологиям Gigabit Ethernet и 10 Gigabit Ethernet, которые зачастую проще в реализации и обходятся дешевле. В региональных сетях технологии ATM также сталкиваются с конкуренцией со стороны Optical Ethernet. Однако *в* глобальных сетях они имеют сильные позиции, поскольку совместимы с сетями SONET и frame relay.

В этой главе технология ATM рассматривается подробно. Вы узнаете о характеристиках ATM-сетей, многоуровневых коммуникациях ATM, а также о том, как в ATM-сетях вместо пакетов используются ячейки и как эти сети работают. После знакомства с основами ATM вы узнаете о компонентах ATM-сети и о том, как технология ATM применяется для организации локальных и глобальных сетей. В заключение будет рассказано о связях между ATM и виртуальными локальными сетями, а также об основных принципам управления ATM-сетями.

Введение в ATM

ATM – это метод высокоскоростной передачи информации (включая данные, речь, видео и мультимедиа) по сети. Основу технологии ATM составляют интерфейс и протокол, с помощью которого по обычному коммуникационному каналу можно коммутировать трафик, имеющий как постоянную так и переменную скорость. Также в состав ATM входят оборудованные программы и передающая среда, отвечающие стандартам протокола ATM. ATM представляет собой интегрированный метод сетевого доступа, который многие производители межсетевого оборудования предлагают для реализации в локальных сетях, а региональные телефонные компании – для организации глобальных сетей. При этом достигаются высокие скорости передачи данных, а стоимость предоставляемых услуг зависит от скорости. На основе ATM реализуется масштабируемая магистральная инфраструктура, которая может взаимодействовать с сетями, имеющими разные размеры скорости и методы адресации.

Разработка технологии ATM началась в конце 1960-х годов и велась компанией Bell Labs, в которой инженеры экспериментировали с высокоскоростной коммутацией ячеек, выступающей в качестве альтернативы коммутаций пакетов. Их задачей являлось объединение коммутации с использованием меток (что является основой для построения сетей с коммутацией пакетов), и временное уплотнение, или мультиплексирование с разделением времен» (time-division multiplexing, TDM) (которое также называется множественным доступом с уплотнением каналов – time division multiple access, TDMA).

Как и в некоторых других технологиях глобальных сетей (например, frame relay), в ATM-сетях используются *виртуальные цепи* (virtual circuit), называемые *каналами* (channel). Скорость каналов ATM может составлять 10 Гбит/с, а на момент написания книги уже почти достигнута скорость 40 Гбит/с. Информация передается в виде ячеек, а не в виде пакетов. В отличие от пакетов, *ячейки* (cell) имеют полезную нагрузку фиксированной длины (ячейки ATM будут рассматриваться подробнее в *разд. "Структура ячейки ATM" данной главы).* Пакеты же обычно передают данные переменной длины.

Передача информации по каналам ATM осуществляется при помощи *коммутации ячеек* (cell switching), при которой во всех ячейках в начало каждого временного интервала (окна) TDM помещается короткий признак (или идентификатор виртуального канала). Это позволяет устройствам асинхронно передавать двоичные данные в коммуникационный канал ATM, что делает операции по передаче информации предсказуемыми и постоянными во времени, обеспечивая заранее установленное *качество обслуживания* (Quality of Service, QoS) для трафика, не терпящего задержки в передаче (например, при передаче речи и видео).

Концепция QoS *(см. главу 3)* применима к технологии ATM, в которой QoS представляет собой механизм обеспечения гарантированного уровня пропускной способности сети и использования ресурсов. Применительно к ATM это означает, что на основе некоторых признаков, указываемых в заголовке ATM-ячейки для различных типов передаваемой информации (например, данных или файлов мультимедиа), задается определенный уровень производительности и использования ресурсов. QoS-средства ATM имеют два важных достоинства: во-первых, они гарантируют, что для успешной передачи данных для определенной задачи выделены соответствующие сетевые ресурсы; во-вторых, они уменьшают вероятность того, что ценные сетевые ресурсы будут использоваться недостаточно теми задачами, которым они не требуются и которые укладываются в отведенные лимиты.

Поскольку концепция ATM изначально разрабатывалась параллельно с сетями B-ISDN, технология коммутации ячеек первоначально называлась Asynchronous Time Division Multiplexing (ATOM) (асинхронное мультиплексирование с разделением времени). Несколькими годами позже союз ITU-T выбрал эту технологию в качестве основного транспортного механизма для сетей B-ISDN и переименовал ее в Asynchronous Transfer Mode (ATM).

В самом начале основные концепции ATM определялись сетями B-ISDN, например:

- ATM-ячейка содержит 48-байтную полезную нагрузку и 5-байтный заголовок;
- Физический уровень определяет способ передачи двоичных разрядов по проводу на передающем узле и способ их интерпретации на принимающем узле;
- Уровень ATM управляет мультиплексированием ячеек и различными служебными операциями;
- Адаптационный уровень ATM (AAL) определяет протоколы подуровнем которые используются для организации различного высокоуровневой трафика с помощью 53-байтных ячеек.
- ATM Forum был основной организацией, продвигающей реализации ATM на рынке локальных и глобальных сетей. *ATM Forum* был организован в 1991 году и представляет собой консорциум производителей аппаратных средств поставщиков телекоммуникационных услуг и пользователей, задача которая состояла в совместной с союзом ITU-T разработке спецификаций на глобальные сети ATM, а в настоящее время – и на локальные ATM-сети. Основателями форума являются компании Northern Telecom (Nortel Network Sprint, Sun Microsystems и Digital Equipment Corporation (DEC).

Совет

Вы можете посетить веб-сайт Форума ATM, имеющий адреса **www.atmforum.cdH** или **www.atmforum.org.**

По мере увеличения количества реализованных ATM-сетей продолжался разработка стандартов, способствующих широкому использованию ATM в прикладных службах и внедрению технологий, связанных с передачей видео, мультимедиа и данных. Хотя технология ATM первоначально предназначалась для глобальных сетей, в настоящее время она с успехом применяется и в локальных сетях. Как только ATM превратилась в широко используемую технологию, ее стали поддерживать несколько организаций ATM стандартизации, включая ANSI, IETF, European Telecommunications Standards Institute (ETSI) и ITU-T. Помимо организаций по стандартизации разработке стандартов ATM принимают участие независимые группы производителей, пользователей и промышленных экспертов. Среди них можно отметить следующие организации:

- ATM Forum, который принимал участие в создании таких спецификаций, как открытые и частные сетевые интерфейсы, User-Network Intelface (UNI) (интерфейс "пользователь-сеть"), Data Exchange Interfa (DXI) (интерфейс обмена данными), Broadband-Intercarrier Interfael (BICI) (интерфейс широкополосной связи частных региональных сетей и Multiprotocol over ATM (MPOA) (многопротокольные коммуникации поверх ATM);
- Internet Engineering Task Force (IETF) (Проблемная группа проектирования Интернета), которая занимается проблемами полной совместимости стандартов ATM с транспортом IP (разработала, например, IETF RFC для спецификации Classical IP over ATM);
- Frame Relay Forum, обеспечивающий совместимость функций ATM с сетями frame relay;
- Switched Multimegabit Data Service Special Interest Group (SMDS SIG) (Специальная группа SMDS), работающая над тем, чтобы службы SMDS могли работать поверх сетей ATM.

В настоящее время технология ATM совместима со следующими технологиями:

- B-ISDN;
- DSL;
- FDDI;
- Frame relay;
- Gigabit Ethernet и Gigabit Ethernet;
- SONET и SDH;
- SMDS;
- беспроводные сети.

Характеристики сетей ATM

Сети ATM могут с высокой скоростью передавать информацию различного типа, для чего данные делятся на ячейки равной длины, к которым прикрепляется заголовок, гарантирующий, что каждая ячейка будет доставлена в указанный узел. Формат ATM-ячейки одинаково пригоден для передачи речи, видео и данных.

Поскольку ATM представляет собой технологию с использованием методов коммутации, она легко масштабируется. По мере увеличения трафика или роста сети можно просто добавлять в сеть новые ATM-коммутаторы. В качестве физических каналов ATM можно использовать разнообразные типы кабеля (с соответствующими скоростями передачи для каждого типа), в том числе: кабель на основе неэкранированной витой пары (UTP) Категории 3, 4 и 5; кабель на основе экранированной витой пары (STP); коаксиальный кабель; многомодовый и одномодовый оптоволоконные кабели. Скорость передачи информации в ATM-сети может составлять 1,544 Мбит/с, 2 Мбит/с (для беспроводных сетей), 2,048 Мбит/с, 6,312 Мбит/с, 34,368 Мбит/с, 44,736 Мбит/с, 25,6 Мбит/с, 51,84 Мбит/с, 100 Мбит/с, 155,52 Мбит/с, 622,08 Мбит/с, 1,2 Гбит/с, 2,048 Гбит/с и 10 Гбит/с (почти реализована скорость 40 Гбит/с). Более низкие скорости (менее 622,08 Мбит/с) характерны для локальных ATM-сетей, а более высокие скорости (свыше 622,08 Мбит/с) используются в глобальных сетях. Производители оборудования стремились к этому, ATM-технологии можно использовать для создания международно-глобальных сетей.

Примечание

Кабель Категории 3 обеспечивает минимальную работоспособность ATM-сети на скорости 25,6 Мбит/с и недостаточно надежен для большинства конфигураций.

Многоуровневые коммуникации ATMI

Архитектура ATM, называемая эталонной моделью протокола ATM (ATM Protocol Reference Model), имеет четыре уровня, которые позволяют множеству устройств одновременно работать в пределах единой сети. Технологию ATM отличает от других методов транспортировки данных то, как ее функции реализованы на коммуникационном уровне, соответствующем MAC-подуровне Канального уровня модели OSI. Тот уровень ATM, который соответствует MAC-подуровню, работает независимо от более высоких уровней, благодаря чему он свободен от задач маршрутизации, связанных с сетевым уровней (поскольку все операции по маршрутизации переданы верхним уровням. В ATM-ячейку можно поместить данные практически любого протокола высокого уровня. Четыре уровня ATM представлены в табл. 8.1. Два из этих уровней (Уровень ATM и Адаптационный уровень ATM, AAL) представляет собой уровни, которые реализуют функции, специфичные для ATM.

Таблица 8.1. *Уровни ATM*

Уровень	Функция
Физический уровень ATM (ATM Physical layer) (содержит два подуровня: Transmission Convergence, TC, и Physical Medium Dependent, PMD)	Преобразует ячейки в двоичные разряды, пере даваемые по физическому носителю, а также содержит электрический и физический интерфейсы для ATM (приблизительно эквивалентен Физическому уровню модели OSI)
Уровень ATM (ATM layer)	Создает ATM-ячейки, управляет маршрутизацией и обнаружением ошибок (приблизительно эквивалентен Канальному уровню модели OSI)
Адаптационный уровень ATM (ATM Adaptation layer, AAL) (содержит два подуровня: Convergence и Segmentation and Reassembly, SAR)	Сегментирует данные, подготавливая процесс создания ATM-ячеек, и управляет обменом ин формацией (т. е. передачей и приемом) с более высокими уровнями (приблизительно эквивалентен Канальному уровню модели OSI)
Уровень служб и приложений ATM (ATM Services and Application layer)	Устанавливает связь между узлом, передающим данные, и Адаптационным уровнем ATM согласно запросам различных уровней обслуживания (нет эквивалентов в эталонной модели OSI)

Физический уровень ATM

физический уровень ATM (ATM Physical layer) преобразует поток ячеек в передаваемые двоичные разряды и управляет работой физического носителя (кабеля). На этом уровне определены параметры электрического и физического интерфейсов, скорости передачи в линии, а также функции управления передачей. Важнейшей задачей рабочей группы ATM были вопросы стандартизации ATM для самых различных типов кабелей.

Физический уровень делится на два подуровня: *Transmission Convergence (TC) sublayer* (Конвергентный подуровень передачи данных[1]) и *Physical Medium Dependent (PDM) sublayer* (Подуровень, зависящий от физической среды передачи данных). Эти подуровни служат для того, чтобы отделить специфические ATM-коммуникации от физического интерфейса, который определяет возможность передачи ATM-ячеек через различные интерфейсы и коммуникационные среды. TC-подуровень выполняет две функции. Во-первых, на принимающем узле он обрабатывает ячейки, поступающие в виде потока двоичных данных от PDM-подуровня. Во-вторых, TC-подуровень управляет изменениями скорости передачи данных через физический интерфейс и Уровень ATM, для чего в поток двоичных данных вставляются пустые ячейки. Это может понадобиться потому, что Уровень ATM в коммутаторе может обрабатывать ячейки быстрее, чем требуется для обеспечения допустимой скорости передачи канала.

PDM-подуровень отвечает за адаптацию коммуникаций к передающей среде и связанным с ней скоростям различных интерфейсов. Физический ATM-интерфейс обеспечивает передачу данных в

виде электрических или оптических сигналов. Поскольку поначалу технология ATM рассматривалась как средство построения глобальных сетей, первые ATM-сети работали по оптоволоконному кабелю с использованием SONET. В настоящее время ATM-сети реализованы для различных транспортных методов и передающих сред, в числе которых можно назвать следующие:

- FDDI со скоростью 100 Мбит/с;
- Fibre Channel со скоростью 155,52 Мбит/с;
- SONET OC-3 со скоростью 155,52 Мбит/с;
- SONET OC-12 со скоростью 622,08 Мбит/с;
- Optical (Gigabit) Ethernet со скоростью 1,2 Гбит/с;
- Optical (10 Gigabit) Ethernet со скоростью 10 Гбит/с;
- DS-1 со скоростью 1,544 Мбит/с;

Его можно было бы также назвать "подуровнем согласования параметров передачи данных". – *Прим. пер.*

- DS-3 со скоростью 44,736 Мбит/с;
- E-1 со скоростью 2,048 Мбит/с;
- E-3 со скоростью 34,368 Мбит/с;
- Universal Mobile Telecommunication Systems (беспроводные сети) со скоростью 2 Мбит/с (для протокола IP).

Уровень ATM

Уровень ATM (ATM layer) отвечает за создание ATM-ячеек. Он определив структуру ячеек, их маршрут и методы обнаружения ошибок, а также обеспечивает качество обслуживания (QoS) для некоторой виртуальной сети или канала. Функции этого уровня выполняются многими устройствам ATM-сети. Существуют две основных разновидности ATM-оборудован ATM-коммутатор и подключенное устройство ATM. *ATM-коммутатор* (ATM switch) попросту передает по сети ATM-трафик, а также обеспечивая качество обслуживания (QoS) для каждого виртуального канала. QoS-марка в заголовке ячейки позволяет ATM-сети идентифицировать тип трафика Для каждого типа трафика имеются свои допустимые параметры, определяющие время задержки, точность и пропускную способность, а QoS-Маркер определяет уровень качества обслуживания (QoS), необходимый для того типа данных, которые содержатся в ячейке. Например, при передаче мультимедийных потоков информации допускаются меньшие задержки, чем при пересылке двоичных данных, а передача данных требует более высокой точности. Если для передачи данных определенного типа нельзя обеспечить качество обслуживания (QoS), запрос на получение доступа к некоторому *виртуальному каналу ATM* (ATM virtual circuit) отклоняется. Примеры режимов использования службы QoS перечислены в табл. 8.2. *Подключенное устройство* ATM/(ATM attached device) преобразует поток данных в поток ATM ячеек, передаваемых по ATM-сети, а также выполняет обратное преобразование. Подключенные устройства ATM представляют собой рабочие станции или серверы, имеющие ATM-интерфейс.

Таблица 8.2. *Режимы использования службы QoS в ATM-сети*

Режим использования службы	**Задержка**	**Точность**	**Производите-льность**
Передача файлов	Допускаются большие задержки	Точность важна, при потере ячейки требуется повторная передача, что снижает пропускную способность сети	Данные передаются пакетами ("взрывообразный" трафик), между которыми имеются периоды ожидания (паузы)
Интерактивный торговый терминал	Допускаются маленькие задержки (интервалы между посылками должны составлять 100 мс и	Потери ячеек не допускаются	Низкая скорость передачи, отсутствуют всплески трафика, низкая нагрузка на сеть

Режим использования службы	Задержка	Точность	Производите-льность
	меньше)		
Интерактивное неподвижное изображение	Допускаются маленькие задержки (интервалы между посылками должны составлять 100 мс и меньше)	Точность важна, при потере ячейки требуется повторная передача, что снижает пропускную способность сети	Средняя скорость передачи и большие периоды ожидания
Видео в реальном масштабе времени	Допускаются очень маленькие задержки	Потери ячеек не до пускаются	Постоянная скорость передачи, всплески трафика и периоды ожидания
Передача речи	Допускаются средние задержки	Допускаются большие потери ячеек (до 1%) только после ухудшение качества становится заметным	Короткие всплески трафика периодами этого ожидания предсказуемой длительности

Некоторые реализации службы QoS в ATM-сети (например, для передачи мультимедиа) требуют, чтобы Уровень ATM задавал уровень обслуживания в процессе согласования условий передачи между передающим узлом и ATM-коммутатором. Служба управления подключением к сети устанавливает согласованную скорость передачи и пропускную способность виртуального канала.

Основная задача ATM-коммутаторов – обеспечить передачу ячеек в заданный принимающий узел, сохранив их очередность. Если обнаруживается потеря некоторой ячейки, передающему узлу посылается запрос на повторную передачу. Когда некоторая ячейка поступает во входной интерфейс ATM-коммутатора, Уровень ATM добавляет в нее *идентификатор виртуального пути/идентификатор виртуального канала* (virtual path identifier/virtual channel identifier (VPI/VCI)). Эти идентификаторы позволяют ячейке выбрать нужный выходной интерфейс, они действуют только локально (т. е. могут анализироваться и интерпретироваться только тем коммутатором, которому они предназначаются), и одни и те же идентификаторы VPI/VCI могут повторно назначаться в каждом ATM-коммутаторе. После того как определен нужный выходной интерфейс, ячейка передается Физическому уровню ATM для передачи в следующий канал. ATM-коммутаторы могут также использоваться для установки флагов перегрузки сети, а также для буферизации и временного хранения ячеек в тех случаях, когда возникает перегруженность сети или имеются конфликты при выборе порта коммутатора.

Адаптационный уровень ATM (AAL)

Адаптационный уровень ATM (ATM Adaptation layer, AAL) в первую очередь отвечает за сегментацию и сборку/разборку данных при создании/анализе ATM-ячеек, а также назначает соответствующий уровень QoS трафику различного типа (например, в процессе передачи речи, видео и двоичных данных). Кроме того, этот уровень обеспечивает четыре класса (типа) обслуживания, что отражено в табл. 8.3.

Таблица 8.3. *Классы обслуживания для Адаптационного уровня*

Класс обслуживания AAL (тип AAL)	Описание
AAL Type 1	Изохронная (равномерная во времени) служба с постоянной скоростью передачи (CBR) для приложений с установлением соединения (connection-oriented),

Класс обслуживания AAL (тип AAL)	Описание
	предназначенных для пересылки речи и видео; обычно используется коммуникационными службами T-1 (обратите внимание на то, что линия DS-1 определяет уровень передачи цифрового сигнала)
AAL Type 2	Изохронная служба с переменной скоростью передачи (VBR) для приложений с установлением соединения (например, для передачи сжатого видео, что включает в себя пакетную передачу речи и непосредственно видеосигналов)
AAL Type 3/4	Служба с переменной скоростью передачи для пакетной передачи данных локальных сетей, одновременно реализует коммуникации как с установлением, так и без установления соединения (connectionless) (изначально предназначалась для совместимости со службой SMDS)
AAL Type 5	Пониженный вариант класса AAL Type 3/4, определяющий службу с переменной скоростью передачи, которая обеспечивает передачу двоичных данных (как с установлением, так и без установления соединения) и совместима с ATM-коммутацией, передачей IP-пакетов, сетями X.25 и frame relay

Адаптационный уровень ATM делится на два подуровня: *Convergence sublayer* (конвергентный подуровень) и *Segmentation and Reassembly (SAR) sublayer* (подуровень сегментации и сборки). Каждый из этих подуровней решает; свои задачи. Сначала конвергентный подуровень получает пакеты от более высоких уровней, назначает класс обслуживания для информации различного типа (речь, видео или двоичные данные) и создает модули данных протокола (PDU), передаваемые SAR-подуровню. SAR-подуровень, в свою очередь, преобразует PDU-модули в 48-байтную полезную нагрузку ячеек и пересылает ячейки Уровню ATM. На принимающем узле информация преобразовывается из ячеек в пакеты, которые затем обрабатываются более высокими уровнями принимающего узла.

Именно на Адаптационном уровне реализованы все специфические особенности технологии ATM и именно на этом уровне функционирует QoS-служба ATM-сети, а также обеспечивается надежность ATM-коммуникаций.

Уровень служб и приложений ATM

Уровень служб и приложений ATM (ATM Services and Application layer) определяет класс обслуживания, необходимый для передачи информации, и устанавливает связь между узлом, генерирующим поток данных, и Адаптационным уровнем ATM. Классы обслуживания ATM-сетей зависят от потребностей приложений, при этом используются следующие критерии: способ передачи потока данных, необходимая полоса пропускания и объем передаваемой информации. Определены четыре класса обслуживания, каждый из которых связан с некоторым типом службы Адаптационного уровня (табл. 8.4).

Таблица 8.4. *Классы обслуживания для Уровня служб и приложений ATM*

	Служба Класса A	**Служба Класса B**	**Служба Класса C**	**Служба Класса D**
Тип службы	Передача речи и видео в реальном масштабе времени	Пакетное видео	Локальный ATM-трафик	SMDS-трафик
Тактирование	Постоянно е	Постоянное	Отсутствует	Отсутствует
Скорость передачи	CBR	VBR	VBR	UBR и ABR
Тип коммуникаций	С установлением соединения	С установлением соединения	С установлением и без	С установлением и без

	Служба Класса A	Служба Класса B	Служба Класса C	Служба Класса D
			установления соединения	установления соединения
Связь с типом AAL	Type1	Type 2	Type 3/4 или 5	Type 3/4 или 5

Классы обслуживания можно также рассматривать по типу передачи данных

- служба с постоянной скоростью передачи (constant bit-rate, CBR) – виртуальный коммуникационный канал с фиксированной полосой проникания, названный службой Класса A;
- служба с переменной скоростью передачи (variable bit-rate, VBR) – виртуальный канал с изменяющейся полосой пропускания, делится на 4 класса: аббревиатура VBR-RT обозначает службу реального времени Класса B, а для службы Класса C, не работающей в реальном времени используется обозначение VBR-NRT;
- служба с неуказанной скоростью передачи (unspecified bit-rate, UBR) виртуальный канал, использующий имеющуюся полосу пропусканий не гарантирующий доставку данных в течение некоторого времени также не обеспечивающий отсутствие потерь данных; называется службой Класса D;
- служба с доступной скоростью передачи (available bit-rate, ABR) – также виртуальный канал, как и UBR-канал, за исключением того, что гарантирует целостность данных; называется службой Класса D.

Структура ячейки ATM

ATM-ячейка очень проста по сравнению со структурами других MOflyjaB данных. Структура ячейки определяется Уровнем ATM, длина ячейка равна 53 байтам. Каждая ячейка имеет 5-байтный заголовок для хранения служебной информации и 48 байтов полезной нагрузки (данных).

Размер ATM-ячейки (рис. 8.1), равный 53 байтам, выбран не сразу, поскольку интересы основных участников Форума ATM различались и предъявляли разные требования к спецификациям. Например, для задач передачи больше подходила ячейка длиной 37 байт, которая соответствовала стандартной 37-байтной ячейке для передачи голоса. Длина в 53 байта была выбрана как компромисс, позволяющий пересылать речь, а также видео данные.

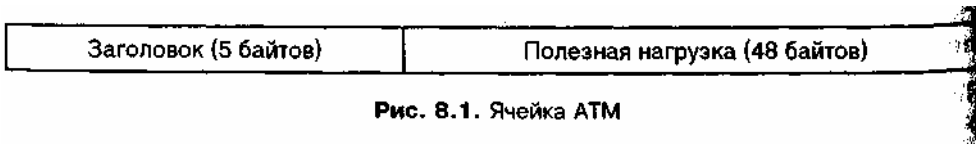


Рис. 8.1. Ячейка ATM

Основная функция заголовка ATM-ячейки (рис. 8.2) – снабдить каждую ячейку информацией о канале и пути. ATM-коммутатор, получив ячейки определяет, по какому виртуальному соединению эта ячейка должна передаваться. Заголовок ячейки содержит следующие поля:

- *Базовое управление передачей* (Generic Flow Control, GFC) – только для функций локального управления; значение этого поля не передается между конечными узлами;
- *Идентификатор виртуального пути* (Virtual Path Identifier, VPI) – содержит первую часть адреса ATM-маршрутизации, определяющую виртуальный путь между пользователями или между пользователем и ATM-сетью;
- *Идентификатор виртуального канала* (Virtual Channel Identifier, VCI) – содержит вторую часть адреса ATM-маршрутизации, определяющую виртуальный канал между пользователями или между пользователем и ATM-сетью;
- *Признак типа полезной нагрузки* (Payload Type Indicator, PTI) – определяет тип данных в поле полезной нагрузки, а также может содержать пользовательскую, сетевую или управляющую информацию;
- *Приоритет потери ячейки* (Cell Loss Priority, CLP) – это поле определяет, может ли ячейка быть выброшена или нет (значение, равное нулю, указывает на то, что ячейка имеет высший

приоритет и не может быть удалена);

- *Управление ошибками заголовка* (Header Error Control, HEC) – используется для обнаружения ошибок и исправления однобитных ошибок.

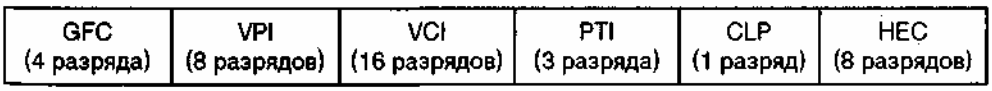


Рис. 8.2. Заголовок ATM-ячейки

Принципы работы сетей ATM

Коммутируемой называется такая сеть, в которой передающий узел находит некоторый путь к принимающему узлу для каждого сеанса передачи данных. При этом во внимание принимаются несколько параметров, в том числе доступность каналов, скорость линии, стоимость канала и надежность доставки. В зависимости от типа передаваемой информации, два устройства могут в разных сеансах связи использовать различные пути. Например, если после речевых коммуникаций осуществляется передача мультимедиа, то для каждого типа коммуникаций требуются разные характеристики времени Доставки и надежности.

Примечание

Процедура определения пути связана с типом используемого канала. В случай коммутируемого виртуального канала путь выбирается при создании канала, по окончании сеанса для следующего сеанса может быть определен другом путь. Для постоянного виртуального канала путь не меняется от одного сеанса связи к другому (виртуальные каналы ATM рассматриваются в следующей разделе).

ATM-коммутатор получает входящую ячейку и намечает для нее маршрут я указанному интерфейсу ATM-коммутатора, чтобы эта ячейка смогла достичь пункта назначения. В зависимости от архитектуры сети, ячейка может пересекать один или несколько ATM-коммутаторов перед тем, как она достигнет последнего коммутатора на своем пути и будет преобразована в пакет, который будет получен принимающим узлом. Пунктом назначения ячейки может быть другой коммутатор или – в случае групповых пересылок – несколько коммутаторов. Эта информация извлекается из заголовка ячейки В тех сетях, в которых имеется множество путей, необходимо применять специальные протоколы ATM-маршрутизации, например, *Private Network-to-Network Interface (PNNI)* (частный межсетевой интерфейс). С помощью этих протоколов коммутаторы обмениваются таблицами соединений. Эти таблицы содержат сведения о различных путях, что позволяет каждому коммутатор выбирать наиболее подходящий путь для каждого сеанса связи.

Виртуальные каналы ATM

В ATM-сетях для создания информационных магистралей между передающим и принимающим узлами используются виртуальные каналы (виртуальные цепи). Виртуальный канал представляет собой некую магистраль между двумя узлами коммутируемой сети, которая выглядит как выделенное двух точечное соединение и "прозрачна" для пользователя. В ATM-сетях существуют три типа виртуальных каналов: постоянные, коммутируемые и интеллектуальные постоянные виртуальные каналы.

Постоянный виртуальный канал (PVC)

Постоянный виртуальный канал ATM (ATM permanent virtual circuit, PVC представляет собой выделенную цепь с заранее определенным путем, которая может иметь фиксированную полосу пропускания между двумя конечными точками. Канал этого типа всегда работоспособен и активен с момент та своего создания, что исключает задержки, вызванные установлением. И разрывом канала. Примером постоянного виртуального канала может служить связь между двумя ATM-совместимыми коммутаторами в сети со *сме*шанной (свободной) коммутацией. Такой канал должен всегда быть активны для каждого коммутатора, т. к. это упрощает коммуникации и обновление информации о маршрутизации, которой обмениваются маршрутизаторы. Постоянные виртуальные каналы вручную устанавливаются поставщиком услуг или сетевым администратором. Если вы получаете PVC-канал от поставщика услуг, то вам нужно сообщить адрес пункта назначения, среднюю полосу пропускания или согласованную скорость передачи

информации (committed information rate, CIR), а также расписание работы канала (когда вы запрашиваете PVC-канал в частной сети, администратору локальной сети известны эти параметры). При этом вы сможете оплачивать услуги ежемесячно. Поставщик PVC-канала или сетевой администратор могут создать канал с помощью удаленного терминала, задавая полосу пропускания канала и выполняя любые другие настройки по его конфигурированию. Одним из недостатков PVC-каналов является то, что их нужно создавать и конфигурировать вручную.

Коммутируемый виртуальный канал (SVC)

Коммутируемый виртуальный канал ATM (ATM switched virtual circuit, SVC) создается и разрывается по мере необходимости. Он представляет собой временное соединение, которое создается по запросу от средств передачи информации и которое активно только в течение того времени, пока устройства обмениваются данными. По завершении коммуникаций канал разрывается, и все его ресурсы возвращаются в пул ресурсов. SVC-канал динамически создается служебными программными средствами с учетом параметров, задаваемых оконечными устройствами, коммуникационным оборудованием и средствами ATM-сети, при этом ручное вмешательство не требуется. Процесс создания SVC-каналов выглядит так:

1. ATM-коммутатор получает от передающего устройства запрос на соединение. Коммутатор проверяет, какую полосу пропускания запросило это устройство, и если требуемая полоса пропускания недоступна, то запрос отвергается. Если полоса пропускания не указана, коммутатор выделяет такую полосу, которая задана по умолчанию.
2. Запрос на соединение пересылается принимающему устройству, и как только это устройство обнаружено, коммутатор(ы) передает(ют) обратно идентификатор виртуального пути (VPI), который указывает, к какому виртуальному каналу необходимо подключить передающее устройство.
3. После того как передающее устройство получит идентификатор виртуального пути, коммутатор заканчивает операцию, назначая некоторый идентификатор виртуального канала (VCI).

Преимущество SVC-каналов состоит в том, что они незаметны для пользователя с точки зрения операций по их созданию и удалению. Эти каналы не требуют ручного конфигурирования, поэтому не создают работы для сетевого администратора. Недостатком каналов этого типа являются задержки, вызванные операциями установления и разрыва канала (хотя, если сеть разработана правильно, эти задержки незаметны для пользователей).

Интеллектуальный постоянный виртуальный канал (SPVC)

Интеллектуальный постоянный виртуальный канал ATM (ATM smart permanent virtual circuit, SPVC) объединяет в себе свойства постоянного и коммутируемого виртуального канала. Такой канал, как и PVC-канал, требует ручного конфигурирования (хотя только на оконечных устройствах). Как и SVC-канале, для каждого сеанса связи с использованием SPVC-канала указывается индивидуальный путь к коммутатору или к тем коммутаторам, через которые данные должны передаваться. Кроме того, как и для PVC каналов, операции создания и удаления SPVC-канала не вызывают задержек, поскольку этот канал сконфигурирован заранее. Подобно SVC-каналам, SPVC-канал отказоустойчив благодаря наличию альтернативных маршрутов. Еще одним достоинством SPVC-канала является то, что он обеспечивает заданную полосу пропускания. Однако, как и в случае PVC-каналом эта полоса пропускания используется не полностью в моменты отсутствия коммуникаций или при низкой нагрузке на сеть. Недостаток SPVC-Канала состоит в том, что для их создания требуется время, а сетевому администратору нужно учиться их использовать.

Характеристики ATM-коммуникаций

ATM представляет собой технологию, предусматривающую создание логических соединений, поскольку ATM-ячейки "привязаны" к конкретному виртуальному каналу и могут передаваться только по нему. Такая особенности делает технологию ATM более эффективной, чем сети Ethernet и ToRing, в которых все подключенные устройства могут видеть весь сетевой трафик.

Виртуальные каналы (виртуальные цепи, virtual circuit) определяют логические каналы, по которым осуществляются ATM-коммуникации. Эти каналы образуются двумя компонентами:

- *виртуальными каналами* (virtual channel, VC), которые являются логическими соединениями между

устройствами;

- *виртуальными путями* (virtual path, VP), каждый из которых представляет собой некоторый набор виртуальных каналов.

Заголовок ATM-ячейки содержит идентификатор виртуального пути (VPI) который является той частью адреса маршрутизации, которая идентифицирует линию связи, организованную с помощью некоторого виртуального пути. Этот идентификатор можно рассматривать как эквивалент порта (например на коммутаторе) или интерфейса, связанного с некоторой подсетью. Идентификатор виртуального канала (VCI), также присутствующий в заголовке ATM-ячейки, определяет виртуальный канал внутри виртуального пути. Каналы внутри некоторого пути, определенного идентификатором виртуального пути (VPI), представляют собой отдельные составляющие всего виртуального пути. Соединения с использованием виртуальных каналов ATM осуществляются подобно тому, как по коммуникационному коробу в здании проходит множество отдельных электрических или телефонных проводов.

Достоинство архитектуры ATM-сетей состоит в том, что ячейки, поступающие во входящий порт ATM-коммутатора, легко можно направить на нужный исходящий порт. Для соединений, которые группируются в некотором общем виртуальном пути, требуется лишь один набор административных служб (т. е. для каждого соединения не нужны отдельные службы). Кроме того, легко создавать новые виртуальные каналы, поскольку начальная конфигурация пути уже определена. Еще одно преимущество заключается в том, что если какой-нибудь путь становится недоступным (из-за перегрузки или отказа сети), все каналы, проходящие по этому пути, автоматически перестраиваются и проблема устраняется.

Вопросы проектирования сетей ATM

На конфигурацию ATM-сети влияют следующие факторы:

- компоненты ATM;
- ATM-коммутаторы;
- характеристики и типы ATM-коммутаторов;
- типы ATM-интерфейсов.

В последующих разделах будет рассматриваться каждый из перечисленных факторов.

Компоненты сетей ATM

Службы ATM-сети реализуются с помощью адаптеров (или сетевых плат) ATM, установленных в устройства, взаимодействующие по сети, а также ATM-коммутаторов. Эти устройства (рис. 8.3) функционируют на самых нижних трех уровнях эталонной модели ATM.

Интерфейс "пользователь-сеть" (User-Network Interface, UNI) и Межсетевой интерфейс (Network Node Interface, NNI) ATM-сетей рассматриваются в этой главе далее.

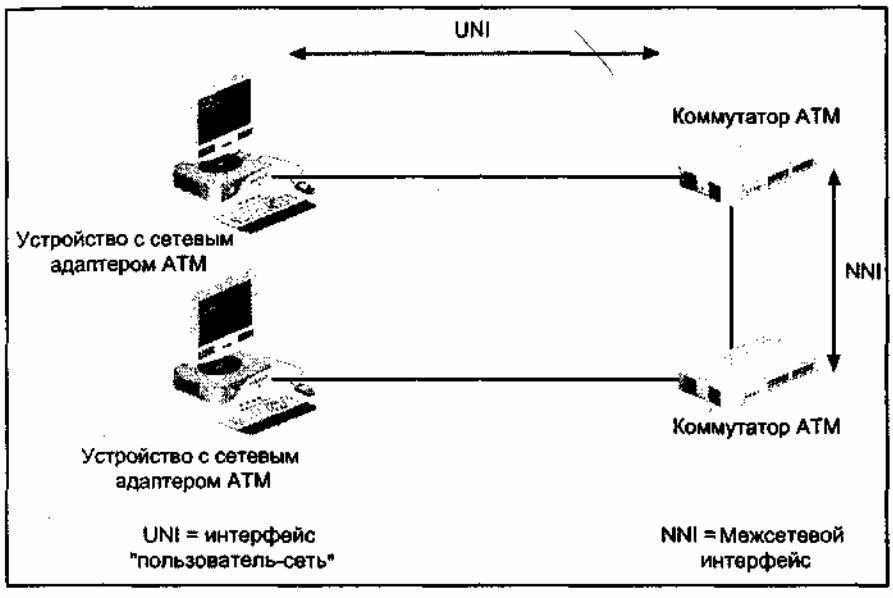


Рис. 8.3. Соединение с использованием сетевых адаптеров ATM

АТМ-коммутаторы

АТМ-коммутатор осуществляет соединение между двумя оконечными устройствами. По сути, он передает АТМ-ячейки от передающего узла к принимающему. Соединение между двумя АТМ-коммутаторами используется совместно в пределах возможностей одной коммуникационной среды, которая делится на множество виртуальных каналов, пересылающих ячейки (рис. 8.4). В отличие от локальных сетей с общей передающей средой, конечные узлы АТМ-сети не используют полосу пропускания совместно, поскольку каждый из них имеет выделенную полосу пропускания и выделенную линию связи – виртуальный канал. Наличие выделенной линии связи делает возможным осуществление одновременных коммуникаций без перегрузки сети (их число ограничено лишь количеством портов коммутатора);

Использование идентификаторов VPI/VCI упрощает процесс коммутации что делает АТМ-коммутаторы очень эффективными. Когда входящая ячейка поступает на интерфейс коммутатора, анализируется адресная информации о маршрутизации и ячейка направляется в соответствующий исходящий интерфейс. АТМ-коммутатор, начиная процесс коммутации, не ждет, пока ячейка будет обработана целиком. Это значительно ускоряет процесс передачи ячейки. Коммутатор считывает целевой адрес ячейки и перенаправляет ее в соответствующий исходящий интерфейс. Кроме того, он выполняя лишь некоторые операции по обнаружению ошибок, в силу чего не возникают задержки, которые могли бы появиться при наличии сложного механизма поиска ошибок. АТМ-сети подобны сетям frame relay в том смысле, что большинство функций по обнаружению ошибок переданы протоколу, передаваемому по АТМ-сети (например, протоколу IP).

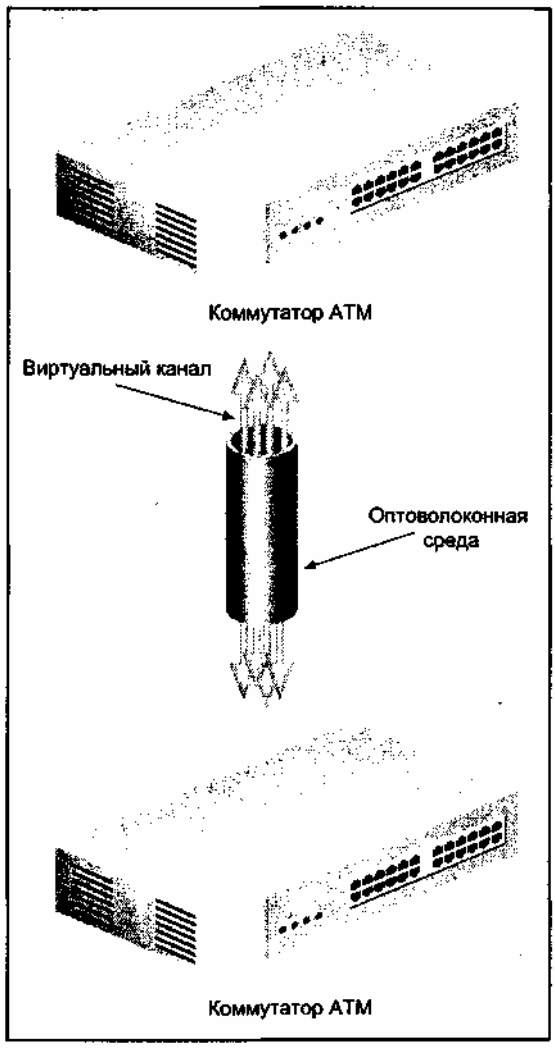


Рис. 8.4. Виртуальные каналы по общей коммуникационной среде

В практическом задании 8-1 вы узнаете больше о коммутаторах и других устройствах АТМ, которые можно приобрести у определенного производителя.

Характеристики и типы АТМ-коммутаторов

При проектировании и реализации АТМ-сети очень важно выбрать такой АТМ-коммутатор, который позволит оптимизировать производительность масштабируемость сети. В первую очередь нужно учесть количество и размер буферов ячеек, имеющихся в коммутаторе. Буферы используются для временного хранения ячеек при их передаче через коммутатор, особенно в тех случаях, когда имеется большой трафик. Коммутатор должен хранить обрабатывать ячейки с максимальной скоростью и эффективностью. Если количество буферов недостаточно или буферы имеют небольшой размер, то коммутатор будет терять ячейки при возникновении большого трафика.

Примечание

Большое количество отброшенных ячеек приведет к значительному числу повторных передач, в результате чего снизится производительность сети

Другим фактором при выборе коммутатора являются конфликты при выборе портов и возможности управления параметрами портов. Во многих случая несколько входящих коммуникационных потоков могут затребовать один тот же исходящий интерфейс. Для портов с большим количеством конфликтов коммутатор должен иметь возможность определения различных приоритетов при выборе порта. Если некоторый порт не успевает, обрабатывая ячейки и создает чрезмерные задержки, приложения с высокими требованиями ко времени доставки (например, передача речи или видео в реальней масштабе времени) будут работать плохо из-за больших потерь информации.

Если развертывается АТМ-сеть на базе коммутаторов, новая архитектура должна быть совместимой с уже существующими сетевыми устройствами приложениями. Например, в силу конструктивных особенностей сеть работает так, что все подключенные узлы принимают информации отправленную любым сетевым устройством. Для использования глобальной или локальной АТМ-сети совместно с Ethernet-сетью необходимо обеспечить их совместимость, для чего существует такая технология, как *эмуляция локальной сети* (LAN Emulation, LANE). С помощью LANE реализуется сеть с групповым вещанием (multicast), позволяющая заданным группам узла принимать информацию, предназначенную для них. Для этого выполняются групповые посылки по определенной группе виртуальных каналов, направленных к оконечным сетевым устройствам. С помощью сервера группового вещания создается большая однородная сеть, образованная множеством устройств с общим коммуникационным каналом.

Еще одним соображением при развертывании АТМ-сети является управление соединениями, для чего имеются программные средства двух типов распределенные и централизованные. Распределенные средства управлений соединениями располагаются на АТМ-коммутаторах, они имеют возможность обновления программ и добавления административных функций по мере роста сети. Распределенное управление соединениями может оказаться сложным в сетях, содержащих сотни коммутаторов, каждый из которых нуждается в индивидуальном конфигурировании и обновлении с участием сетевого администратора. При централизованном управлении соединениями программное обеспечение располагается на некотором центральном устройстве (например, на сервере). Достоинства такого решения заключаются в уменьшении затрат на администрирование (в расчете на отдельный коммутатор), а также в том, что все управление осуществляется из одного места (включая обновление и расширение программных средств). Недостаток такого метода управления состоит в том, что центральный сервер является единственной точкой отказа, т. е. при выходе сервера из строя становится невозможном управление соединениями во всей сети.

Ниже перечислены дополнительные критерии, влияющие на выбор коммутаторов для АТМ-сети:

- время задержки, представляющее собой время, необходимое коммутатору на обработку и пересылку ячейки;
- типы физических интерфейсов и их максимальное количество, поддерживаемое коммутатором;
- типы межсетевых интерфейсов, поддерживаемых коммутатором;
- типы (классы обслуживания) AAL, поддерживаемые программными средствами управления соединениями;
- приоритеты QoS, поддерживаемые программными средствами управления соединениями;
- наличие поддержки PVC-, SVC- и SPVC-каналов;
- наличие функций управления трафиком и перегрузкой сети;
- поддержка виртуальных локальных сетей (VLAN) рассматриваются в этой главе позже;
- возможности по обеспечению отказоустойчивости. Существуют три основных типа АТМ-

коммутаторов:

- ATM-коммутаторы для локальных сетей, предназначенные для создания локальных соединений с оконечными узлами, оборудованными ATM-адаптерами;
- ATM-модули для существующих многопротокольных сетевых концентраторов, устанавливаемые в имеющиеся стойки, которые обеспечивают подключение как к ATM-сети, так и к обычным сетям Ethernet и Token Ring (ATM-модуль представляет собой плату, вставляемую в слот объединительной платы; он образует одно соединение между концентратором и ATM-коммутатором);
- многопротокольные концентраторы, имеющие как ATM-коммутатор, так и коммутатор Ethernet или Token Ring (обычно такие устройства имели несколько ATM-портов для подключения оконечных ATM-узлов или других ATM-коммутаторов).

Типы ATM-интерфейсов

Форум ATM предложил типы стандартного интерфейса для подключения конечных узлов и ATM-коммутаторов к открытым и частным сетям. Благодаря разработке этих стандартов, упростились соединения между устройствами и сетями различных типов, в результате чего все служебные и вспомогательные функции стали глобально совместимыми. В настоящее время применяются интерфейсы двух типов: Интерфейс "пользователь-сеть" (\Jiim Network Interface, UNI) и Межсетевой интерфейс (Network Node Interface NNI). UNI-интерфейс предназначен для создания соединения между оконным узлом и коммутатором. Он может также использоваться для связи пользовательской станции, многопротокольного концентратора или маршрутизатора с ATM-коммутатором.

UNI-интерфейсы бывают частными (private) и общедоступными Частным называется интерфейс между оконечным устройством и коммутатором частной сети, чаще всего он встречается в небольших и средних локальных сетях. Общедоступным называется UNI-интерфейс между конечным устройством и коммутируемой сетью общего пользования, применяется в глобальных сетях. Этот интерфейс может также применяться для создания соединения между коммутатором частной сети и коммутируемой сетью общего пользования. Общедоступный UNI-интерфейс называется элементом "административной границы", т. е. к нему предъявляются более строгие требования, чем к устройствам локальных сетей, и он обычно является частью услуг и оборудования, которые предоставляются провайдером сети общего пользования.
NNI-интерфейс предназначен для связи двух ATM-коммутаторов. Эти коммутаторы могут располагаться в частной или общедоступной сети, а могут соединять частную сеть с сетью общего пользования. Подобно UfH интерфейсам, NNI-интерфейсы могут быть частными и общедоступными. Частным называется NNI-интерфейс между двумя коммутаторами в частной сети, а общедоступный NNI-интерфейс – это интерфейс между коммутирующими устройствами ATM-сети общего пользования, он является элементом глобальной ATM-сети. В США существуют два базовых типа подключений с использованием общедоступных NNI-интерфейсов:

- NNI-интерфейсы между ATM-коммутаторами в некоторой локальной области доступа и связи (local access and transport area, LATA; см. *главу 10*
- NNI-интерфейсы между местными телефонными компаниями и компаниями дальней связи, называемые Broadband Intercarrier Interfaces (BICI) (Интерфейс широкополосной связи частных региональных сетей).

В предложениях Форума ATM указывается на то, что ATM-коммутаторы должны автоматически определять тип интерфейса (UNI или NNI) и конфигурировать параметры так, чтобы они соответствовали интерфейсу. Также Форум ATM предложил, чтобы ATM-сети на базе оборудования от разных производителей создавались в соответствии со спецификацией частного межсетевого интерфейса (Private Network-to-Network Interface, PNNI). PNNI-интерфейс определяет некий протокол, позволяющий сетевым администраторам проектировать и реализовывать сети с использованием коммутируемых виртуальных каналов (SVC) между двумя любыми PNNI-совместимыми ATM-устройствами. Совместимость с PNNI-интерфейсом позволяет устройству находить пути в сети, не имея информации о топологии всей сети. Это возможно благодаря тому, что вся сеть делится на равноправные группы. В каждой такой группе имеется один коммутатор (с наименьшим адресом), выступающий в роли лидера группы, который собирает сведения о сети и коммуникациях с лидерами других групп. В крупных сетях лидеры групп делятся на группы более высокого порядка, что позволяет эффективнее организовать коммуникации между группами.

Области применения ATM

Технология ATM, как метод передачи данных в сети, имеет множество средств и возможностей, которые позволяют ей отвечать специфическим требованиям корпоративных сетей. На рис. 8.5 приведен пример ATM-сети, который иллюстрирует использование данной технологии для реализации следующих задач:

- организация магистрали локальной сети;
- построение локальных сетей;
- организация высокоскоростного доступа к серверам локальной сети;
- подключение настольных систем;
- построение глобальных сетей.

Каждая из перечисленных областей применения технологии ATM рассматривается в следующих разделах.

ATM-сеть как магистраль локальной сети

Чаще всего технология ATM применяется в локальных сетях для организации магистральной (опорной) сети, а локальные сети чаще всего реализуются в пределах некоторой территории (кампуса), где расстояния между узлами сети могут быть достаточно большими. При правильном подходе использование ATM-сети в качестве магистрали может упростить управление сетью, поскольку в этом случае межсетевая среда будет более простой.

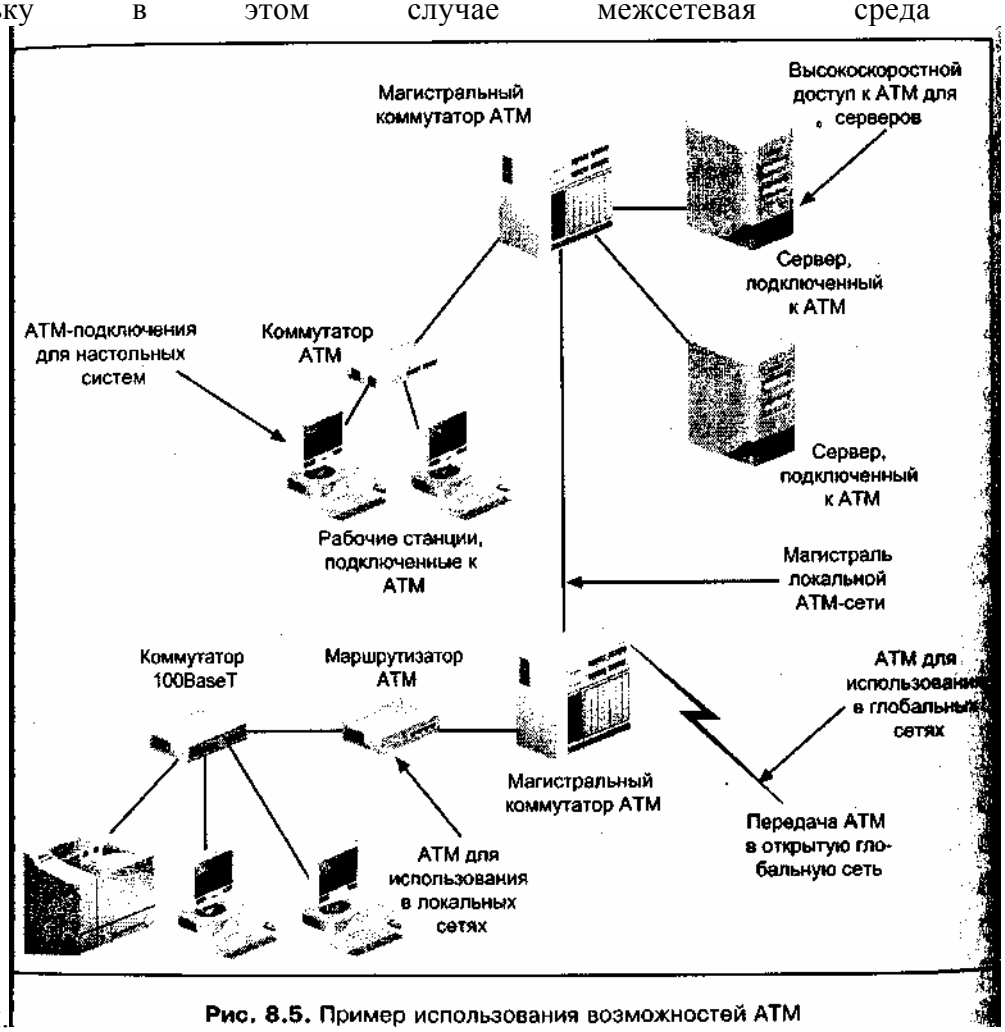


Рис. 8.5. Пример использования возможностей ATM

Примечание

При ошибках в проектировании и реализации (например, если коммутатор не справляется с сетевой нагрузкой или неправильно организовано управлении соединениями) ATM-сети могут получиться очень запутанными и сложными в управлении. Отдельные сегменты локальной сети, образующие типовую сеть кампуса, обычно работают с меньшей скоростью, чем магистраль. В этом

случае общая производительность сети получается достаточно высокой. Однако по мере роста сети и появления новых типов данных (например, мультимедийных) также должны увеличиваться и скорости, отвечающие требованиям настольных систем. Иногда проектировщики сети не предусматривают возможностей увеличения скорости магистрали (например, меняя 100-мегабитный Ethernet на сеть со скоростью 155,52 Мбит/с и выше). Технология ATM позволяет ступенчато увеличивать скорость магистрали до нескольких Гбит/с и выше. Также она позволяет разработчику предусмотреть перспективы развития сети.

ATM-сеть хорошо подходит для замены существующих магистралей с умеренными и средними характеристиками, например, в крупной сети, состоящей из локальных сетей. Модернизируемая магистраль (что особенно распространено) входит в состав некоторой уже развернутой сети Ethernet или Token Ring, в которой существующие задачи требуют повышения скорости магистрали, или которая должна соединяться с другими локальными сетями.

В действующих локальных сетях устройства, использованные для организации магистрали и связи сетей, должны быть совместимыми с многопротокольным оборудованием (например, со стоечным концентратором, оборудованным модулями для связи с имеющимися локальными сетями и для создания ATM-соединений) (рис. 8.6). Можно также использовать маршрутизатор и подключить ATM-коммутатор к существующей локальной сети. Если маршрутизатор не используется, форматы MAC-фреймов (например, Ethernet или Token Ring) в разных сетях должны совпадать. Преобразование фреймов не производится. Если же линия связи организуется с применением маршрутизатора, то возможно преобразование фреймов в разные форматы, для чего в маршрутизаторе должны присутствовать модули для соответствующих технологий.

Крупные многосегментные сети состоят из локальных сетей или сегментов локальных сетей, которые должны взаимодействовать на большом удалении и в которых должна присутствовать избыточность для обеспечения бесперебойных коммуникаций. В таких случаях магистраль должна состоять из нескольких ATM-коммутаторов. На рис. 8.7 изображена сеть со смешанными связями и магистралью на основе нескольких коммутаторов, которые создают резервные пути, благодаря которым в случае выхода из строя одного коммутатора данные могут передаваться по другим путям.

Примечание

В некоторых крупных организациях необходимы магистральные сети, позволяющие соединить множество локальных сетей, в которых используются разные технологии. В этом случае для преобразования протоколов и фреймов необходимо
применять многопротокольные концентраторы. Зачастую такие концентраторы работают и как маршрутизаторы, что определяется требованиями безопасности и необходимостью обеспечить совместимость нескольких технологий.

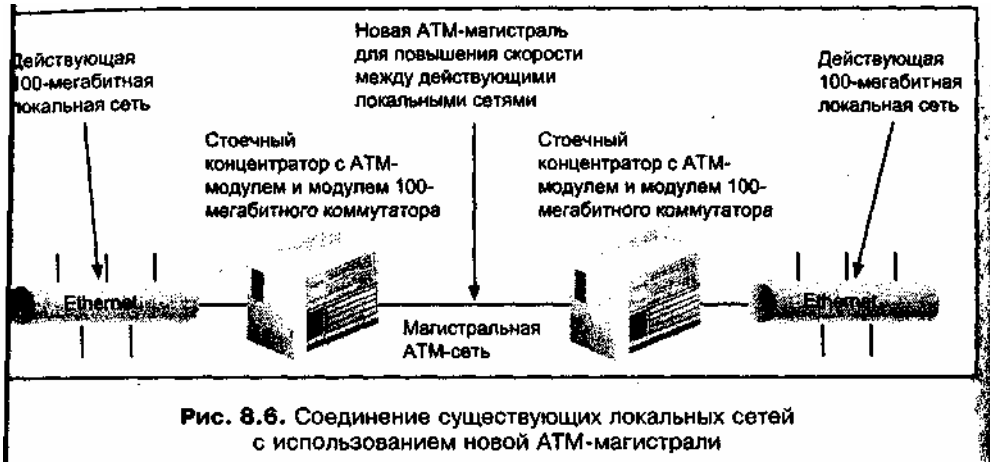


Рис. 8.6. Соединение существующих локальных сетей с использованием новой ATM-магистрали

Применение технологии ATM

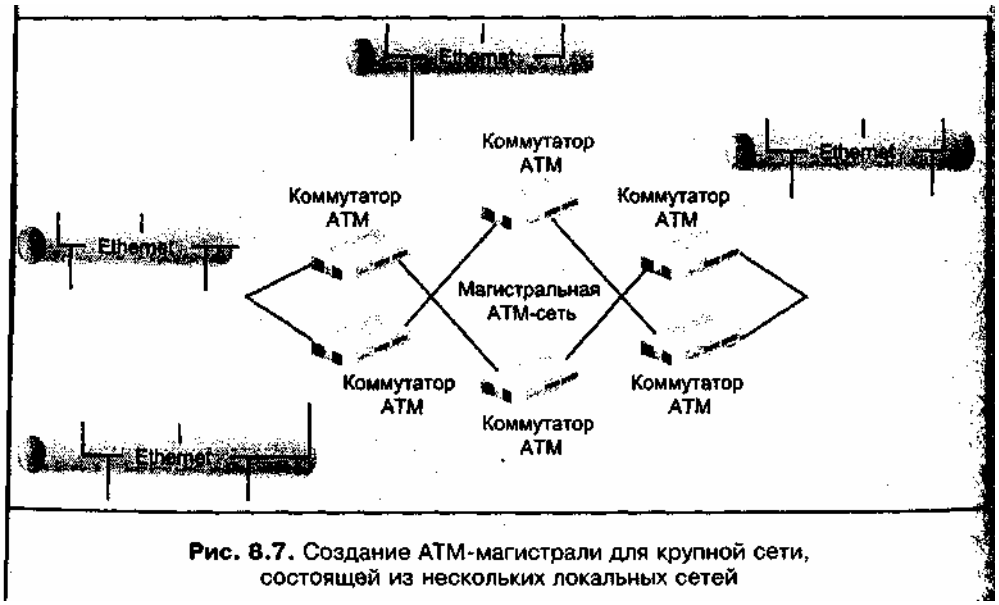


Рис. 8.7. Создание ATM-магистрали для крупной сети, состоящей из нескольких локальных сетей

при построении локальных сетей

Спецификация LANE, разработанная Форумом ATM, очень важна для интеграции технологии ATM в сети, где эта технология не использована. Спецификация LANE описывает не зависящий от протоколов метод взаимодействия устройств, подключенных к локальной сети, с помощью которого они могут обмениваться информацией через ATM-магистраль. Эта спецификация реализована на Уровне 2 модели OSI и функционирует как протокол моста, который делает ATM-сети с установлением соединений похожими на сети Ethernet или Token Ring, где соединения не устанавливаются. Спецификация LANE имеет следующие достоинства:

- существующее оборудование локальных сетей (например, сетевые адаптеры и связанные с ними программные драйверы Уровня 2) совместимо с LANE;
- прикладные программы и высокоуровневые протоколы могут взаимодействовать по LANE-сети;
- LANE-клиент может располагаться в любой точке ATM-сети (в том числе и в различных географических точках), и на него не распространяются ограничения на длину сегментов существующей локальной сети;
- большой сетевой трафик не вызывает проблем в работе, поскольку данные передаются по независимым виртуальным каналам, выделенным для эмулируемой локальной сети.

LANE-службы весьма ценны, т. к. они используют технологию ATM, ориентированную на установление соединений, и не требуют никаких изменений в аппаратных и программных средствах имеющейся локальной сети. Можно без модификаций применять устройства, подключенные к сети Ethernet, Token Ring или FDDI, что оправдывает затраты, вложенные в существующую сеть. Для этой сети требуется лишь некоторый интерфейс для связи локальной сети с ATM-сетью (в соответствии с топологией и типом оборудования). При наличии сети FDDI фрейм FDDI должен транслироваться во фрейм Ethernet или Token Ring.

Примечание

Существующие технологии локальных сетей нельзя смешивать в эмулируемых сетях, если не используется маршрутизатор для трансляции. Например, в ATM-сетях без маршрутизаторов все имеющиеся локальные сети должны быть одного типа: Ethernet, Token Ring или FDDI. Ethernet-сеть можно подключить к сети Token Ring через маршрутизатор, а коммутатор можно использовать для эмулируемых локальных сетей, работающих на основе одной и той же технологии.

LANE-компоненты

В эмулируемой локальной сети используются программные средства, осуществляющие функции преобразования и управления, причем эти средства располагаются в различных устройствах ATM-сети. Двумя самыми важными компонентами являются *клиент-эмулятор локальной сети* (LAN

Emulation Client, LEG) и *служба эмуляции локальной сети* (LAN Emulation Services). Программы LEC-клиента могут размещаться в устройстве связи локально сети с ATM-сетью или они могут входить в пакет программ, располагающихся на подключенном устройстве ATM (например, на некотором сервере). Главная задача программ LEC-клиента – обеспечивать соответствия MAC-адресов и адресов ATM при разрешении адресов. Программное обеспечение службы эмуляции локальной сети реализовано в виде трех логических серверов:

- LAN Emulation Server (LES) – главный сервер, который обеспечивает регистрацию адресов и разрешение MAC-адресов в адреса ATM, а также преобразование дескрипторов маршрутизации в адреса ATM;
- Broadcast and Unknown Server (BUS) – центр управления широковещательными и групповыми посылками для новых станций, подключающихся к эмулируемой локальной сети, а также для размещения и маршрутизации ATM-ячеек к целевым узлам;
- LAN Emulation Configuration Server (LEGS) – сервер, содержащий информацию о конфигурации ATM-сети, включая сведения обо всех эмулируемых локальных сетях.

Для того чтобы добиться наилучшей производительности и надежности ATM-сети, размещение перечисленных серверов нужно планировать заранее. Все три сервера можно установить на один ATM-коммутатор, а может распределить их по сети между различными коммутаторами или ATM совместимыми маршрутизаторами. Например, LES-сервер можно установить на некотором коммутаторе ATM-магистрали, LECS-сервер может работать на сервере, подключенном к ATM-сети, а BUS-сервер может находится в модуле связи локальной сети и ATM-сети.

Примечание

Размещение серверных служб LANE требует тщательного планирования крупных и сложных ATM-сетях, содержащих сотни ATM-устройств и клиентов работающих с различными интерфейсами и скоростями.

Спецификация LANE 2.0 описывает улучшенные серверные службы, в особенности изменения касаются масштабируемости эмулируемых локальных сетей. В спецификации LANE 1.0 имеется ограничение: для каждой эмулируемой локальной сети допускается только один LECS-, LES- и BUS1 сервер. Спецификация LANE 2.0 предусматривает резервирование LANE с использованием нескольких LECS-, LES-, и BUS-серверов. Кроме того, в отличие от версии 1.0, версия LANE 2.0 поддерживает качество обслуживания (QoS) и службу с доступной скоростью передачи (ABR).

Передача IP поверх ATM (Classical IP over ATM)

Еще один способ передачи существующего трафика по ATM-сети описан в спецификации *Classical IP over ATM,* определенной группой IETF. Эта спецификация использует MAC-подуровень протокола IP и, в отличие от эмуляции LANE (которая совместима со всеми протоколами локальных сетей, относящимися к верхним уровням модели OSI), поддерживает только один протокол – IP. При этом она не эмулирует MAC-подуровень. Поскольку ATM-сети не используют широковещательные рассылки, спецификация Classical IP over ATM (описанная в RFC 2225) для разрешения MAC-адресов в IP-адреса использует протокол Address Resolution Protocol (ARP) *(см. главу 6).*

Для реализации Classical IP over ATM необходимо, чтобы каждая подсеть имела собственный ARP-сервер. Этот сервер располагается на IP-совместимом маршрутизаторе, и все коммуникации между различными подсетями должны проходить через один или несколько маршрутизаторов. Данная спецификация детализирована в RFC 1577 и описывает регистрацию клиента в сети. Процесс регистрации инициируется клиентом с учетом имеющегося у него адреса ARP-сервера. Клиент подключается к ARP-серверу, сообщая ему свой ATM-адрес и протокольный адрес. После этого ARP-сервер помещает данную информацию в свой кэш для последующих ссылок, она используется при установлении соединений для клиентов, запрашивающих передачу данных. Передающий узел запрашивает соединение с принимающим узлом, а сервер ищет адрес целевого узла в своем кеше. Если в кеше имеются соответствующие сведения, сервер возвращает клиенту адрес. Если эти сведения отсутствуют, сервер передает ARP-запрос для поиска в сети принимающего узла. После того как узел найден, сервер отвечает на запрос клиента, который использует полученную адресную информацию для осуществления вызова по целевому ATM-адресу принимающего узла.

Спецификация Classical IP over ATM проще в реализации, чем LANE, и генерирует меньше служебной информации. Однако она требует, чтобы любое устройство, подключенное к имеющейся

локальной сети, при связи с целевым устройством передавало данные через маршрутизатор.

Многопротокольные коммуникации поверх ATM (Multiprotocol over ATM, MPOA)

Спецификация *Multiprotocol over ATM (MPOA)* (Многопротокольные коммуникации поверх ATM) позволяет маршрутизировать трафик через ATM-сеть. При этом для осуществления коммуникаций через границы подсетей протоколы сетевого уровня используют маршрутизаторы – как и спецификация LANE, для реализации которой нужно, чтобы коммуникации между эмулируемыми локальными сетями выполнялись через маршрутизаторы. В крупных сетях с интенсивным трафиком это снижает производительность, поскольку SAR-подуровень (Segmentation and Reassambler) ATM-сети создает задержки при пересылке пакетов и ячеек. Спецификация Multiprotocol over ATM объединяет LANE и протокол *Next Hop Resolution Protocol (NHRP)* (Протокол разрешения следующей пересылки), управляющий оконечными системами, которые не подключены к одному и тому же связующему уровню ATM-сети. Передающий узел использует протокол NHRP для определения адреса Канального уровня, необходимого для установления связи с целевым узлом. В работе протокола участвуют серверы Next Hop Server (NHS), хранящие и находящие наилучшие пути между узлами, а также обеспечивающий прямые соединения между узлами через ATM-сеть.

Ниже перечислены компоненты, необходимые для реализации MPOA-сети:

- сервер, включающий NHS-серверы, которые поддерживают таблицы маршрутизации и оценивают сетевые маршруты, а также взаимодействуют *m* другими серверами, в том числе и с другими серверами маршрутизации;
- клиент (также называемый краевым устройством), который принимает MPOA-коммуникации. Клиентами являются интеллектуальные сетевые коммутаторы и сетевые адаптеры в подключенных устройствах ATM, которые управляют потоком данных и выполняют запросы на установления связи по сети;
- хост, являющийся стандартным клиентом-эмулятором локальной сети MPOA-клиентов, а также имеющий специальные MPOA-расширения. Хост выполняет протокольные функции, посылая и отвечая на MPOA-запросы идентифицируя сетевые потоки, обеспечивая инкапсуляцию Уровня 2 и устанавливая прямые связи;
- LAN Emulation Server (LES), который идентифицирует MPOA-компоненты и выполняет функции сервера регистрации для MPOA-совместимых клиентов;
- LAN Emulation Configuration Server (LEGS), используемый для конфигурирования всех MPOA-совместимых клиентов и серверов. Он также указывает MPOA-клиентам, когда нужно запрашивать связь. Оба сервера требуют спецификации LANE 2.0.

Обеспечение высокоскоростного доступа к серверам локальной сети

Если технология Fast Ethernet уже не в состоянии справиться со всем трафиком, идущим к серверам локальной сети, то ATM-сеть является одним из решений этой проблемы (другое решение – Gigabit Ethernet). Некоторый организации непосредственно подключают серверы к ATM-сети, устанавливая на серверы адаптеры ATM и соединяя их с ATM-коммутатором, располагающимся на ATM-магистрали. Обычно при этом используются скорости ATM, равные 155,52 Мбит/с или 622,08 Мбит/с, но по мере надобности можно создать и более быстрые каналы связи.

Примечание

Системы Windows 2000 (Professional и Server), Windows XP Professional и Windows Server 2003 имеют службы, позволяющие этим системам поддерживать установку адаптера ATM. Например, спецификация NDIS компании Microsoft совместима с драйверами адаптеров ATM, и имеется административная утилита ATM, позволяющая просматривать параметры подключения, выполненные через адаптер ATM (в практическом задании 8-2 более подробно рассказано об этой утилите). Также в этих операционных системах имеется программа UNI Call Manager, которая позволяет работать с постоянными (PVQ и коммутируемыми (SVC) виртуальными каналами ATM. Более того, эти системы реализуют разрешение ATM-адресов, когда работают с протоколом ARP при выполнении коммуникаций с использованием TCP/IP.

Во многих сетях серверы расположены в одном помещении (например, в закрытом машинном зале),

поэтому никто, кроме администраторов серверов, не имеет к ним доступа. Иногда такие серверы называются группой серверов (server farm). Такое размещение серверов имеет заметные преимущества, поскольку их близость друг к другу упрощает подключение к одному или нескольким АТМ-коммутаторам, располагающимся на сетевой магистрали. Другие преимущества группы серверов перечислены ниже:

- упрощается модификация линий связи с серверами с целью повышения полосы пропускания (например, с 155,52 Мбит/с до 622,08 Мбит/с), причем эта операция обходится дешевле, чем в случае, когда серверы разбросаны по разным помещениям;
- расположение серверов на сетевой магистрали позволяет сетевому администратору упростить управление доступом к серверам, направляя трафик, идущий к ним, через маршрутизаторы магистрали;
- наличие общей площадки позволяет обезопасить серверы от злоумышленников (можно закрыть двери в помещение);
- серверы, расположенные в одном помещении, проще подключать к фильтрованной силовой сети и источникам бесперебойного питания;
- при правильном выборе оборудования можно сэкономить средства, используя общий монитор для нескольких серверов.

Подключение настольных систем к АТМ-сети

Технология АТМ обычно рассматривалась как основа для создания магистралей локальных и глобальных сетей, но ее можно распространить и на рабочие станции, если требуется уменьшить нагрузку на сеть со стороны ресурсоемких прикладных программ (например, мультимедийных) или нужно обеспечить качество обслуживания (QoS). В настоящее время для подключения пользовательских станций имеются спецификации АТМ, определяющие скорости 25,6 Мбит/с и 51,84 Мбит/с. Чтобы реализовать АТМ-службы з настольной системе, нужно в каждое оконечное устройство установить сетевой адаптер АТМ (при этом внутренняя шина должна иметь достаточное быстродействие, чтобы смена сетевой технологии имела смысл). В практическом задании 8-3 рассказано, как установить LANE-совместимый адаптер, в системе Windows 2000.

Совет

Если вы конфигурируете систему Windows 2000 или Windows XP для работы с АТМ-адаптером, убедитесь в том, что установлена АТМ-служба APR/MARS. Для этого в системе Windows 2000 выберите значок **My Network Places** (Мой сетевое окружение), щелкните правой кнопкой мыши и в контекстном меню выполните команду **Properties** (Свойства). В системе Windows XP в меню **Start**(Пуск) выберите опцию **My Network Places** (Мое сетевое окружение), щелкните правой кнопкой мыши и в контекстном меню выполните команду **Propertied**(Свойства). В открывшемся окне нажмите кнопку **Install** (Установить), дважды щелкните по опции **Protocol** (Протокол), а затем – по опции **ATM APR/MAR Service** (Служба АТМ APR/MARS).

Применение технологии АТМ
при построении глобальных сетей

Многие телекоммуникационные компании предоставляют услуги глобальной связи через АТМ-сети, которые в настоящее время позволяют обеспечивать быстродействие глобальных сетей до 10 Мбит/с, причем практически и достигнуты скорости до 40 Мбит/с. Подключение к глобальной АТМ-сети ; выглядит естественным для сети, в которой уже имеется АТМ-магистраль для этого зачастую достаточно установить дополнительный модуль в имеющийся АТМ-коммутатор или маршрутизатор.

Если в локальной сети, подключаемой к глобальной АТМ-сети, технологии АТМ не используются (например, если в сети передаются пакеты Ethernet то между локальной и глобальной сетями нужно установить АТМ-коммутатор или интерфейс (например, какой-нибудь АТМ-интерфейс в маршрутизаторе), который будет осуществлять коммуникации, преобразовывая пакеты в ячейки (и наоборот).

Помимо соединения нескольких локальных сетей с помощью глобально АТМ-сети, имеются и другие области применения технологии АТМ в глобальных сетях, в том числе:

- передача ATM-ячеек через сети SONET;
- соединение глобальных сетей frame relay с использованием глобальной ATM-сети:
- соединение глобальных сетей SMDS с использованием глобальной ATM-сети.

Все перечисленные типы коммуникаций рассматриваются в следующих разделах.

Передача ATM-ячеек по сети SONET

Обычно для передачи ATM-ячеек через сети SONET используется стандарт ITU-T I.432 (для отображения ATM-ячейки во фрейм SONET STS-1) и спецификация ATM to SONET, разработанная Форумом ATM и обеспечивающая скорость 622,08 Мбит/с. В обоих случаях локальные или глобальные ATM-сети, расположенные на значительном удалении друг от друга, можно соединить через сеть SONET, используя достоинства этой сети, а именно – высокую полосу пропускания и доступность. Например, в крупной торговой компании магистральные локальные ATM-сети могут быть развернуты в административном офисе и больших магазинах. Все эти сети можно связать в масштабах страны, передавая ATM-ячейки по сетям **SONET.**

Передача ATM-ячеек по сетям SONET является особо удачным сочетанием, поскольку структура ATM-ячейки идеально подходит для отображения во фреймы SONET. Кроме того, используемые в ATM-сетях виртуальные каналы и технология мультиплексирования с разделением времени (TDM) в значительной степени совместимы со структурой виртуальных блоков (virtual tributary) и методами коммутации, применяемыми в сетях SONET.

Передача пакетов frame relay по ATM-сети

Сети ATM и frame relay совместимы друг с другом, благодаря чему глобальные сети frame relay можно связать через ATM-сеть. Например, иногда две глобальные сети frame relay дешевле соединить по выделенной линии глобальной ATM-сети, что позволяет сэкономить затраты на выделенные линии frame relay. В других случаях может понадобиться увеличить скорость передачи сети frame relay по протяженной линии связи, для чего две глобальные сети frame relay со средним быстродействием можно соединить через скоростную глобальную ATM-сеть. В таком случае ATM-сеть будет играть роль магистрали для связи друг с другом пользователей сети frame relay.

Frame Relay Forum разработал стандарт *Internetworking Function (IWF)* (Функция межсетевого обмена), обеспечивающий функции отображения и инкапсуляцию, позволяющие сохранить параметры служб frame relay при передаче по ATM-сети. Стандарт IWF допускает использование одного из двух методов инкапсуляции (которые несовместимы друг с другом): взаимодействие сетей (network internetworking) и межсетевое взаимодействие служб (service internetworking).
При взаимодействии сетей конечный ATM-узел между сетью frame relay и ATM-сетью незначительно изменяет инкапсулированный фрейм сети Frame Relay. По сути, преобразование фрейма выполняется прозрачно для сети Frame Relay, поскольку оно осуществляется ATM-устройствами (например, коммутаторами в глобальной ATM-сети). Фрейм сети frame relay попросту отображается в ATM-ячейки, для чего из фрейма удаляется поле контрольной последовательности кадра (FCS) и добавляется завершающее поле AAL 5 для совместимости с ATM. На рис. 8.8 представлен пример взаимодействия сетей, в котором коммутаторы ATM-сети выполняют трансляцию фреймов.

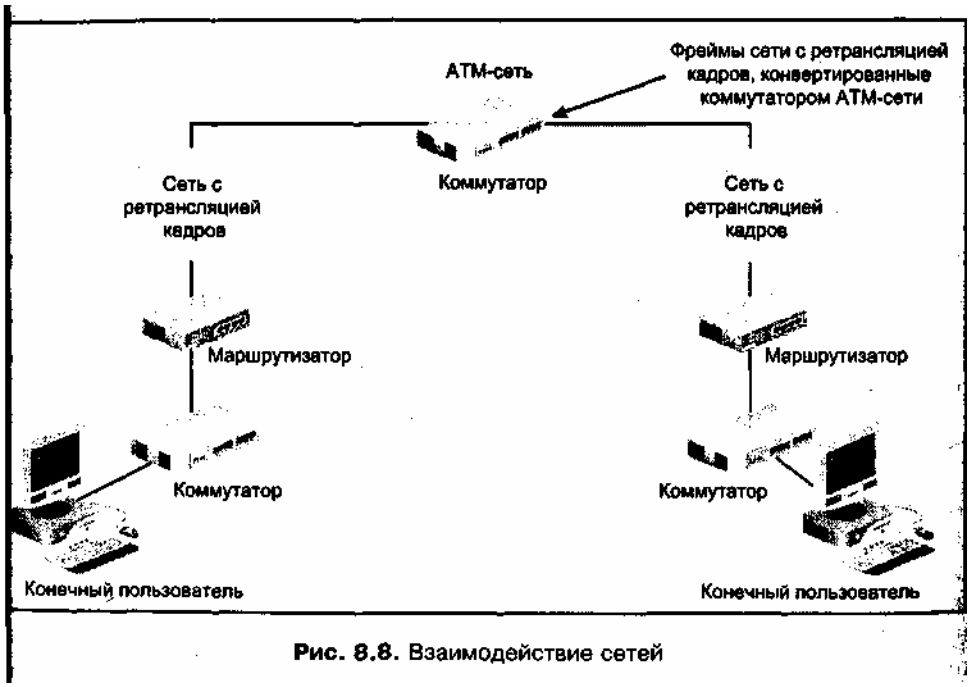


Рис. 8.8. Взаимодействие сетей

межсетевое взаимодействие служб – это более сложная технология, чем взаимодействие сетей, т. к. краевые устройства сети frame relay (например 'коммутаторы или маршрутизаторы) выполняют значительные преобразования фреймов для пересылки по глобальной АТМ-сети. Поэтому преобразование фрейма сети frame relay в АТМ-ячейку не является прозрачным frame relay, поскольку оно выполняется до того, как фрейм отправится 1 АТМ-сеть. Во всех краевых устройствах сети frame relay (в том числе на коммутаторах и маршрутизаторах) устанавливаются адаптеры или модули АТМ, которые выполняют необходимую инкапсуляцию фреймов в ячейки передаче данных и обратное преобразование – при получении данных. В процессе инкапсуляции фрейма в ячейку преобразуются функции заголовка, добавляется (или удаляется) информация о классе обслуживания AAL Type 5, включаются сведения о приоритете и изменяется информация для преобразования адресов. Межсетевое взаимодействие служб иллюстрируется на рис. 8.9.

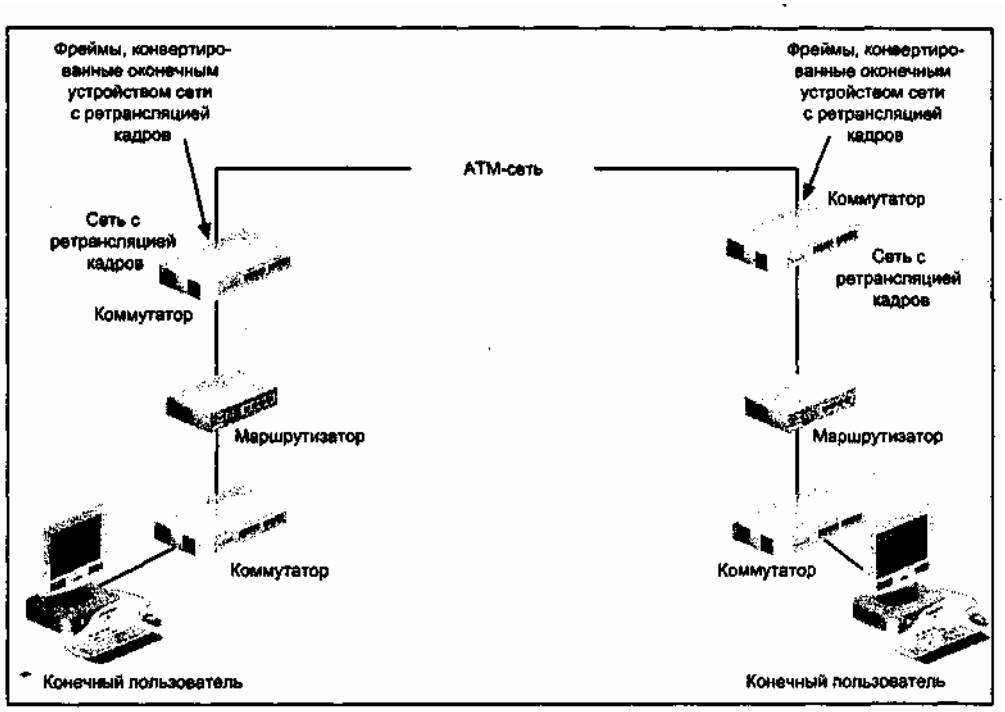


Рис. 8.9. Межсетевое взаимодействие служб

В практическом задании 8-4 вы познакомитесь с предоставляемыми компанией AT&T услугами по связи сетей frame relay и глобальных АТМ-сетей.

Передача пакетов SMDS по АТМ-сети

Служба Switched Multimegabit Data Service (SMDS) и ее европейский эквивалент – служба Connectionless Broadband Data Service (CBDS) – могут быть развернуты поверх ATM-сети. Они описаны в стандарте региональных сетей IEEE 802.6 на шину Distributed Queue Dual Bus (DQDB). Структура ячейки DQDB похожа на формат ATM-ячейки, что упрощает совместимость сетей, особенно потому, что спецификация шины DQDB напоминает требования к Конвергентному подуровню AAL Type 3/4 сетей ATM. Эта реализация также называется LANE over Public Networks (LANE поверх сетей общего пользования).
Операции сегментации и сборки напоминают аналогичные операции в ATM1I сетях, ими управляет SMDS Internet Protocol (SIP). Подключение стандартных ATM-устройств к сетям SMDS требует внешней реализации Internetworking Function (IWF), для чего она чаще всего встраивается в маршрутизатор, поддерживающий Конвергентный подуровень AAL Type 3/4.

Виртуальные локальные сети

Технология ATM в значительной степени совместима с *виртуальными локальными сетями* (virtual LAN, VLAN), которые иногда создаются для повышения эффективности сети (они обсуждались в *главе 4).* VLAN-сеть представляет собой набор устройств, которые динамически группируются протоколу, участию в эмуляции локальной сети или MAC-адресу, в результате чего создаются независимые области коллизий и широковещания ДЛЯ решения задач управления трафиком и обеспечения безопасности. При использовании в ATM-магистрали VLAN-сеть может включать в себя пользовательские станции, как имеющейся локальной сети, так и ATM-сеть, VLAN-сеть может также пересекать границы глобальной сети и охватывала любое количество сетевых устройств. Такая сеть позволяет одной группе устройств непосредственно взаимодействовать с другой группой при отсутствии физической связи через мост или маршрутизатор. Клиенты VLAN-сети могут находиться в любой точке коммутируемой сети, поскольку член сетевых устройств в логической подсети (или же в одной или нескольких VLAN-сетях) задается программными средствами. Клиенты VLAN-сети связываются между собой при помощи одного из двух способов: либо он» непосредственно соединяются с подключенным устройством ATM, они соединяются с устройством связи локальной сети с ATM-сетью.

Виртуальные локальные сети, построенные на базе ATM-сетей, имеют следующие преимущества:

- сеть может быть разбита на логические сегменты, т. е. ограничения физической сети можно обойти (например, в одну VLAN-сеть можно поместив две рабочие станции, находящиеся в разных физических сегментах);
- повышается производительность сети, поскольку имеется больше возможностей для сегментации областей коллизий и широковещания;
- дополнительные функции управления сетью позволяют клиентам VLAN-сети располагаться в любой физической точке или менять местоположение без изменений архитектуры сети;
- клиенты VLAN-сети могут находиться в той же VLAN-сети, что и серверы, к которым они чаще всего обращаются; это уменьшает количество пересылок при маршрутизации и снижает требования к полосе пропускания.

В практическом задании 8-5 вы познакомитесь с основами планирования и реализации VLAN-сетей в коммутируемой сети.

Управление локальными и глобальными ATM-сетями

Ниже перечислены некоторые основные задачи управления локальными и глобальными ATM-сетями:

- необходимость мониторинга и управления всеми постоянными (PVC) и коммутируемыми (SVC) виртуальными каналами;
- необходимость управления топологией сети, чтобы обеспечить совместимость с ATM;
- необходимость мониторинга состояния каждого сетевого устройства.

Главной является задача мониторинга перегрузки сети и управления потоками данных для оптимизации трафика. Проблема перегрузки АТМ-сети менее актуальна в небольших территориальных конфигурациях, поскольку расстояния в них относительно малы, а трафик ячеек ниже, чем в средних и крупных сетях. Проблемы перегрузки возрастают по мере увеличения локальной или глобальной сети и становятся критически важными в глобальных сетях с далеко разнесенными узлами. Если сеть испытывает перегрузку и целевой коммутатор должен запросить исходный коммутатор о прекращении отправки ячеек, возникают потери ячеек из-за задержки в работе функций управления потоком или команд понижения скорости. В этом случае некоторые приложения могут войти в состояние тайм-аута или прекратить работу. Мониторинг перенасыщения сети позволяет принять меры (например, сконфигурировать VLAN-сети) до того, как перегрузка приведет к потере ячеек.

Резюме

1. АТМ – это высокоскоростная технология передачи данных в локальных и глобальных сетях, предназначенная также для подключения настольных систем, которая позволяет пересылать речь, видео, данные и мультимедиа. В АТМ-сети по виртуальным каналам передаются ячейки, *а* не пакеты,

2. Технология АТМ имеет многоуровневую архитектуру, Соответствующую эталонной модели OSI, однако ее верхний уровень выполняет функции, специфические для АТМ. Такое решение позволяет АТМ-сетям взаимодействовать с разнообразными протоколами и методами передачи данных, в том числе с сетями Ethernet, Token Ring, FDDI, Frame Relay, SONET, ISDN, DSL, SMDS и беспроводными сетями. Также по АТМ-сетям можно передавать протокол IP и осуществлять передачу нескольких протоколов одновременно.

3 АТМ-ячейка имеет фиксированную длину и состоит из 5-байтного заголовка и 48-байтной полезной нагрузки.

4. АТМ – это технология с установлением логических соединений, для чего создаются виртуальные каналы, служащие в АТМ-сети информационными магистралями между узлами.

5. В АТМ-сетях используются постоянные виртуальные каналы и коммутируемые виртуальные каналы. Первый тип каналов представляет собой выделенную логическую цепь между двумя конечными точками. Каналы второго типа создаются по мере необходимости и существуют столько времени, сколько длятся коммуникации между устройствами.

6. При проектировании АТМ-сети следует рассматривать такие элементы сети, как АТМ-компоненты и АТМ-коммутаторы, а также характеристики коммутаторов и типы АТМ-интерфейсов.

7. Технология АТМ имеет много областей применения: АТМ-сеть как магистраль локальной сети, построение локальных сетей на базе АТМ, создание высокоскоростных линий доступа к серверам, подключение настольных систем к АТМ-сетям, а также построение глобальных сетей на базы АТМ.

8 Виртуальные локальные сети (VLAN), построенные на базе АТМ-сети позволяют разбивать сеть на логические сегменты без учета ограничений физической конфигурации сети и использовать логическое сегментирование для повышения производительности сети.

9. К задачам управления АТМ-сетью относится мониторинг виртуальный каналов, сетевой топологии и состояния устройств АТМ-сети.

Основные термины

ATM Adaptation layer Адаптационный уровень АТМ. В терминологюЯ АТМ – уровень, ответственный за сегментацию и упаковку/распаковку данных, преобразуемых в формат ячейки АТМ или получаемых из нее.

***TM* attached device Подключенное устройство АТМ.** Устройство, преобразующее поток данных в поток ячеек АТМ или обратно: например, АТМ-Ц интерфейс на сервере.

ATM Forum Форум АТМ. Консорциум производителей аппаратных средств, поставщиков телекоммуникационных услуг и пользователей, которые вместе с ITU-T работают над спецификациями по использованию АТМЦ в локальных и глобальных сетях.

ATM layer Уровень АТМ. В терминологии АТМ – уровень, отвечающий за создание АТМ-ячеек.

ATM permanent virtual circuit (РУС) Постоянный виртуальный канал АТМ.
Выделенная цепь, имеющая предопределенный путь и фиксированную полосу пропускания между двумя

указанными конечными точками.

ATM Physical layer Физический уровень ATM. В терминологии ATM – уровень, обеспечивающий преобразование потока ячеек в передаваемые двоичные разряды, а также управляющий функционированием физической среды или кабеля.

ATM Protocol Reference Model Эталонная модель протокола ATM. Четырехуровневая модель ATM-коммуникаций, обеспечивающая одновременное функционирование множества устройств в единой сети.

ATM Services and Application layer Уровень служб и приложений ATM. В терминологии ATM – уровень, определяющий класс обслуживания, необходимый для передачи данных. Этот уровень также обеспечивает связь между узлом, генерирующим поток данных, и Адаптационным уровнем ATM.

ATM smart permanent virtual circuit (SPVC) Интеллектуальный постоянный виртуальный канал ATM. Сочетает в себе характеристики PVC- и SVC-каналов. Подобно PVC-каналу, SPVC-канал можно конфигурировать вручную (однако только для конечных устройств); как и в SVC-канале, каждый сеанс передачи данных имеет свой собственный путь к одному или нескольким коммутаторам, через которые информация должна передаваться.

ATM switch Коммутатор ATM. Коммутатор, реализующий механизм передачи ячеек, описанный многоуровневой моделью ATM.

ATM switched virtual circuit (SVC) Коммутируемый виртуальный канал ATM.
Цепь, образуемая и используемая для отдельного сеанса обмена данными и удаляемая по завершении сеанса.

ATM virtual circuit Виртуальный канал (виртуальная цепь) ATM. Определяет логические каналы, по которым выполняется передача ATM-данных. Логические каналы ATM образуются двумя компонентами: 1) виртуальными каналами (channels), представляющими собой логические соединения между устройствами; 2) виртуальными путями (paths), каждый из которых является набором виртуальных каналов.

Internetworking Function (IWF) Функция межсетевого обмена. Стандарт, описывающий функции отображения и инкапсуляции для реализации передачи пакетов frame relay по сети ATM.

Next Hop Resolution Protocol (NHRP) Протокол разрешения следующей пересылки. Протокол, позволяющий передающему узлу одной сети определять адрес Канального уровня для установления связи с принимающим узлом Другой сети в тех случаях, когда эти сети соединены через ATM-сеть.

Physical Medium Dependent (PDM) sublayer Подуровень, зависящий от фи41 **зической среды передачи данных.** Один из двух подуровней Физического! уровня ATM. Он обеспечивает функционирование передающей среды и реализует различные скорости передачи данных, возможные для этой среды. Ц

Private Network-to-Network Interface (PNNI) Частный межсетевой интер**фейс.** Протокол ATM-маршрутизации, с помощью которого коммутаторы обмениваются между собой информацией, содержащейся в таблицах соединений. Таблицы соединений содержат сведения о различных путях в eerie поэтому .с их помощью некоторый коммутатор может выбрать путь, наиболее подходящий для конкретной операции пересылки данных.

Segmentation and Reassembly (SAR) sublayer Подуровень сегментации И сборки. Подуровень Адаптационного уровня ATM, который преобразует моли данных протокола в 48-байтные поля полезной нагрузки ячейки и пересылает их Уровню ATM.

Transmission Convergence (TC) sublayer Конвергентный подуровень передача данных. Один из двух подуровней Физического уровня ATM, обрабатывающий входящие ячейки, передаваемые в виде потока двоичных данных PDM-подуровня, на принимающем узле. Также управляет изменением скорости передачи данных в физическом интерфейсе.

User-Network Interface (UNI) Интерфейс "пользователь-сеть". ATM- интерфейс, используемый для связи оконечного оборудования узла и коммутатора.

Virtual path identifier/virtual channel identifier (VPI/VCI) Идентификатор вир**туального пути/идентификатор виртуального канала.** Двоичное число в АТМШ ячейке, позволяющее направить ее в указанный выходной интерфейс.

Виртуальная локальная сеть Virtual LAN (VLAN). Логическая сеть, состоящая из подсетей рабочих групп, созданных при помощи специальных программных средств на основе коммутаторов и маршрутизаторов, и независящая от физической топологии сети.

Виртуальный канал Virtual circuit. Логический коммуникационный путь формирующийся на Сетевом уровне модели OSI, для передачи данных. *См. ATM virtual circuit.*

Качество обслуживания Quality of Service (QoS). Совокупная характеристика сети, определяющая ее способность передавать информацию и отражающая качество, скорость и надежность связи.

Клиент-эмулятор локальной сети LAN Emulation Client (LEC). Программные средства сети ATM, используемые в устройстве сопряжения локальной сети с ATM-сетью или входящие в состав программного обеспечения поключенного устройства ATM (например, некоторого сервера). Их основна функция – выполнять разрешение адресов путем сопоставления MAC-Я адресов адресам сети ATM.

Коммутация ячеек Cell switching. Метод коммутации, при котором используются временное уплотнение (time-division multiplexing, TDM) и виртуальные каналы. При выполнении коммутации ячеек в начало каждого временного интервала (окна) TDM помешается короткий признак (идентификатор виртуального канала).

Конвергентный подуровень Convergence sublayer. Подуровень Адаптационного уровня ATM, получающий пакеты от более высоких уровней, назначающий класс обслуживания и создающий модуль данных протокола для передачи SAR-подуровню Адаптационного уровня ATM.

Межсетевой интерфейс (интерфейс сетевых узловNetwork Node Interface (NNI). ATM-интерфейс, используемый для связи двух ATM-коммутаторов. Иногда носит название Network-to-Network Interface.

Многопротокольные коммуникации поверх ATM Multiprotocol over ATM (MPOA). Коммуникационная технология, позволяющая пересылать по ATM-сети пакеты различных протоколов.

Передача IP поверх ATM Classical IP over ATM. Пересылка IP-пакетов по ATM-сети. Эта технология ориентирована исключительно на поддержку протокола IP.

Служба эмуляции локальной сети LAN Emulation Service. Программные средства ATM-сети, размещаемые на различных серверах и выполняющие три функции. Во-первых, они обеспечивают регистрацию адресов и разрешение MAC-адресов в адреса ATM-сети (на сервере эмуляции локальной сети – LAN Emulation Server). Во-вторых, они обеспечивают функции центра управления широковещательными и групповыми рассылками для новых станций, подключающихся к эмулируемой локальной сети, а также выполняют размещение и маршрутизацию ATM-ячеек (на сервере, называемом Broadcast and Unknown Server). В-третьих, эти программы содержат всю информацию о конфигурации ATM-сети (на сервере конфигурации средств эмуляции локальной сети – LAN Emulation Configuration Server).

Эмуляция локальной сети A LAN Emulation (LANE). Метод адаптации технологии ATM к сетям Ethernet; для его реализации создается широковещательная сеть, позволяющая заранее определенным группам Ethernet-узлов принимать передаваемую информацию.

Ячейка Cell. Модуль данных фиксированного размера для высокоскоростной передачи данных; обычно применяется в технологии ATM.

Вопросы для повторения

1. В ATM-сетях интерфейс между сервером и ATM-коммутатором называется . .

а) интерфейсом "пользователь-сеть" (User-Network Interface);
б) Межсетевым интерфейсом (Network Node Interface);
в) Межузловым интерфейсом (Node-to-Node Interface);
г) интерфейсом AAL Type S.

2. Аббревиатура LANE означает_____ .
3. Какой тип виртуального канала не применяется в сетях ATM?

а) постоянный виртуальный канал;
б) кластерный виртуальный канал;
в) коммутируемый виртуальный канал;
г) интеллектуальный постоянный виртуальный канал.

4. Адаптер ATM, установленный в сервере, называется _____

а) виртуальным канальным мультиплексором;
б) коммутирующим устройством ATM;
в) интерфейсом ячеек;
г) подключенным устройством ATM.

5. Маршрутизация ATM осуществляется на _____ .

а) Адаптационном уровне ATM;
б) Физическом уровне ATM;
в) Уровне служб ATM;

г) Уровне АТМ.

6. Форматирование АТМ-ячейки выполняется на _____.

а) Адаптационном уровне АТМ;
б) Физическом уровне АТМ;
в) Уровне служб АТМ;
г) Уровне АТМ.

7. Какие из перечисленных скоростей возможны при подключении стольной системы к АТМ-сети?

а) 51,84 Мбит/с;
б) 622,08 Мбит/с;
в) 2,4 Гбит/с;
г) все перечисленные;
д) только б) и в).

8. Что из перечисленного не является компонентом LANE?

а) Broadcast and Unknown Server;
б) LAN Emulation and Configuration Server;
в) LAN Emulation Server;
г) Network Routing Emulator.

9. Какой размер имеет АТМ-ячейка?

а) 5 байт;
б) 48 байт;
в) 53 байта;
г) 144 байта.

10. Многопротокольные коммуникации поверх АТМ. (Multiprotocol over ATM, MPOA) интегрируют спецификацию LANE и _____.

а) FDDI;
б) Routing Information Protocol (RIP);
в) Next Hop Resolution Protocol (NHRP); г) SMDS.

11. Технология передачи IP поверх АТМ (Classical IP over ATM) эмулирует MAC-подуровень модели OSI. Да или нет?

12. Какой класс АТМ используется для передачи пакетного видео?

а) Класс А;
б) Класс В;
в) Класс С;
г) Класс D.

13. Какой тип кабеля используется для АТМ?

а) многомодовый оптоволоконный кабель;
б) одномодовый оптоволоконный кабель;
в) кабель на основе неэкранированной витой пары;
г) все перечисленные;
д) только а) и б).

14. При передаче видео в реальном масштабе времени трафик в сети АТМ можно охарактеризовать как.

а) "взрывообразный" (со всплесками);
б) имеющий постоянную скорость передачи;
в) короткие всплески трафика с периодами ожидания предсказуемой длительности;
г) короткие всплески трафика с периодами ожидания непредсказуемой длительности.

15. Скорость АТМ-коммуникаций для беспроводных сетей Universal МоЫЦ Telecommunication Systems составляет _____.

а) 1,544 Мбит/с;
б) 2 Мбит/с; в) 25,6 Мбит/с;
г) 1,2 Гбит/с.

16. При пересылке пакетов frame relay по сети АТМ используется класс обслуживания

а) AAL Type 1;

б) AAL Type 2;
в) AAL Type 3/4;
г) AAL Type 5.

17. Служба с неуказанной скоростью (UBR) в сетях ATM представляет собой

18. Какие из перечисленных полей в заголовке ячейки ATM содержат адресную информацию о маршрутизации

а) Базовое управление передачей (Generic Flow Control, GFC); б)Идентификатор виртуального пути (Virtual Path Identifier, VPI);
в) Идентификатор виртуального канала (Virtual Channel Identifier, VCI);
г) все перечисленные;
д) только б) и в).

19. Private Network-to-Network Interface (PNNI) является примером nротkола ATM-маршрутизации. Да или нет?

20. Технология ATM хорошо подходит для передачи ее данных по сети) SONET, поскольку
а) ячейка ATM хорошо укладывается во фрейм SONET STS-1;
б) в технологии ATM не используется мультиплексирование с разделинием времени (TDM), не совместимое с SONET;
в) ATM поддерживает только пакетный ("взрывообразный") трафик;
г) при таком способе передачи данных ATM-сеть напоминает сеть ISDN.,

21. Internetworking Function (IWF, функция межсетевого обмена) используете для

22. В виртуальных локальных сетях _____ .

а) для обеспечения безопасности не нужны маршрутизаторы, поскольку для упрощения конфигурации средства безопасности реализуют только коммутаторами;
б) отсутствуют области коллизий;
в) устройства группируются динамически, что повышает безопасность и производительность сети;
г) все коммуникации являются полудуплексными.

23. Технология ATM не совместима с DSL или FDDI. Да или нет?

24. В сетях ATM _____ уровень определяет класс обслуживания, используемый для передачи данных.

25. Какое из перечисленных устройств можно использовать для подключения ATM-коммутатора к существующей локальной сети?
а) пассивный концентратор;
б) маршрутизатор;
в) повторитель;
г) DLC-шлюз.

Практические задания

Задание 8-1

В этом задании вы посетите веб-сайт компании Cisco (одного из производителей ATM-устройств) и будете выбирать маршрутизаторы и коммутаторы с возможностью подключения к ATM-сетям.

Чтобы найти маршрутизаторы и коммутаторы с возможностью подключения к ATM-сетям, выполните такие действия:

1. Для доступа в Интернет запустите веб-браузер.
2. Введите адрес **www.cisco.com** и нажмите клавишу <Enter>.
3. На домашней странице сайта выберите ссылки **Products & Services** или **Technologies** (или же воспользуйтесь функцией поиска по сайту – ссылка **Search)** и найдите устройства перечисленных ниже типов, имеющие возможность работы в ATM-сетях:
   - серверы доступа;
   - оптические устройства;
   - маршрутизаторы;
   - коммутаторы.
4. Всю собранную информацию о возможностях ATM-устройств занесите в текстовый файл.

5. Скорость ATM-коммуникаций для беспроводных сетей Universal Mobile Telecommunication Systems составляет _____ а) 1,544 Мбит/с;
   б) 2 Мбит/с;
   в) 25,6 Мбит/с;
   г) 1,2 Гбит/с.
6. При пересылке пакетов frame relay по сети ATM используется класс обслуживания .
   а) AAL Type1;
   б) AAL Type 2;
   в) AAL Type 3/4;
   г) AAL Type 5.
7. Служба с неуказанной скоростью (UBR) в сетях ATM представляет собой
8. Какие из перечисленных полей в заголовке ячейки ATM содержат адресную информацию о маршрутизации?

   а) Базовое управление передачей (Generic Flow Control, GFC);
   б) Идентификатор виртуального пути (Virtual Path Identifier, VPI);
   в) Идентификатор виртуального канала (Virtual Channel Identifier, VCI);
   г) все перечисленные;

   д) только б) и в).

9. Private Network-to-Network Interface (PNNI) является примером прокола ATM-маршрутизации. Да или нет?

Э. Технология ATM хорошо подходит для передачи ее данных по сетями SONET, поскольку

а) ячейка ATM хорошо укладывается во фрейм SONET STS-1; б) в технологии ATM не используется мультиплексирование с разделением времени (TDM), не совместимое с SONET;
в) ATM поддерживает только пакетный ("взрывообразный") трафик;
г) при таком способе передачи данных ATM-сеть напоминает сеть ISDN.

1. Internetworking Function (IWF, функция межсетевого обмена) используется для

2. В виртуальных локальных сетях _____

а) для обеспечения безопасности не нужны маршрутизаторы, поскольку для упрощения конфигурации средства безопасности реализуются только коммутаторами; б) отсутствуют области коллизий;
в) устройства группируются динамически, что повышает безопасность и производительность сети;
г) все коммуникации являются полудуплексными.

23. Технология ATM не совместима с DSL или FDDI. Да или нет?

24. В сетях ATM _____ уровень определяет класс обслуживания, используемый для передачи данных.

25. Какое из перечисленных устройств можно использовать для подключения ATM-коммутатора к существующей локальной сети?
   а) пассивный концентратор;
   б) маршрутизатор;
   в) повторитель;
   г) DLC-шлюз.

Практические задания

Задание 8-1

В этом задании вы посетите веб-сайт компании Cisco (одного из производителей ATM-устройств) и будете выбирать маршрутизаторы и коммутаторы с возможностью подключения к ATM-сетям.

Чтобы найти маршрутизаторы и коммутаторы с возможностью подключения к ATM-сетям, выполните такие действия:

1. Для доступа в Интернет запустите веб-браузер.
2. Введите адрес **www.cisco.com** и нажмите клавишу <Enter>.
3. На домашней странице сайта выберите ссылки **Products & Services** или **Technologies** (или же воспользуйтесь функцией поиска по сайту – ссылка **Search)** и найдите устройства перечисленных ниже типов, имеющие воз можность работы в ATM-сетях:

- серверы доступа;
- оптические устройства;
- маршрутизаторы;
- коммутаторы.

4. Всю собранную информацию о возможностях ATM-устройств занесите в текстовый файл.

Задание 8-2

В этом задании вы узнаете о том, как в системах Windows 2000 и Window™ XP использовать команду atmadm, позволяющую просматривать коммуникационные параметры для установленного ATM-адаптера.

Для знакомства с командой atmadm в системах Windows 2000 и Windows выполните следующие операции:

В системе Windows 2000 нажмите кнопку **Start** (Пуск) и в меню **Prograngl** (Программы) выберите подменю **Accessories** (Стандартные), а в нем -Д опцию **Command Prompt** (Командная строка). В системе Windows XP нажмите кнопку **Start** (Пуск) и в меню **All Programs** (Все программы) выберите подменю **Accessories** (Стандартные), а в нем – опцию **Сотта Prompt** (Командная строка).

1. В окне команд введите atmadm /? и нажмите клавишу <Enter>.
2. Какие параметры можно использовать? Запишите их в лабораторный журнал или в текстовый файл.
3. Если на вашем компьютере стоит адаптер ATM, подключенный к АТМЯ сети, проверьте в работе все параметры команды atmadm.
4. Закройте окно командной строки.

Задание 8-3

В этом задании вы узнаете, как в системе Windows 2000 вручную установите адаптер ATM, совместимый с LANE.

Для ручной установки адаптера ATM в системе Windows 2000 нужно выпол нить следующие действия:

1. Нажмите кнопку **Start** (Пуск) и в меню **Settings** (Настройка) выберйта пункт **Control Panel** (Панель управления).
2. Дважды щелкните по значку **Add/Remove Hardware** (Установка оборудования).
3. В окне программы Add/Remove Hardware Wizard (Мастер установки оборудования) нажмите кнопку Next (Далее).
4. На следующей странице мастера оставьте предлагаемую по умолчании опцию **Add/Troubleshoot a device** (Добавить/провести диагностику устройства) и нажмите кнопку Next (Далее).
5. Подождите несколько минут, пока мастер пытается обнаружить новое оборудование.
6. На странице "Choose a Hardware Device" ("Выбор устройства") выберите опцию **Add a new device** (Добавление нового устройства) и нажмите кнопку **Next** (Далее).
7. Далее выберите опцию **No, I want to select the hardware from a list** (Нет, выбрать оборудование из списка) и нажмите кнопку Next (Далее).
8. Затем выберите опцию **Network adapters** (Сетевые платы) и нажмите кнопку **Next** (Далее).
9. В списке **Manufacturers** (Изготовители) выберите компанию Eicon Technology.
10. Обратите внимание на то, что один из адаптеров, выпускаемых этим производителем, представляет собой ATM-адаптер, названный "Eicon NDIS LAN Emulation" ("Эмуляция LAN Eicon NDIS"). Почему в системе Windows 2000 важно, чтобы этот адаптер был NDIS-совместимым?
11. Закройте окно мастера, нажав кнопку **Cancel** (Отмена).
12. Закройте окно панели управления.

Задание 8-4

Некоторые телекоммуникационные компании (например, AT&T) предлагают средства для обеспечения взаимодействия сетей frame relay и ATM. В этом задании вы будете знакомиться со службами,

предлагаемыми компанией AT&T.

Для знакомства с предлагаемыми компанией AT&T услугами по связи сетей frame relay и ATM требуются следующие действия:

1. Запустите веб-браузер.
2. Введите адрес **www.att.com** и нажмите клавишу <Enter>. На сайте компании выполните поиск по ключевым словам "frame relay ATM".
3. Какой тип виртуальной сети предлагается?
4. Какие скорости сети frame relay анонсируются?
5. Какие возможности ATM предлагаются?
6. Какие услуги предлагаются в масштабах страны, а какие – в международном масштабе?
7. Занесите полученную информацию в журнал или текстовый файл.
8. Закройте окно браузера.

Задание 8-5

В этом задании вы будете знакомиться с документом, описывающим планирование и реализацию виртуальных локальных сетей на базе сети с коммутацией пакетов.

Чтобы узнать о методах планирования и реализации VLAN-сетей, выполните следующие операции:

1. Запустите веб-браузер.
2. Введите адрес **www.att.com** и нажмите клавишу <Enter>. На сайте компании выполните поиск по ключевой фразе "planning and implementing VLANs".

Какие общие моменты следует учитывать перед тем, как конфигурировать виртуальную локальную сеть?

Какие рекомендации даются в документе относительно безопасности виртуальной локальной сети?

Запишите собранные сведения в журнал или сохраните их в виде текстового файла.

Закройте окно браузера.

Учебные задачи

предлагаемом сценарии вы работаете с колледжем Canyon College *(см. 7)* и компанией One-Stop Office *(см. главу 6)*. Кроме того, у вас появились два новых клиента – взаимодействующие друг с другом компании Digi PrqBuctions и Wild Landscapes. Помимо этого, вы помогаете своему коллеге на несколько вопросов по поводу сетей ATM.

.Колледж Canyon College недавно обновил магистраль своей сети, реализовав ее на базе ATM, и ищет технологию для некоторых глобальны коммуникаций, выбирая между frame relay и SONET.

Компания One-Stop Office, пользуясь вашими рекомендациями, развернула TCP/IP в своей сети, но еще не решила, как осуществлять глобальные коммуникации. В настоящий момент у них имеются вопросы технологиям ATM. Расскажите, какие преимущества могут иметь ATM сети для этой компании. Как она сможет реализовать ATM в уже существующей Ethernet-сети на базе TCP/IP? Можно ли помимо ATM развернуть службу SMDS?

Digi Productions – компанил, предлагающая различные услуги по монтажу фильмов (в т. ч. документальных фильмов о природе, выпускаемых компанией Landscapes). Первая компания находится в Лос Анджелесе (Калифорния), а вторая имеет площадки в Калгари (Канада) Лондоне (Великобритания). Компания Digi Productions располагает EthfHernet-сетью на базе TCP/IP, насчитывающей 200 узлов. Ethernet-ceTffiB компании Wild Landscapes относительно небольшие, работают на TCP/IP и имеют 30 и 50 узлов. Эти компании просят вас решить следующие задачи:

- трафик в сети компания Digi Productions стал чрезмерным, поскольку обрабатываются файлы видео и мультимедиа. Как можно справиться таким большим трафиком?
- предложите способ для организации глобальных коммуникаций между компанией Digi Productions и подразделением компании Wild Land-IBscapes, расположенным в Калгари. Укажите преимущества предложенного решения;
  - создайте блок-схему, иллюстрирующую предложенное решение;

- расскажите, как при помощи глобальной сети можно связать обе площадки компании Wild Landscapes (в Калгари и Лондоне), и опишите достоинства и недостатки выбранного решения;
- создайте блок-схему, иллюстрирующую ваше предложение по организации связи между сетями компании Wild Landscapes.

4. Один из ваших коллег не совсем понимает принципы организации многоуровневых коммуникаций ATM. Расскажите ему об уровнях ATM и о том, как они соотносятся с уровнями эталонной модели OSI.
5. Кроме этого, ваш коллега спрашивает о различиях между постоянными (PVC), коммутируемыми (SVC) и интеллектуальными постоянными вир туальными каналами (SPVC). Расскажите о каждом типе канала. Какие каналы, по вашему мнению, лучше всего применять для организации глобальной сети в тех случаях, когда эта сеть используется периодически?

Дополнительные учебные задачи для групповой работы

1. Компания Network Design Consultants работает с корпоративным заказчиком, у которого имеется звездообразная сеть с 950 узлами, для организации которой в настоящий момент используются коммутаторы и концентраторы Fast Ethernet. Этот клиент хочет развернуть более скоростные сетевые службы – как в магистрали, так и для подключения всех на стольных систем. Одни из ваших коллег утверждают, что имеющуюся сеть нужно преобразовать в сеть Fast Ethernet/Gigabit Ethernet, а другие склоняются в пользу ATM. Организуйте группу для выбора наилучшего решения для описанной ситуации (с точки зрения требуемой скорости и в плане перспектив развития сети в будущем). Изучите и сравните преимущества обоих технологий и подготовьте отчет.
2. Компания Network Design Consultants изучает номенклатуру устройств, пригодных для использования ATM при подключении настольных систем. Соберите команду для анализа оборудования, имеющегося в данное время на рынке и выпускаемого такими производителями сетевых устройств, как 3Com, Asante, Cisco, Intel, Nortel/Bay Networks, а также другими фирмами.

Глава 9

Технологии беспроводных сетей

По прочтении этой главы и после выполнения практических заданий вы сможете:

- рассказать о современных технологиях беспроводных сетей;
- изложить историю развития беспроводных сетей и их преимущества;
- описать технологии радиосетей;
- рассказать о радиосетях стандарта 802.11;
- описать альтернативные технологии радиосетей (такие как Bluetooth, HiperLAN и HomeRF Shared Wireless Access Protocol);
- обсудить беспроводные технологии, использующие инфракрасное излучение;
- рассказать о микроволновых сетях;
- описать беспроводные сети, использующие низкоорбитальные (LEO) спутники Земли.

Беспроводные сети представляют собой развивающуюся технологию, вызывающую большой интерес по многим причинам. Самой очевидной причиной является то, что такие сети обеспечивают мобильность портативных и ручных компьютерных устройств, позволяя пользователю забыть о кабелях. Другая причина состоит в том, что в настоящее время беспроводные технологии стали более надежными и в некоторых ситуациях их развертывание обходится дешевле, чем создание кабельных сетей. Имеется несколько альтернативных кабелю беспроводных сред для передачи сетевых пакетов: радиоволны, инфракрасное (ИК) излучение и микроволны (волны СВЧ-диапазона). При использовании всех перечисленных технологий сигналы передаются по воздуху или в атмосфере, что делает их хорошей альтернативой в тех случаях, когда трудно или невозможно применить кабель.

В этой главе вы познакомитесь со многими типами беспроводных сетевых коммуникаций. Сначала вы узнаете, какие беспроводные сети используются настоящее время, а затем ознакомитесь с краткой историей таких сетей *m* іх преимуществами. После общего описания сетей, использующих радио волны, будет подробнее рассказано о распространенном стандарте беспроводных сетей IEEE 802.11. Также вы узнаете об альтернативных технологиям радиосетей: Bluetooth, HiperLAN и HomeRF Shared Wireless Access Protocol затем будут описаны технологии на базе рассеянного ИК-излучения, обеспечивающие относительно защищенные беспроводные коммуникации , наконец, будет рассказано о том, как в сетях применяются микроволновые технологии на базе наземных и спутниковых каналов (включая сети широко орбитальных спутников Земли).

Современные технологии беспроводных сетей

В настоящее время для создания беспроводных сетей применяются следующие технологии:

- технологии, использующие радиоволны;
- технологии на базе ИК-излучения;
- микроволновые (СВЧ) технологии;
- сети на базе низкоорбитальных спутников Земли (специальный космический проект с

использованием СВЧ-волн).

Технологии, использующие радиоволны, очень распространены и представляют собой быстро растущий сектор беспроводных сетевых коммуникации. Сюда же входит стандарт беспроводных сетей 802.11, а также альтернатив промышленные стандарты, такие как Bluetooth, HiperLAN и HoteShared Wireless Access Protocol (SWAP).

Технологии на базе ИК-излучения не так распространены, как радиосетям однако они имеют некоторые преимущества, поскольку позволяют создавав относительно более защищенные беспроводные сети (т. к. сигнал сложнее перехватить незаметно). Обе технологии (радиоволны и ИК-излучение) используются для организации коммуникаций на малых расстояниям в пределах офиса, здания или между зданиями.

Микроволновые (СВЧ) технологии применяются для связи на больших расстояниях и могут обеспечить сетевые коммуникации между континентами через спутники).
Сети на базе низкоорбитальных спутников являются еще одной разновидностью беспроводных сетей, на основе которых в определенный момента может быть создана "всемирная сеть", доступная во всех точках планеты.
Обо всех перечисленных технологиях будет рассказано в этой главе. Однако сначала мы обратимся к истории развития беспроводных сетей и узнаем об их преимуществах.

Краткая история беспроводных сетей и их достоинства

Историю беспроводных сетей можно рассматривать формально и неформально. Неформальным прародителем беспроводных сетей является любительская радиосвязь, операторы которой получают от Федеральной комиссии связи (FCC) лицензии на передачу речи, азбуки "Морзе, данных, спутниковых и видеосигналов с использованием волн радио- и СВЧ-диа-пазонов. Хотя радиолюбительство обычно считается хобби, Федеральная комиссия связи рассматривает его как важный источник идей и опыта для развития коммуникаций.

Примечание

Радиоволны и СВЧ-волны представляют собой один из диапазонов спектра электромагнитных волн, который включает в себя видимый свет, радиоволны, ИК-излучение, рентгеновские лучи, СВЧ-волны (микроволны) и гамма-лучи. Все это – разновидности электромагнитного излучения, которое распространяется в атмосфере Земли и в космосе. Оно имеет и свойства волны, и свойства частицы. Дополнительную информацию о спектре электромагнитных волн можно найти по адресам

http://imagine.gsfc.nasa.gov/docs/science/knowJ1/emspectrum.html и http://imagine.gsfc.nasa.gov/docs/science/knowJ2/emspectrum.html.

В 1980-х годах лицензированные радиолюбители получили от Федеральной комиссии связи разрешение на передачу данных на нескольких радиочастотах в диапазонах от 50,1–54,0 МГц (нижний диапазон) до 1240–1300 МГц (верхний диапазон). Большинству людей эти частоты знакомы, т. к. они используются для передачи музыки радиостанциями AM- и FM-диапазонов. Эти частоты представляют собой лишь малую часть возможных радиочастот, на которых можно передавать сигналы. Основной единицей измерения радиочастоты является *герц (Гц)* (Hertz (Hz)). В технике одному герцу соответствует один период переменного напряжения или излученного сигнала за секунду.

Примечание

Радиочастоты представляют диапазон волн с частотой свыше 20 кГц, с помощью которых электромагнитный сигнал может излучаться в пространство.

С тех пор, когда в начале 1980-х годов компания IBM создала персональный компьютер, прошло немало времени, пока радиолюбители не связали персональные компьютеры в сеть, используя радиоволны (обычно в более высоких диапазонах 902–928 МГц и 1240–1300 МГц). Для этого они создал устройство, названное контроллером терминального узла (terminal node controller, TNC). Это устройство

помещалось между компьютером и приемопередатчиком и служило для преобразования компьютерного цифрового сала в аналоговый сигнал, усиливаемый приемопередатчиком и излучаемый через антенну. Полученная в результате технология была названа пакетной радиосвязью. Обнаруженный радиолюбителями факт, что пакетная радиосвязь хорошо работает на частотах 902 МГц и выше, был вскоре проанализирован компаниями, предоставляющими коммерческие услуги беспроводных сетей. В 1985 году Федеральная комиссия связи разрешила для коммерческого использования в беспроводных компьютерных сетях частотой для промышленных, научных и медицинских приложений (Industrial, ScietfJtitle and Medical, ISM), которые можно применять для маломощных нелицензируемых общедоступных коммуникаций на фиксированных частотах» диапазоне от 902 МГц до 5,825 ГГц. В Телекоммуникационном а 1996 года Конгресс подготовил следующий этап в развитии беспроводный! коммуникаций, закрепив понятие "узел (местоположение) беспроводной связи" и установив для нее стандарты, а также создав стимулы для дальнейшего развития телекоммуникационных технологий, в т. ч. и беспроводный коммуникаций (дополнительную информацию можно найти по адрес www.fcc.gov/telecom.html). Вскоре после этого институт IEEE создал групп по стандартам беспроводных сетей 802.11, которая отвечала за первый стандарт 802.11, установленный в 1997 году. В настоящее время беспроводный сети разрабатываются и внедряются для обеспечения многих потребностей в числе которых можно назвать следующие:

- реализация коммуникаций в тех областях, где сложно развернуть кабельную сеть;
- снижение затрат на развертывание;
- обеспечение "произвольного" доступа тем пользователям, которые не могут быть привязаны к определенному кабельному подключению;
- упрощение процедуры создания сетей в небольших и домашних офисах;
- обеспечение доступа к данным, необходимым в конкретной конфигурации

Почему кабельные сети можно использовать не всегда?

В некоторых ситуациях кабельную сеть развернуть сложно и даже невозможно. Рассмотрим такой сценарий. Два здания нужно связать одной сетью однако между ними проходит федеральное шоссе. В таком случае имеется несколько способов организации сети. Во-первых, можно прорыть траншею под шоссе, для чего потребуются большие расходы и перерывы в движении, вызванные рытьем траншеи, прокладкой кабеля, закапыванием траншеи и полным восстановлением дороги. Во-вторых, можно создать региональную сеть, связывающую два здания. Здания можно подключить к линиям Т-1 или к региональной сети Optical Ethernet, воспользовавшись услугами владельца сети общего пользования или местной телефонной компании. Затраты при этом будут меньше, чем при прокладке нового кабеля, однако аренда телекоммуникационных линий потребует постоянных отчислений. В-третьих, можно развернуть беспроводную сеть, для чего понадобятся единовременные расходы на оборудование, а также появятся текущие издержки на управление сетью. Однако все эти затраты будут, скорее всего, наиболее оправданы, если рассматривать большие отрезки времени.

Рассмотрим еще один сценарий. Арендатору большого офиса необходимо развернуть сеть для 77 сотрудников. Владелец помещения запрещает прокладывать постоянную кабельную систему. Данное помещение во всех смыслах устраивает арендатора, кроме того, плата за него ниже, чем в других альтернативных вариантах. Решением проблемы будет создание беспроводной сети.

И, наконец, третий сценарий. Общедоступная библиотека располагается в историческом месте. Несмотря на то, что эта библиотека принадлежит городу, строгие общественные и частные договоры не позволяют руководству библиотеки получить необходимое разрешение на прокладку сетевого кабеля. Библиотека на много лет отстала в создании электронного каталога книг, поскольку не может связать в сеть компьютеры своих сотрудников и справочную службу для своих клиентов. Поэтому руководство библиотеки может решить свои проблемы, развернув беспроводную сеть, позволяющую сохранить целостность здания и не нарушать никакие договоры.

Экономия средств и времени при использовании беспроводных сетей

Затраты и время на создание беспроводной сети могут оказаться меньшими, чем на развёртывание кабельной сети. Например, в старых зданиях часто имеются опасные материалы, скажем, в старых эксплуатационных шахтах, содержащих ничтожное количество хлора, выделяющегося из

воздуховодов и асбеста. Поскольку шахты не используются, их можно просто замуровать. Или же можно начать дорогостоящую программу по удалению опасных материалов, чтобы эти шахты можно было использовать для прокладки сетевого кабеля. В такой ситуации намного дешевле замуровать шахты и вместо кабеля развернуть беспроводную сеть.

Можно рассмотреть случай, когда одному университету потребовалась рабочая сеть, поскольку в его развитие были вложены крупные средства. Университет пригласил дорогую консалтинговую компанию, которая выделила
на проект пять человек и организовала 18 новых рабочих мест. За несколько дней до начала работ руководство университета поняло, что для новых сотрудников и консультантов нет сетевых подключений. Прокладывать новые кабели дорого, да к тому же и невозможно в ближайшие несколько месяцев поскольку IT-отдел университета уже перегружен работой. Выход найден в виде беспроводной сети, которая может быть развернута в рекордно короткое время.

Неограниченный доступ к сети

Некоторым пользователям компьютеров доступ к сети нужен практически из любой точки. Рассмотрим, к примеру, большой склад автомобильных частей, в котором необходимо регулярно проводить ревизии, используя СЩ меры штрих-кодов, подключаемые к сети. Беспроводная сеть дает пользователям таких сканеров возможность неограниченного доступа, поскольку пользователи не привязаны к кабельным подключениям. Еще один пример Врач в больнице может носить с собой небольшой портативный компьютер с адаптером беспроводной связи, с помощью которого можно обновлять иа истории болезни, выписывать направления на анализы или организовывая уход за больными.

Упрощение сетевых технологий для новичков

В сфере компьютеризации небольших или домашних офисов беспроводной сетью, на голову выше кабельной разводки. Сети таких офисов могут быть весьма неудовлетворительном состоянии, поскольку они обычно создаются непрофессионалами. В результате может быть выбран кабель не того типа. Кабель может проходить мимо источников радиопомех и электромагнитных излучения или он может оказаться поврежденным (например, передавши под стулом, столом или в дверном проеме). Поэтому пользователя таком офисе может непродуктивно тратить свое время на поиски неработоспособности сети. В такой ситуации беспроводная сеть может оказаться проще в установке и эксплуатации. Как правило, во многих онлайновых компьютерных магазинах пользователей небольших и домашних офисах спрашивают о том, не хотят ли они приобрести беспроводные устройства для организации сети между купленными компьютерами.

Достоинством беспроводных сетей для такого класса пользователей являет то, что в настоящее время стоимость беспроводных устройств вполне умеренная. Беспроводная сеть в сочетании с возможностью автоматическая назначения IP-адресов в системах Windows 2000 и Windows XP позволяв создать полноценную домашнюю сеть при наличии минимального опыта или даже при его отсутствии.

Совершенствование доступа к данным

Беспроводные сети позволяют значительно усовершенствовать доступ к некоторым типам данных и прикладным программам. Рассмотрим для примера большой университет, в котором на постоянной основе работают десять аудиторов, посещающих каждый день по нескольку подразделений (и площадок) и нуждающихся в доступе к финансовым данным, отчетам и другой информации, имеющейся в этих подразделениях. При наличии портативного компьютера, снабженного адаптером беспроводной сети, аудитор может легко перемещаться между площадками и иметь постоянный доступ к любым финансовым документам. В качестве другого примера можно рассмотреть инженера-химика, работающего в разных точках химического завода. В одной точке он может наблюдать за данными в ходе некоторой реакции производственного цикла. В другой точке ему может потребоваться номенклатура химикатов, чтобы убедиться в наличии компонентов, нужных для запуска другого производственного процесса. В третьей точке этот инженер может обратиться к онлайновой научной библиотеке компании. Беспроводный доступ позволит ему легко справиться со всеми перечисленными задачами.

Организации, поддерживающие технологии беспроводных сетей

Существует несколько организаций, занимающихся продвижением беспроводных сетей. Одной из таких организаций, являющейся ценным источником информации по беспроводным сетям, является *Wireless LAN Association (WLANA)*. Эта ассоциация образована производителями устройств беспроводных сетей, а также заинтересованными компаниями и организациями, в числе которых Alvarion, Cisco Systems, ELAN, Intermec, Intersil, Raylink и Wireless Central. Выполните практическое задание 9-1 и познакомьтесь с ситуациями, в которых можно использовать беспроводные локальные сети, а также с информационными ресурсами, предлагаемыми ассоциацией WLANA.

WINLAB (Wireless Information Network Laboratory) – это расположенный в Университете Рутжерса (Rutgers University) центр исследований в области беспроводных сетей, поддерживаемый несколькими университетами. WINLAB спонсируется из фондов National Science Foundation и работает, начиная с 1989 года. Выполнив практическое задание 9-2, вы узнаете о самых последних исследованиях, выполненных лабораторией WINLAB.

Технологии радиосетей

Сетевые данные передаются с помощью радиоволн подобно тому, как вещает местная радиостанция, однако для сетевых приложений используются волны
гораздо более высоких частот. Например, местная радиостанция AM-диапазона (средние и длинные волны) может вести вещание на частоте 1290 кГц, поскольку интервал частот для широковещания с амплитудной модуляцией составляет 535–1605 кГц. Интервал частот для FM-вещания (УКВ) имеет границы 88–108 МГц. В США сетевые сигналы передаются на более высоких частотах в интервалах 902-928 МГц, 2,4–2,4835 ГГц или 5-5,825 ГГц.

Примечание

Каждый из упомянутых интервалов частот также называется диапазоном: диапазон 902 МГц, диапазон 2,4 ГГц и диапазон 5 ГГц. Диапазон 902 МГц в первую очередь используется в старых нестандартизованных беспроводных устройствах и далее в книге не рассматривается.

В радиосетях сигнал передается в одном или нескольких направлениях в зависимости от типа используемой антенны. В примере, изображенном на рис. 9.1, сигнал является направленным, поскольку он передается от антенны, расположенной на одном здании, к антенне, расположенной на другом здании. Волна имеет очень малую длину и небольшую мощность (если оператор связи не имеет специальной лицензии от Федеральной комиссии связи на многоваттные коммуникации), т. е. она лучше всего подходит для *передач в пределах прямой видимости* (line-of-sight transmission) с малым радиусом действия.

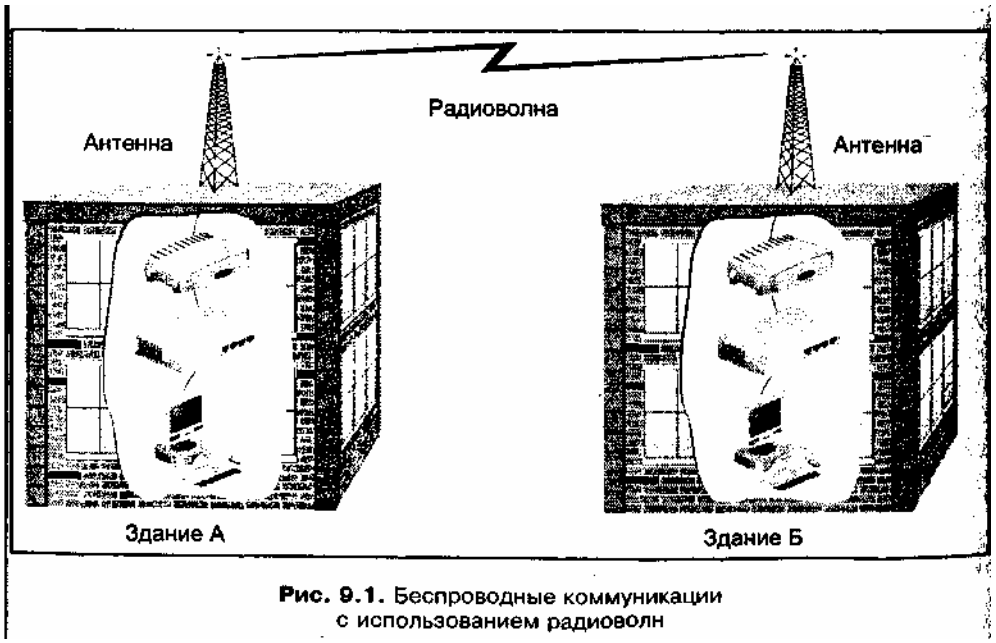


Рис. 9.1. Беспроводные коммуникации с использованием радиоволн

При передаче в пределах прямой видимости сигнал передается от одной точки к другой, следуя искривлению Земли, а не отражается от атмосферы, пересекая страны и континенты. Недостатком

такого типа передачи является наличие преград в виде больших возвышенностей на поверхности Земли (например, холмы и горы). Маломощный (1 – 10 Вт) радиосигнал может передавать данные со скоростью от 1 до 54 Мбит/с и даже выше.

Для передачи пакетов в оборудовании беспроводных радиосетей чаще всего используется технология работы с расширенным спектром (spread spectrum technology), когда для передачи сигнала с большей полосой пропускания задействуются одна или несколько смежных частот. Интервал частот с расширенным спектром очень высок: 902–928 МГц и намного выше. Коммуникации с расширенным спектром обычно обеспечивают передачу данных со скоростью 1–54 Мбит/с.

Коммуникации с использованием радиоволн позволяют сэкономить средства в тех случаях, когда сложно или очень дорого прокладывать кабель. Радиосети особенно полезны, когда используются портативные компьютеры, которые часто перемещаются. По сравнению с другими беспроводными технологиями, радиосети относительно недороги и просты в установке.

Использование радиоволн в коммуникациях имеет несколько недостатков. Многие сети передают данные со скоростью 100 Мбит/с и выше для организации высокоскоростных коммуникаций при пересылке большого трафика (в том числе и больших файлов). Радиосети пока не могут обеспечить коммуникации с такой скоростью. Другим недостатком является то, что некоторые частоты беспроводной связи используются совместно радиолюбителями, военными и операторами сотовых сетей, в результате чего на этих частотах возникают помехи от различных источников. Естественные препятствия (например, холмы) также могут уменьшить или исказить передаваемый сигнал.

Одна из основных технологий радиосетей описана стандартом IEEE 802.11. Также используются и другие технологии, в число которых входят Bluetooth, HiperLAN и HomeRF Shared Wireless Access Protocol (SWAP). Все эти технологии будут рассмотрены в следующих разделах этой главы.

Радиосети стандарта IEEE 802.11

Для реализации беспроводных коммуникаций используются различные типы радиосетей, однако в плане совместимости и надежности значительные преимущества имеет стандарт IEEE 802.11. Многие пользователи беспроводных сетей применяют устройства, отвечающие этому стандарту, поскольку такие устройства не связаны с нестандартизованными коммуникациями (особенно в нижнем и медленном диапазоне 902–928 МГц, типичном для старых беспроводных устройств) и устройства стандарта 802.11, выпущенные разными производителями, являются взаимозаменяемыми. Такие устройства отвечают открытому стандарту, поэтому различные модели могут взаимодействовать друг с другом, и в них легче реализовать новые функции беспроводной связи. Поэтому разработчику беспроводных сетей важно понимать стандарт IEEE 802.11 и принципы работы устройств, соответствующих этому стандарту.

Стандарт IEEE 802.11 также носит название IEEE Standard for Wireless LANledium Access (MAC) and Physical Layer (PHY) Specifications. Этот стандарта распространяется на стационарные и мобильные станции беспроводным коммуникаций. Стационарной называется станция, которая не перемещается мобильной называется станция, которая может перемещаться быстро, или медленно, как шагающий человек.

Стандарт 802.11 предусматривает два типа коммуникаций. Первый тип синхронные коммуникации, когда передача данных происходит отдельны блоками, начало которых отмечено стартовым разрядом, а конец – стоповым разрядом. Ко второму типу относятся коммуникации, осуществляет в определенных временных рамках, когда сигналу дается определенной для достижения точки назначения, а если сигнал не укладывается Я >то время, то он считается потерянным или искаженным. Временные ограничения делают стандарт 802.11 похожим на стандарт 803.11, согласно которому сигнал также должен достигнуть заданного целевого узла за указанной время. Стандарт 802.11 предусматривает поддержку служб управления сеть пример, протокола SNMP). Также обеспечивается аутентификация сети, стандарт 802.11 ориентирован на использование Канального и Физического уровней модели OSI. На MAC- и LLC-подуровнях Канального уровня определены стандарты на метод доступа (о котором будет рассказано далее этой главе), адресацию и способы проверки данных с использованием контрольных сумм (CRC). На Физическом уровне стандарт 802.11 определял скорости передачи данных на заданных частотах. Также предусмотрены методы (например, технологии с расширенным

спектром) для передачи цифровых сигналов с помощью радиоволн и ИК-излучения.

С точки зрения рабочей среды стандарт 802.11 различает беспроводный коммуникации в помещении (комнатные) и на открытом воздухе (наруби). Комнатные коммуникации могут, к примеру, осуществляться в здания офиса, промышленной зоне, магазине или частном доме (т. е. везде, где не распространяются дальше отдельного здания). Наружные коммуникаций могут выполняться в пределах университетского кампуса, спортивной площадки или автостоянки (т. е. там, где передача информации ведется меж зданиями). Далее вы познакомитесь со следующими аспектами, касающимися функционирования беспроводных сетей стандарта 802.11:

- беспроводные компоненты, используемые в сетях IEEE 802.11;
- методы доступа в беспроводных сетях;
- способы обнаружения ошибок при передаче данных;
- коммуникационные скорости, используемые в сетях IEEE 802.11;
- методы обеспечения безопасности;
- использование аутентификации при разрыве соединения;
- топологии сетей IEEE 802.11;
- использование многоячеечных беспроводных локальных сетей.

Компоненты беспроводной сети

В реализации беспроводных коммуникаций обычно участвуют три основных компонента: плата, выполняющая функции приемника и передатчика (трансивера), точка доступа и антенны.

Плата трансивера называется *адаптером беспроводной сети* (wireless NIC, WNIC), который функционирует на Физическом и Канальном уровнях модели OSI. Большинство таких адаптеров совместимы со спецификациями Network Interface Specification, NDIS (компания Microsoft) и Open Datalink Interface, ODI (компания Novell). Как вы уже знаете из *главы 5,* обе эти спецификации позволяют передавать по сети несколько протоколов и служат для связи компьютера и его операционной системы с WNIC-адаптером.

Тонка доступа (access point) представляет собой некоторое устройство, подключенное к кабельной сети и обеспечивающее беспроводную передачу данных между WNIC-адаптерами и этой сетью. Как говорилось в *главе 4,* точка доступа обычно является мостом. Она может иметь один или несколько сетевых интерфейсов перечисленных ниже типов, позволяющих подключить ее к кабельной сети:

- AUI;
- 10Base2;
- 10BaseT;
- 100BaseTX, 100BaseT, 100BaseT2 и 100BaseT4;
- FDDI.

Совет

В настоящее время некоторые поставщики беспроводных сетей предлагают точки доступа с возможностями маршрутизаторов.

Антенна – это устройство, посылающее (излучающее) и принимающее радиоволны. И WNIC-адаптеры, и точки доступа оборудованы антеннами. Большинство антенн беспроводных сетей являются или направленными, или всенаправленными.

Совет

При покупке устройств стандарта 802.11 посмотрите, сертифицированы ли они союзом Wireless Ethernet Compatibility Alliance (WECA), в который входят свыше 150 компаний, выпускающих беспроводные устройства. Более подробную ин формацию об этом союзе можно получить на веб-сайте **www.wi-fi.com.**

Направленная антенна

Направленная антенна посылает радиолучи в одном главном направлении обычно может усиливать

излучаемый сигнал в большей степени, чем всенаправленная антенна. Величина усиления излученного сигнала называется *коэффициентом усиления* (gain). В беспроводных сетях направленные антенна обычно применяются для передачи радиоволн между антеннами, располагающимися на двух зданиях и подключенными к точкам доступа (рис. 9.2) такой конфигурации направленная антенна обеспечивает передачу на больших расстояниях по сравнению с всенаправленной антенной, поскольку она, вероятнее всего, излучает более сильный сигнал (с большим коэффициентом усиления) в одном направлении. Рассматривая рис. 9.2, обратите внимание на то, что на самом деле антенна излучает сигнал не только в одном правлении, т. к. часть сигнала рассеивается по сторонам.

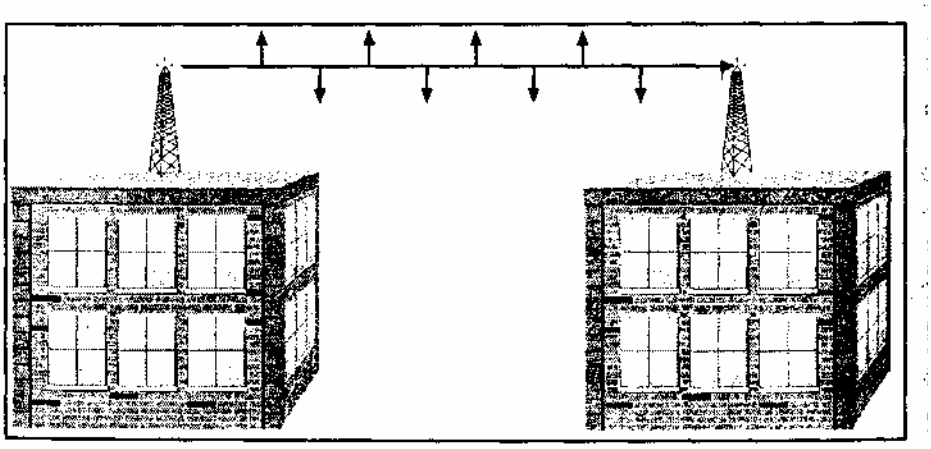


Рис. 9.2. Направленные антенны

Примечание

Для знакомства с компонентами беспроводных сетей выполните практическое задание 9-3. Кроме того, в практических заданиях 9-4 и 9-5 рассказывается о том, как установить WNIC-адаптер в системах Windows 2000 и Windows XP Professional. В практическом задании 9-6 вы узнаете о том, как установить там кой адаптер в системе Red Hat Linux *7.x.*

Всенаправленная антенна

Всенаправленная антенна излучает радиоволны во всех направлениях. Поскольку сигнал рассеивается больше, чем при использовании направленной антенны, он, по всей видимости, будет иметь и меньший коэффициент усиления. В беспроводных сетях всенаправленные антенны часто применяются в комнатных сетях, в которых пользователи постоянно перемешаются и сигналы нужно передавать и принимать во всех направлениях. Кроме того, в таких сетях, как правило, не нужно, чтобы коэффициент усиления сигнала был таким же высоким, как в наружной сети, поскольку расстояния между беспроводными устройствами в помещении намного меньше. На рис. 9.3 показана беспроводная сеть, использующая всенаправленные антенны

Рис. 9.3. Всенаправленные антенны

WNIC-адаптер для портативных устройств (например, портативных, карманных и планшетных компьютеров) может снабжаться небольшой схемной всенаправленной антенной. Точка доступа для локальной комнатной сети может иметь съемную всенаправленную антенну или же антенну, подключаемую к точке доступа с помощью кабеля. Точка доступа для наружной сети, соединяющей два здания, обычно имеет антенну с высоким коэффициентом усиления, которая подключается к точке доступа по кабелю.

Методы доступа в беспроводных сетях

Стандарт 802.11 предусматривает два метода доступа: доступ в порядке приоритетов и множественный доступ с контролем несущей и предотвращен ем конфликтов. Оба этих метода работают на Канальном уровне.

При использовании *доступа в порядке приоритетов* (priority-based access точка доступа также выполняет функции точечного координатора, который задает период без возникновения конфликтов, в течение которого станций) (помимо самого координатора) не могут работать на передачу, не обратившись сначала к координатору. В течение этого периода координатор поочередно опрашивает

станции. Если некоторая станция посылает короткий пакет, указывающий на то, что ее нужно опросить, поскольку у нее имеет сообщение на передачу, точечный координатор помещает эту станцию свой опросный лист. Если некоторая станция не опрашивается, координатор посылает ей сигнальный фрейм, указывающий на то, сколько нужно ждать до начала следующего периода без возникновения конфликтов. этого станции, входящие в опросный лист, поочередно получают право осуществление коммуникаций. Когда все эти станции получили возможность передать данные, сразу же задается следующий период без возникновения конфликтов, в течение которого координатор снова опрашивает укажет станцию, определяя необходимость включения в опросный лист станции ждущих возможности передачи.

Доступ в порядке приоритетов предназначается для коммуникаций, требующих малых задержек пересылки информации. К таким типам коммуникаций обычно относится передача речи и видеоизображений, а также организация видеоконференций – т. е. такие приложения, которые лучше всего работают в непрерывном режиме. Согласно стандарту 802.11 доступ в рядке приоритетов также называется *функцией точечной координации*

Чаще в беспроводных сетях применяется *множественный доступ с контролем несущей и предотвращением конфликтов* (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA), который также называется *функции распределенной координации* (distributed coordination function). В этом случае станция, ожидающая возможности передачи, прослушивает частоту коммуникаций и определяет ее занятость, проверяя уровень индикатора мощности сигнала в приемнике (Receiver Signal Strength Indicator, RSSI). В 14 момент, когда передающая частота свободна, наиболее вероятно конфликтов между двумя станциями, которые одновременно захотят начать передачу. Как только передающая частота освобождаете! каждая станция ждет несколько секунд (число которых определяется параметром DIPS), чтобы убедиться в том, что частота остается незанятой. DIFS – это аббревиатура от термина Distributed coordination function's In-tra-Frame Space (интервал между фреймами функции распределенной координации), который определяет заранее установленное время обязательного ожидания (задержки).

Если станции ожидают в течение времени, определенного интервалом DIFS, вероятность возникновения конфликта между станциями уменьшается, поскольку для каждой станции, требующей передачи, вычисляется разное значение времени задержки (отсрочки), по истечении которого станция снова будет проверять занятость передающей частоты. Если частота остается незанятой, то передачу начинает станция, имеющая минимальное время отсрочки. Если частота оказывается занятой, то станция, требующая передачи, ждет пока частота не освободится, после чего простаивает еще в течение уже вычисленного времени отсрочки.

При определении времени отсрочки длительность заранее заданного интервала времени умножается на случайное число. Временной интервал – это некоторое значение, хранящееся в базе управляющей информации (MIB), имеющейся на каждой станции. Значение случайного числа лежит в диапазоне от нуля до величины максимального размера окна конфликтов, который также хранится в базе управляющей информации станции. Таким образом, для каждой станции, ожидающей передачи, определяется уникальное время отсрочки, что позволяет станциям избегать конфликтов.

Обработка ошибок передачи данных

Коммуникации в беспроводных сетях зависят от погодных условий, солнечных бликов, других беспроводных коммуникаций, естественных препятствий и других источников помех. Все эти помехи могут нарушить успешный прием данных. Стандартом 802.11 предусмотрен *автоматический запрос на повторение* (automatic repeat-request, ARQ), который позволяет учитывать возможность появления ошибок передачи.

Если при использовании ARQ-запросов станция, отправившая пакет, не получает подтверждения (ACK) от целевой станции, то она автоматически повторяет передачу пакета. Количество повторов, сделанных передающей станцией до того момента, как она определит невозможность доставки пакета, зависит от размера пакета. Каждая станция хранит две величины: максимальный размер короткого пакета и размер длинного пакета. Кроме этого, имеются два дополнительных параметра: количество повторов для отправки Короткого пакета и количество повторов для длинного пакета. Анализ всех этих значений позволяет станции принять решение о прекращении повторных передач некоторого пакета.

В качестве примера обработки ошибок с использованием ARQ-запросов рассмотрим станцию, для

которой короткий пакет имеет максимальную длину 776 байт, а количество повторов для короткого пакета равно 10. Допустим, что станция передает пакет длиной 608 байт, но не получает подтверждения от принимающей станции. В этом случае передающая станция будет 10 раз передавать этот пакет повторно при отсутствии подтверждения. После 10 неудачных попыток (т. е. не получив подтверждения) станция прекратит передавать этот пакет.

Скорости передачи

Скорости передачи и соответствующие частоты сетей 802.11 определяются двумя стандартами: 802.11a и 802.1111b. Коммуникационные скорости, указанные в этих стандартах, относятся к Физическому уровню модели OSI.

Для беспроводных сетей, работающих в диапазоне 5 ГГц, стандарт 802.11 предусматривает следующие скорости передачи данных:

- 6 Мбит/с;
- 24 Мбит/с;
- 9 Мбит/с;
- 36 Мбит/с;
- 12 Мбит/с;
- 48 Мбит/с;
- 18Мбит/с;
- 54 Мбит/с.

Примечание

Все устройства, отвечающие стандарту 802.11a, должны поддерживать скорости 6, 12 и 24 Мбит/с. Стандарт 802. Па реализуется на Физическом уровне модели OSI и для передачи информационных сигналов с использованием радиоволн предусматривает применение *ортогонального мультиплексирования каналов, разделенных частоте* (Orthogonal Frequency Division Multiplexing, OFDM). При работе данному методу мультиплексирования 5-гигагерцовый диапазон частот делится на 52 субнесущие (52 подканала). Данные разбиваются между этими субнесущими и передаются одновременно по всем 52 субнесущим. Такие передачи называются параллельными. Четыре субнесущих используются для управления коммуникациями, а 48 передают данные. Стандарт 802.11b используется в диапазоне частот 2,4 ГГц, им предусмотрены следующие коммуникационные скорости:

- 1 Мбит/с;
- 10Мбит/с;
- 2 Мбит/с;
- 11Мбит/с.

Примечание

На момент написания книги ожидалось утверждение расширения стандарта 802.11Ь, получившее название 802.11 д. Стандарт 802.11д позволяет передавать данные в диапазоне 2,4 ГГц со скоростями до 54 Мбит/с.

В стандарте 802.11b используется *модуляция с прямой последовательностью и расширенным спектром* (Direct sequence spread spectrum modulation, DSSS), которая представляет собой способ передачи информационных сигналов с применением радиоволн и относится к Физическому уровню. При DSSS-модуляции данные распределяются между несколькими каналами (общим числом до 14), каждый из которых занимает полосу 22 МГц. Точное число каналов и их частоты зависят от страны, в которой осуществляются коммуникации. В Канаде и США используются 11 каналов в диапазоне 2,4 ГГц. В Европе число каналов равно 13, за исключением Франции, где задействуются только 4 канала. Информационный сигнал передается поочередно в каналы и усиливается до значений, достаточных для превышения уровня помех.

На момент написания книги стандарт 802.11a предлагал большие скорости, чем стандарт 802.11b. Однако увеличение скорости достигается за счет уменьшения рабочих расстояний. В настоящее время устройства стандарта 802.11a могут передавать данные на расстояние до 18 м, в то время как устройства стандарта 802.11b работоспособны на расстояниях до 90 м. Это означает, что если вы используете устройства 802.На, то для увеличения общей рабочей зоны взаимодействующих устройств вам нужно будет приобрести больше точек доступа.

Помимо скорости, преимуществом стандарта 802. Па является то, что полный интервал имеющихся для него частот диапазона 0,825 ГГц почти в два раза превышает интервал частот диапазона 0,4835 ГГц для стандарта 802.11b. Это означает, что в процессе вещания можно передать намного больше данных, поскольку чем шире интервал частот, тем больше информационных каналов, по которым передаются двоичные данные.

Для приложений, требующих большей полосы пропускания (например, для передачи речи и видеоизображений) планируйте использование устройств стандарта 802. Па. Кроме того, рассматривайте возможность применения таких устройств в тех ситуациях, когда в пределах небольшой зоны (например, в компьютерной лаборатории) имеется большое количество пользователей. Более высокая полоса пропускания позволит всем клиентам сети работать лучше и быстрее.

Область применения устройств стандарта 802.11b охватывает те конфигурации, когда наличие высокой полосы пропускания не столь важно (например, для коммуникаций, предназначенных преимущественно для передач данных). Кроме того, стандарт 802.11b хорошо подходит для малобюджетных проектов, поскольку для него нужно меньше точек доступа, чем при использовании стандарта 802.11a. Это объясняется тем, что стандарт 802.11a обеспечивает более широкую рабочую зону (до 90 м против 18 м, допускаемых стандартом 802.11a). В настоящее время стандарт 802.11b используется чаще, чем 802.11a, поскольку сети на его основе дешевле в реализации, а на рынке более широко представлена номенклатура предназначенных для нее устройств (выпуск которых, к тому же, был начат раньше). Характеристик стандартов 802.11a и 802.11b представлены в табл. 9.1.

Таблица 9.1. *Характеристики стандартов 802.11a и 802.11b*

	802.11 a	**802.11Ь**
Рабочая частота	5 ГГц	2,4 ГГц
Рабочие скорости (полоса пропускания)	6, 9, 12, 18, 24, 36, 48, 54 Мбит/с	1, 2, 10, 11 Мбит/с
Метод коммуникаций	Ортогональное мультиплексирование деления частоты (Orthogonal Frequency Division spread spectrum Multiplexing, OFDM)	Модуляция с прямой последовательностью и расширенным спектром (Direct sequence modulation DSSS)
Максимальное рабочее расстояние в настоящее время	18,18м	90м
Стоимость реализации	Относительно высокая из-за необходимости в дополнительных точках доступа	Относительно низкая из-за использования небольшого количества точек доступа

Методы обеспечения безопасности,

Безопасность так же важна в беспроводных сетях, как и в кабельных. Стандарт 802.11 предусматривает два механизма обеспечения безопасности: аутентификацию открытых систем и аутентификацию с общим ключом. При использовании аутентификации открытых систем (open system authentication) любые две станции могут аутентифицировать друг друга. Передающая станция попросту посылает целевой станции или точке доступа запрос: на аутентификацию. Если целевая станция подтверждает запрос, это означает завершение аутентификации. Такой метод аутентификации не обеспечивает достаточной безопасности, и вы должны знать, что в устройствах,

выпускаемых многими производителями, он используется по умолчанию.

Гораздо лучшую защиту обеспечивает *аутентификация с общим ключом* (shared key authentication), поскольку в ней реализуется *Wired Equivalent Privacy (WEP).* При использовании этого механизма защиты две станции (например, WNIC-адаптер и точка доступа) работают с одним и тем же ключом шифрования, генерируемым WEP-службами. Ключ шифрования WEP представляет собой некий 40- или 104-битный ключ с добавлением контрольной суммы и инициирующей информации, что в результате определяет общую длину ключа, равную 64 или 104 разрядам.

При использовании аутентификации с общим ключом и WEP одна станция обращается к другой с запросом на аутентификацию. Вторая станция отсылает обратно некоторый специальный текстовый запрос. Первая станция шифрует его с помощью ключа шифрования WEP и посылает зашифрованный текст второй станции, которая расшифровывает его, используя тот же самый WEP-ключ, и сравнивает полученный текст с посланным изначально текстовым запросом. Если оба текста совпадают, вторая станция аутентифицирует первую и коммуникации продолжаются.

Использование аутентификации при разрыве соединения

Еще одной функцией аутентификации является разрыв соединения после того, как заканчивается сеанс коммуникаций. Процесс аутентификации при разрыве соединения важен потому, что две взаимодействующие станции не могут быть случайно разъединены другой, не аутентифицированной, станцией. Соединение между двумя станциями разрывается, если одна из них посылает извещение об отказе в аутентификации. В этом случае коммуникации мгновенно прекращаются.

Топологии сетей IEEE 802.11

Стандартом 802.11 предусмотрены две основные топологии. Самой простой является *топология с набором независимых базовых служб* (Independent Basic Service Set (IBSS) topology), образуемая двумя или несколькими станциями беспроводной связи, которые могут взаимодействовать друг с другом. Сеть такого типа в некоторой степени непредсказуема, поскольку новые станции часто появляются неожиданно. IBSS-топология образуется произвольными одноранговыми (равноправными) коммуникациями между WNIC-адаптера ми отдельных компьютеров (рис. 9.4).

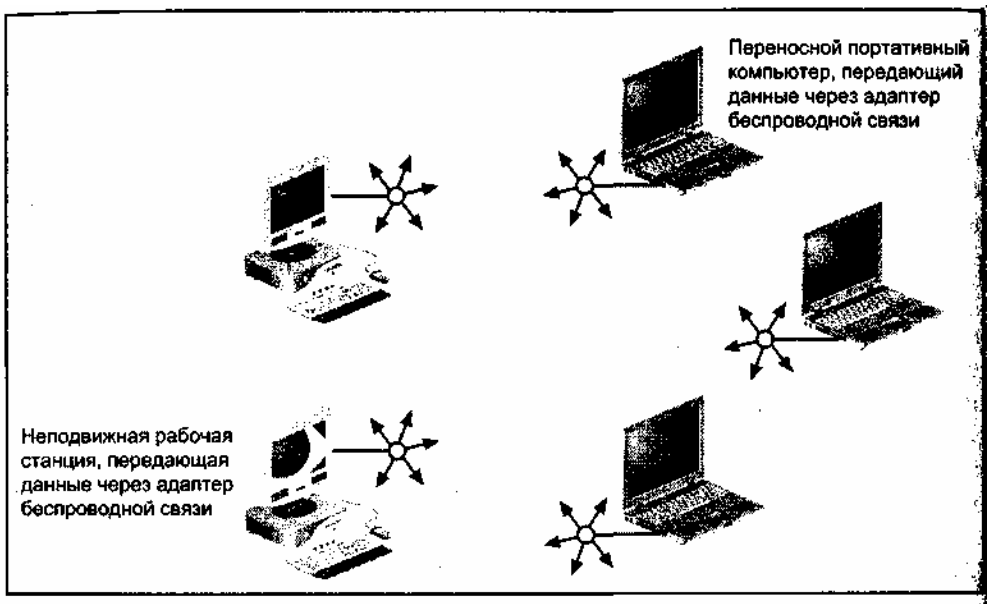


Рис. 9.4. Беспроводная топология IBSS

По сравнению с IBSS-топологией, *топология с расширенным набором* (Extended service set (ESS) topology) имеет большую область обслуживание т. к. в ней имеется одна или несколько точек доступа. На базе ESS-топологии можно создать небольшую, среднюю или большую сеть и значительна! расширить зону беспроводных коммуникаций. ESS-топология показана рис. 9.5.

Если вы используете устройства, совместимые со стандартом 802.11, сеть и IBSS-топологией несложно преобразовать в сеть на основе ESS-топологии. Однако не следует сети с разными

топологиями располагать поблизости, т. к. одноранговые IBSS-коммуникации ведут себя нестабильно в присутствии точек доступа, используемых в ESS-сети. Также могут нарушиться коммуникации и в ESS-сети.

Совет

Дополнительную информацию о стандарте IEEE 802.11 можно получить на веб-сайте IEEE по адресу www.ieee.org. На этом сайте можно заказать полную копию этого стандарта.

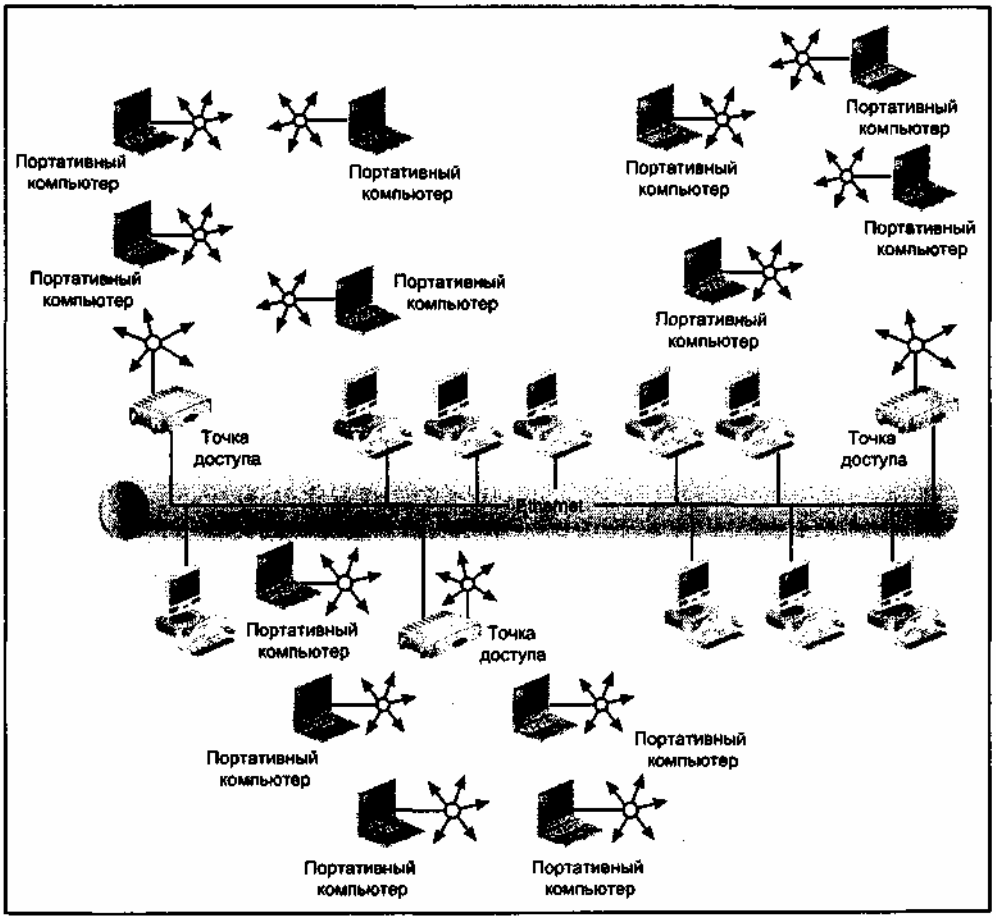


Рис. 9.5. Беспроводная топология ESS

Многоячеечные беспроводные локальные сети

Когда в сети на основе ESS-топологии используются две или несколько точек доступа, такая сеть превращается в *многоячеечную беспроводную локальную сеть* (multiple-cell wireless LAN). Широковещательная область вокруг некоторой точки в такой топологии называется *ячейкой* (cell). Если, к примеру, комнатная сеть внутри здания имеет пять точек доступа, то в этой сети пять ячеек. Кроме того, если все пять ячеек сконфигурированы одинаково (имеют одну рабочую частоту, одинаковую скорость передачи и общие параметры безопасности), то персональный компьютер или ручное устройство, оборудованное WNIC-адаптером, можно перемещать от одной ячейки к другой. Этот процесс называется *роумингом* (roaming).

В качестве примера роуминга в беспроводной ESS-топологии рассмотрим университетский факультет, в котором развернута беспроводная сеть, имеющая пять точек доступа, связанных с ячейками с номерами от I до V.1 Ячейка I может принадлежать библиотеке. Ячейки II и III могут охватывать зону преподавательских офисов. Ячейка IV может находиться в офисе администрации, а ячейка V может располагаться в учебной лаборатории. Если все ячейки сконфигурированы одинаково, любой студент, преподаватели или служащий офиса может перемещать портативный компьютер, оборудованный WNIC-адаптером, от одной ячейки к другой, сохраняя при этом доступ к сети факультета. Хотя стандартом 802.11 и не предусмотрена спецификация для протокола роуминга, производители беспроводных устройств разработали один подобный протокол, названный *Inter-Access Point Protocol (IAPP),* который в основных моментах отвечает этому стандарту. Протокол IAPP позволяет

мобильной станции перемещаться между ячейками, не теряя соединения сетью. Для обеспечения коммуникаций с роумингом IAPP инкапсулируем протоколы UDP и IP.

Примечание

Как вы уже знаете из *главы 6,* User Datagram Protocol (UDP) представляет собой протокол без установления соединений, который может использоваться сочетании с протоколом IP вместо TCP, являющегося протоколом с установлением соединений.

Протокол IAPP позволяет оповестить имеющиеся точки доступа о подключении к сети нового устройства, а также позволяет смежным точкам доступе обмениваться между собой конфигурационной информацией. Кроме того протокол предоставляет некоторой точке доступа, обменивающейся данными с мобильной станцией, возможность автоматической передачи сведении об исходном подключении (включая любые данные, ожидающие отправки другой точке доступа в тех случаях, когда мобильная станция перемещается от ячейки, обслуживаемой первой точкой доступа, к ячейке, связанной си второй точкой доступа.

Альтернативные технологии радиосетей

К числу самых распространенных коммуникационных технологий с использованием радиоволн относятся следующие технологии, альтернативные стандарту IEEE 802.11:

- Bluetooth;
- HiperLAN;
- HomeRF Shared Wireless Access Protocol (SWAP).

Каждая перечисленная технология представляет собой спецификацию беспроводных сетей и поддерживается определенными производителями. Все эти технологии рассматриваются в следующих разделах.

Bluetooth

Bluetooth – это технология беспроводной связи, описанная особой группой Bluetooth Special Interest Group. Данная технология привлекла внимание таких производителей, как 3Com, Agere, IBM, Intel, Lucent, Microsoft, Motorola, Nokia и Toshiba. В ней используется перестройка частоты в диапазоне 2,4 ГГц (2,4–2,4835 ГГц), выделенном Федеральной комиссией связи для нелицензируемых ISM-коммуникаций[2]. Метод перестройки частоты предполагает изменение несущей частоты (выбирается одна из 79 частот) для каждого передаваемого пакета. Достоинством этого метода является уменьшение вероятности возникновения взаимных помех в случаях одновременной работы нескольких устройств.

При использовании многоваттных коммуникаций технология Bluetooth обеспечивает передачу данных на расстояния до 100 м, однако на практике большинство устройств Bluetooth работают на расстоянии до 9 м. Обычно используются асинхронные коммуникации со скоростью 57,6 или 721 Кбит/с. Устройства Bluetooth, обеспечивающие синхронные коммуникации, работают со скоростью 432,6 Кбит/с, однако такие устройства менее распространены.

В технологии Bluetooth применяется *дуплексная передача с временным разделением каналов* (time division duplexing, TDD), при которой пакеты передаются в противоположных направлениях с использованием временных интервалов. Один цикл передачи может задействовать до пяти различных временных интервалов, благодаря чему пакеты могут передаваться и приниматься одновременно. Этот процесс напоминает дуплексные коммуникации. Одновременно могут взаимодействовать до семи устройств Bluetooth (некоторые производители утверждают, что их технологии обеспечивают подключение восьми устройств, однако это не соответствует спецификациям). Когда устройства обмениваются информацией, одно из них автоматически выбирается ведущим (master). Это устройство определяет функции управления (например, синхронизацию временных интервалов и управление пересылками). Во всех других аспектах коммуникации Bluetooth напоминают одноранговую сеть.

Совет

Узнать больше о технологии Bluetooth можно на официальном веб-сайте по адресу

www.bluetooth.com. Выполните практическое задание 9-7, в котором вы познакомитесь с веб-сайтом Bluetooth, где описаны области применения Blue-tooth для беспроводных коммуникаций с универсальным доступом.

HiperLAN

Технология *HiperLAN* была разработана в Европе, и в настоящее время существует ее вторая версия, названная HiperLAN2. Эта технология использует диапазон 5 ГГц и обеспечивает скорости передачи данных до 54 Мбит/с. Помимо скорости, достоинством HiperLAN2 является совместимость с коммуникациями Ethernet и ATM.

Технология HiperLAN2 поддерживает *Data Encryption Standard (DES)* – стандарт шифрования данных, разработанный институтами National Institute on Standards and Technology (NIST) (Национальный институт стандартов и технологий) и ANSI. В нем используется открытый (public) ключ шифрования, доступный для просмотра всеми сетевыми станциями, а также частный. (private) ключ, выделяемый только передающим и принимающим станциям. Для дешифрации данных необходимы оба ключа.

Технология HiperLAN2 обеспечивает качество обслуживания (QoS), предоставляя гарантированный уровень коммуникаций для различных классов обслуживания (например, для передачи речи или видеоизображений). Это возможно благодаря тому, что точки доступа централизованно управляют беспроводными! коммуникациями, и планируют все сеансы передачи информации.

Сеть HiperLAN2 работает в двух режимах. Непосредственный режим (directlmode) представляет собой топологию одноранговой сети (подобную 1B58 топологии в сетях 802.11), которая образуется только взаимодействующим станциями. Другой режим называется централизованным (centralized mode) поскольку он реализуется в больших сетях, где имеются точки доступа, концентрирующие сетевой трафик и управляющие им. Методом коммуникаций для обоих режимов служит дуплексная передача с временным разделением каналов (TDD) – та же технология, которая применяется в Bluetooth.

Совет

Для более близкого знакомства с HiperLAN2 посетите веб-сайт **www.hiperian2.com.**

HomeRF Shared Wireless Access Protocol (SWAP)

HomeRF Shared Wireless Access Protocol (SWAP) (Протокол совместного беспроводного доступа HomeRF) – это технология, поддерживаемая такими компаниями, как Motorola, National Semiconductor, Proxim и Siemens. Эта
технология работает в диапазоне 2,4 ГГц и обеспечивает скорость в сети до 10 Мбит/с. В качестве метода доступа она использует CSMA/CA (как и стандарт 802.11) и предназначена для домашних сетей, где передаются данные, речь, видеоизображения, мультимедийные потоки и другая информация.

Примером типичного использования технологии HomeRF SWAP является беспроводная сеть, объединяющая несколько персональных компьютеров и обеспечивающая им доступ в Интернет. Другой областью применения является реализация беспроводных соединений для центров развлечений (например, для связи друг с другом нескольких телевизоров и стереосистем). Сеть HomeRF SWAP может связать между собой несколько телефонов. Также с ее помощью можно обеспечить связь между устройствами управления домом (освещением, кондиционерами, кухонными агрегатами и т. д.). Для обеспечения безопасности в сетях HomeRF SWAP используется 128-битное шифрование данных и 24-разрядные сетевые идентификаторы.

На момент написания книги в процессе разработки находилась технология HomeRF SWAPS, обеспечивающая коммуникации со скоростью 25 Мбит/с. Создатели этой технологии стремятся к тому, чтобы встроить ее в телевизоры и мультимедийные серверы с целью расширения возможностей сложных видеосистем.

(Совет)

Более детально познакомиться с HomeRF SWAP можно на сайте **www.homerf.org.**

Сетевые технологии с использованием инфракрасного излучения

Инфракрасное (И К) излучение (infrared) можно использовать в качестве передающей среды для сетевых коммуникаций. Вы хорошо знакомы с этой технологией, благодаря пультам дистанционного управления для телевизоров и стереосистем. ИК-излучение представляет собой электромагнитный сигнал, подобно радиоволнам, однако его частота ближе к диапазону видимых электромагнитных волн, называемых видимым светом.

ИК-излучение может распространяться либо в одну сторону, либо во всех направлениях, при этом светодиод (LED) используется для передачи, а фотодиод – для приема. ИК-излучение относится к Физическому уровню, его частота составляет 100 ГГц – 1000 ТГц (терагерц), а длина электромагнитной волны лежит в диапазоне от 700 до 1000 нанометров (нм, 10^{-9}).

Подобно радиоволнам, ИК-излучение может оказаться недорогим решением в случае невозможности прокладки кабеля или при наличии мобильных пользователей. Его преимущество заключается в том, что ПК-сигнал сложно перехватить незаметно. Другим достоинством является устойчивость ИКЦ сигнала к радио- и электромагнитным помехам. Однако эта коммуникационная среда имеет и ряд существенных недостатков. Во-первых, при направленных коммуникациях скорость передачи данных не превышает 16 Мбит/с, а при всенаправленных коммуникациях эта значение меньше, чем 1 Мбит/с. Во-вторых, ИК-излучение не проходив сквозь стены, в чем несложно убедиться, попробовав управлять телевизором с пульта дистанционного управления из другой комнаты. С другой стороны этот недостаток оборачивается достоинством, т. к. из-за ограниченности области распространения коммуникации с использованием ИК-сигналов делаются более безопасными. В-третьих, инфракрасная связь может подвергаться помехам со стороны сильных источников света.

Совет

> В инфракрасных технологиях могут использоваться точки доступа, позволяющие расширять рабочую область и создавать крупные сети.

При передаче информации с помощью рассеянного инфракрасного излучения (diffused infrared) посланный ИК-сигнал отражается от потолка, как показано на рис. 9.6. Для таких коммуникаций существует стандарт IEEE 802. предусматривающий работу на расстоянии от 9 до 18 м в зависимости высоты потолка (чем выше потолок, тем меньше область охвата сети). Для рассеянного ИК-излучения этим стандартом определены скорости передачи данных, равные 1 и 2 Мбит/с. Длины волн рассеянного ИК-сигнала, ИСЩ пользуемого в стандарте 802.11R, лежат в диапазоне 850–950 нм (из всех диапазона ИК-лучей, составляющего 700–1000 нм). Для сравнения, видимый свет имеет диапазон длин волн, приблизительно равный 400–700 Мегагерц. Максимальная оптическая излучаемая мощность сигнала согласно стандарт 802.11R составляет 2 Вт.

> **Совет**
>
> Хотя рассеянные ИК-сигналы не подвержены радио- и электромагнитным помехам, окна в зданиях могут создавать помехи, поскольку эти сигналы чувствительны к сильным источникам света. Учтите наличие окон при проектирования беспроводной сети с использованием рассеянного ИК-излучения.

Метод передачи сигналов, использованный стандартом IEEE 802.11R, называется *фазоимпульсной модуляцией* (Pulse position modulation, PPM). Согласно этому методу, двоичное значение сигнала связывается с расположением импульса в наборе возможных положений в спектре электромагнитного излучения. Для коммуникаций со скоростью 1 Мбит/с стандарт 802.11R предусматривает шестнадцать возможных положений импульса (16-PPM), этом каждое положение представляет четыре двоичных разряда. При коммуникациях со скоростью 2 Мбит/с каждый импульс представляет два разряда, и возможных положений импульса всего четыре (4-PPM). Импульс в определенной позиции указывает на то, что некоторое значение присутствует, а отсутствие импульса означает, что значения нет. PPM – это метод символьного кодирования, напоминающий двоичное кодирование в том смысле, что в нем используются только нули и единицы.

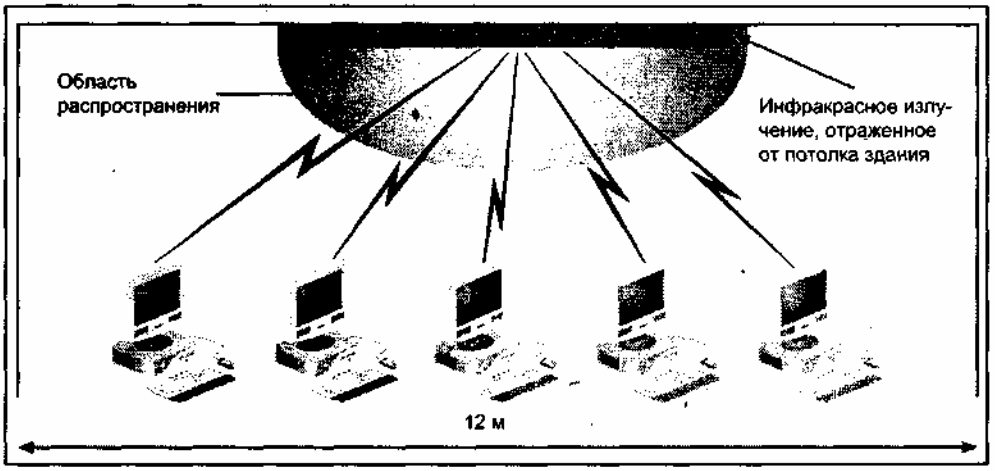


Рис. 9.6. Беспроводные коммуникации
с использованием рассеянного ИК-излучения

Микроволновые сетевые технологии

Микроволновые системы работают в двух режимах. Наземные сверхвысокочастотные (СВЧ) каналы (terrestrial microwave) передают сигналы между двумя направленными параболическими антеннами, которые имеют форму тарелки (рис. 9.7). Такие коммуникации осуществляются в диапазонах частот 4–6 ГГц и 21–23 ГГц и требуют, чтобы оператор связи получал лицензию от Федеральной комиссии связи (FCC).

Спутниковые микроволновые системы передают сигнал между тремя антеннами, одна из которых располагается на спутнике Земли (рис. 9.8). Спутники в таких системах находятся на геосинхронных орбитах на высоте 35000 км над Землей. Чтобы некоторая организация могла использовать такую технологию связи, она должна либо запустить спутник, либо арендовать канал у компании, предоставляющей подобные услуги. Из-за больших расстояний задержки: при передаче составляют от 0,5 до 5 секунд. Коммуникации ведутся в диапазоне частот 11–14 ГГц, которые требуют лицензирования.

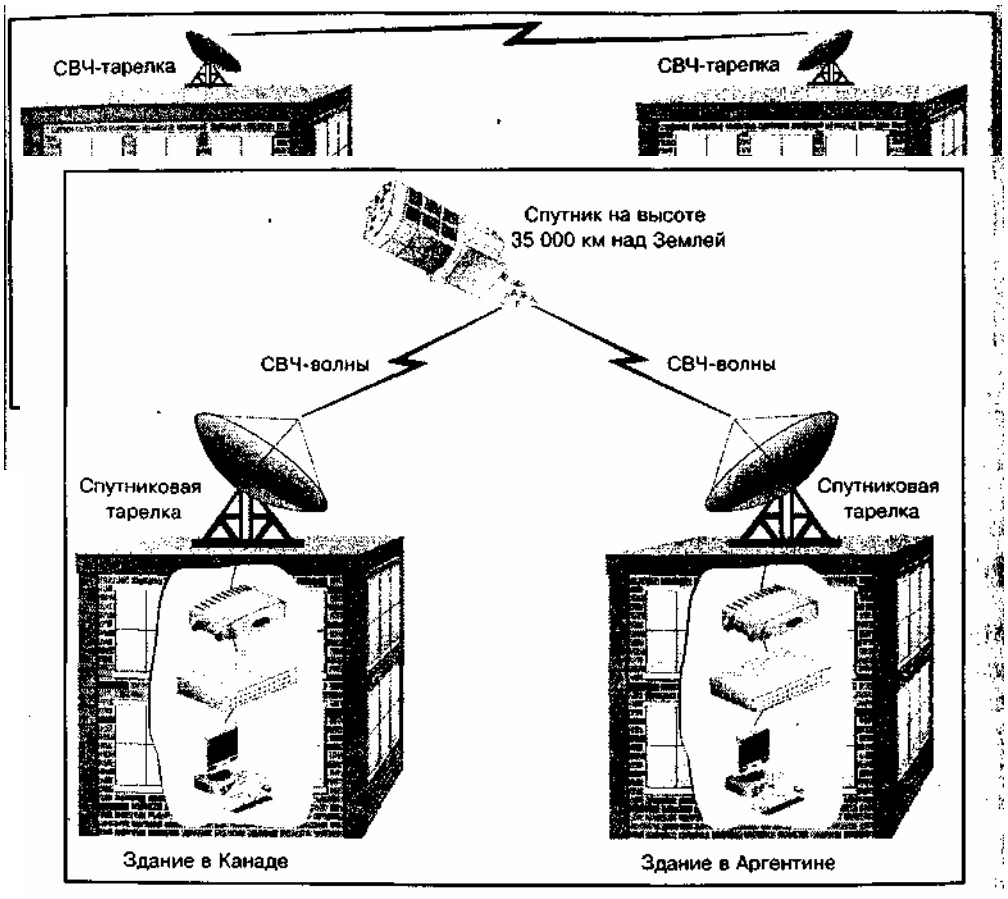


Рис. 9.8. Спутниковые коммуникации

Как и другие среды беспроводной связи, микроволновые технологий используются тогда, когда кабельные системы стоят слишком дорого или если прокладка кабеля невозможна. Наземные СВЧ-каналы могут оказаться хорошим решением при прокладке коммуникаций между двумя большими зданиями в городе. Спутниковые системы связи являются единственно возможным способом объединения сетей, находящихся в разных странах или на разных континентах, однако это решение очень дорогое.

Микроволновые коммуникации имеют теоретическую полосу пропускания до 720 Мбит/с и выше, однако на практике в настоящее время скорости обычно лежат в диапазоне 1–10 Мбит/с. Микроволновые системы связи имеют некоторые ограничения. Они дороги и сложны в развертывании и эксплуатации. Качество микроволновых коммуникаций может ухудшаться из-за условий атмосферы, дождя, снега, тумана и радиопомех. Более того, микроволновый сигнал может быть перехвачен, поэтому при использовании данной передающей среды особо важное значение имеют средства аутентификации и шифрования.

Беспроводные сети на базе низкоорбитальных спутников Земли

Орбиты спутников связи находятся на расстоянии примерно 30000 км над Землей. Из-за большого удаления этих спутников и возмущений в верхних слоях атмосферы могут возникать задержки в передаче сигнала, которые недопустимы для коммуникаций с высокими требованиями к этому параметру связи (в т. ч. для передачи двоичных данных и мультимедиа).

В настоящее время несколько компаний разрабатывают *низкоорбитальные спутники* (Low Earth Orbiting (LEO) satellite), орбиты которых должны находиться на расстоянии от 700 до 1600 км от поверхности Земли, что должно ускорить двустороннюю передачу сигналов. Из-за своей более низкой орбиты LEO-спутники охватывают меньшие территории, и, следовательно, для того чтобы полностью покрыть поверхность планеты, необходимо около тридцати LEO-спутников. В настоящее время компании Teledesic, Motorola и Boeing разрабатывают сеть таких спутников, с помощью которых Интернет и другие услуги глобальных сетей станут доступными в любой точке Земли. Пользователи взаимодействуют с LEO-спутниками при помощи специальных антенн и аппаратуры декодирования сигналов. Начиная с 2005 года, LEO-спутники можно будет использовать в следующих областях:

- широковещательные интернет-коммуникации; проведение всепланетных видеоконференций;
- дистанционное обучение;
- другие коммуникации (передача речи, видео и данных).

Ожидается, что скорости коммуникаций на базе LEO-спутников составят от 128 Кбит/с до 100 Мбит/с для восходящих потоков (к спутнику) и до
720 Мбит/с для нисходящих потоков (от спутника). LEO-спутники используют ультравысокие частоты, утвержденные Федеральной комиссией связи в США и аналогичными организациями в разных частях света. Электромагнитный спектр коммуникаций с использованием LEO-спутников также одобрен союзом ITU. Рабочие частоты лежат в диапазоне 28,6–29,1 ГГц дли восходящих каналов и 18,8–19,3 ГГц для. нисходящих каналов. Когда эта сеть войдет в эксплуатацию (архитектура сети представлена на рис. 9.9), руководитель проекта, например, из Бостона сможет проводить видеоконференции или обмениваться важными двоичными файлами с исследователем живущим в горной хижине в Вайоминге, а хозяин животноводческой фермы из Аргентины сможет обращаться за сельскохозяйственными данными сети Университета Северной Каролины (Колорадо). (Выполните практическое задание 9-8 для того, чтобы получить дополнительную информацию он использовании LEO-спутников для построения сетей.)

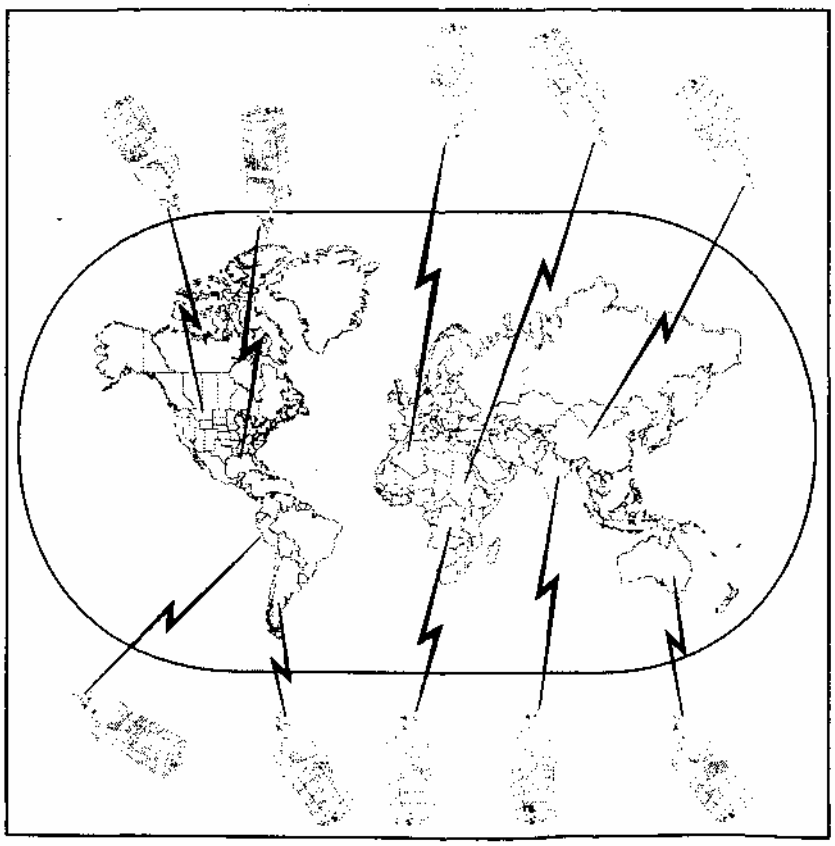


Рис. 9.9. Глобальная сеть на базе низкоорбитальных (LEO) спутников Земли

Резюме

1 В современных технологиях беспроводных сетей применяются радиоволны, инфракрасное излучение, СВЧ-волны и низкоорбитальные спутники.

2 Основой для беспроводных сетей послужили эксперименты с пакетной радиосвязью, которые давно проводили операторы-радиолюбители.

3 В настоящее время беспроводные сети используются во многих областях (например, когда сложно развернуть кабельные сети). Кроме того, такие сети позволяют уменьшить затраты на установку сети и обеспечивают связь с мобильными компьютерами.

4 В технологиях радиосвязи обычно используются коммуникации в пределах прямой видимости, которые осуществляются от одной точки к другой вдоль поверхности Земли (вместо того, чтобы радиосигнал отражался от атмосферы Земли). В таких технологиях также применяются коммуникации с расширенным спектром, когда радиоволны передаются по нескольким смежным частотам.

5 Стандарт IEEE 802.11 в настоящее время используется в радиосетях различного типа. Этот стандарт предусматривает три основных компонента: адаптер беспроводной сети (WNIC), точка доступа и антенна. Приняты два стандарта (802.11a и 802.11b), которые определяют скорости коммуникаций, отвечающих стандарту 802.11. Внедряется новый стандарт – 802.11g, который представляет собой расширение стандарта 802.11b.

6 К распространенным альтернативам стандарту 802.11 относятся технологии Bluetooth, HiperLAN и HomeFR Shared Wireless Access Protocol.

7 Стандарт 802.11R предусматривает использование рассеянного инфракрасного (ИК) излучения для построения небольших, относительно защищенных сетей, размещающихся в довольно замкнутых офисах или рабочих зонах.

8 Микроволновые сети существуют в двух видах: сети на базе наземных СВЧ-каналов и спутниковые сети. Спутниковые сети, конечно, могут стоить очень дорого из-за высоких расходов на запуск спутника в космос.

9 Сети на базе низкоорбитальных (LEO) спутников предусматривают использование группы спутников, располагающихся на очень низких орбитах над уровнем Земли, благодаря чему задержки при передаче сигналов получаются значительно меньше, чем в обычных спутниковых коммуникациях. Когда сети

на базе LEO-спутников будут развернуты, возможность работы в сетях станет доступной в любой точке планеты.

10 В табл. 9.2 перечислены достоинства и недостатки сетевых коммуникаций с использованием радиоволн, ИК-излучения и СВЧ-волн.

Таблица 9.2. *Достоинства и недостатки беспроводных технологий связи*

	Радиоволны	**ИК-излучение**	**СВЧ-волны**	**Низкоорбитальные спутники**
Досто-инства	Недорогая альтернатива для тех случаев, когда сложно реализовать коммуникации по кабелю. Одно из средств реализации мобильных телекоммун-икаций Обычно не требует лицензирования.	Сигнал трудно перехватить незаметно.	Недорогая альтернатива для тех случаев, когда сложно реализовать коммуникации по кабелю, особенно на большие расстояния. Наземный СВЧ канал на больших расстояниях может оказаться более дешевым, чем арендуемые телекоммуника-ционные линии	Может разполагаться над Землей при создании глобальной сети. Не создают таких задержек при передачи сигналов, как геосинхронные спутники.
Недо-статки	Могут не соответствовать требованиям высокоскоростных сетей. Подвержены помехам со стороны сотовых сетей, военных, обычных и других источников радиосигналов. Подвержены помехам естественного происхождения.	Могут не подойти для высокоскоро-стных коммуникаций. Подвержены помехам со стороны посторонних источников света. Не передаются через стены. Номенклатура предлагаемых устройств меньше, чем для других типов беспроводных сетей	Могут не подойти для высокоскоро-стных коммуникаций Дороги в установке и эксплуатации. Подвержены помехам природного характера (дождь, снег, туман) и радиопомехам, а также зависят от состояния атмосферы.	Будут доступны лишь в 2005 году

Глава 10

Совместная передача речи, видеоизображений и данных

По прочтении этой главы и после выполнения практических заданий вы сможете:

- рассказать о технологиях передачи аналоговых и цифровых видеоизображений;
- описать технологии создания аудиофайлов;
- объяснить принципы дискретизации аудио- и видеосигналов;
- рассказать о технологии Voice over IP;
- оценить полосу пропускания и производительность сети;
- описать способы передачи мультимедийных данных;
- спроектировать локальную и глобальную сеть для мультимедийных приложений;
- обсудить перспективы развития мультимедийных коммуникаций.

Мультимедийные, приложения, ориентированные на передачу голоса и видеоизображений, широко распространены в сетях и Интернете. Многие люди просматривают новые видеоклипы, слушают музыку или учатся, используя интерактивное видео, – при этом всю информацию они получают через сеть. Врачам доступны средства телемедицины, позволяющие знакомиться с новыми процедурами на веб-сайтах. Студенты могут пройти полный курс обучения в частных институтах, колледжах и университетах, которые предлагают свои сертификаты и ученые степени исключительно через Интернет. Во многих областях бизнеса проведение телеконференций через локальные и глобальные сети позволяет сэкономить тысячи долларов, потраченных на поездки. В следующем десятилетии новые мультимедийные приложения для образования, развлечений и бизнеса, приложения, которые сейчас даже трудно себе представить, будут восприниматься как нечто само собой разумеющееся.

Специалисту по сетям для оценки затрат на совместную передачу речи, видеоизображений и данных необходимо хорошо понимать специфику этих коммуникаций, а также уметь создавать надежные сети. В начале этой статьи вы познакомитесь с аналоговыми и цифровыми видеотехнологиями, после чего будет рассмотрено множество технологий создания аудиофайлов. Будет рассказано о дискретизации аудио- и видеосигналов, а также о способах совместной передачи речи, видео и данных по сети. Вы узнаете о технологии передачи голоса по IP-протоколу (VIP) и о способах определения; полосы пропускания сети и ее производительности. Также будут описаны методы передачи пакетов и фреймов для интегрированных мультимедийных приложений. И, наконец, вы познакомитесь с методами проектирования локальных и глобальных сетей, позволяющих передавать мультимедийный трафик, а также узнаете о факторах, определяющих перспективы развития мультимедийных коммуникаций.

Технологии передачи видеоизображений

Корни компьютерных видеотехнологий лежат в аналоговом телевидении. В настоящее время все наоборот: компьютерные технологии проникают в телевидение. Таким образом, границы между компьютерным воспроизведением видеоизображений и цифровым телевидением становятся неразличимыми. В следующих разделах излагаются основы аналоговых и цифровых видеотехнологий, а затем рассматриваются три основных технологии, применяемые в компьютерах: Audio Video Interleave (AVI), Motion Pictures Experts Group (MPEG) и фрактальные преобразования.

Аналоговая передача изображений

Исторически передаваемые видеоизображения представляли собой аналоговый сигнал, в первую очередь, используемый в телевидении. Первые телевизионные системы передавали черно-белые кадры в соответствии со стандартами, определенными Федеральной комиссией связи в начале 1940-х годов. В начале 1950-х годов телевидение стало быстро развиваться, возник большой интерес к трансляции цветных телевизионных сигналов. Для созданиям стандартов телевещания был организован комитет National Television Standards Committee (NTSC), который в 1954 году установил стандарт для цветного

телевидения. Стандарты NTSC применяются в Канаде, Центральной Америке, Японии и США. Они согласованы со стандартами электропитания, принятыми в этих странах, в соответствии с которыми используется переменный ток с частотой 60 Гц.

Изображение, видимое на телеэкране, представляет собой последовательность быстро передаваемых отдельных картинок, которые создают иллюзию[4], движения, поскольку каждая картинка немного отличается от другой. Одна картинка составляет телевизионный кадр. Стандарт NTSC для цветного вещания на одном канале (в одном диапазоне частот) определяет 525 строкой развертки по вертикали и частоту передачи, равную 30 кадрам в секунду. Строки развертки (scan line) представляют собой отдельные линии, отображаемые сверху вниз и используемые для создания одного изображения (кадра) на экране телевизора.

Помимо стандартов NTSC, используются и два других стандарта телевещания: Phase Alternation Line (PAL) и Systems Electronic Couleur Avec Memiore (SECAM). В первую очередь эти стандарты применяются в странах, где основное силовое напряжение имеет частоту 50 Гц. Стандарт PAL распространен в Африке, Европе, на Ближнем Востоке и в Южной Америке. Он предусматривает 625 строк вертикальной развертки (вместо 525), и передача ведется с частотой 25 кадров в секунду. В стандарте SECAM также предусмотрено 625 строк развертки, однако в телевизорах SECAM используется другой источник опорных синхросигналов подмагничивания. Эти сигналы выполняют те же функции, что и идентификаторы при передаче фреймов данных. SECAM применяется во Франции, в России и некоторых странах Африки.

Цифровая передача изображений

Появление компьютерных технологий позволило улучшить способы воспроизведения видеоизображений на компьютерах и в телевизорах. В настоящее время цифровые видеоизображения широко распространены в Интернете, где имеются видеофайлы всех типов.

В области телевидения Федеральная комиссия связи (FCC) работает над тем, чтобы большинство коммерческих телекомпаний перешли с аналогового вещания на цифровое приблизительно к 2006 году. Цифровое изображение можно передавать на большее расстояние, при этом картинка получается четче. Это стало возможным благодаря тому, что ошибки передачи, вызванные радио и электромагнитными помехами, можно скорректировать с помощью контрольной информации, передаваемой вместе с цифровым сигналом. Коды исправления ошибок позволяют телевизору мгновенно обнаруживать и исправлять искажения, вызванные перекрестными помехами. Сигнал может передаваться (без необходимости преобразования из аналогового представления в цифровое) со скоростью 20 Мбит/с и выше.

Совет

Дополнительную информацию о планах перехода от аналогового вещания к цифровому телевидению можно найти на веб-сайте FCC по адресу **www.fcc.gov/dtv.**

Цифровое телевидение и передача видеоизображений в сети являются близкими родственниками, поскольку они используют оцифрованные изображения. Важным различием между ними является то, что для сетевых передач видео применяются несколько технологий, а в цифровом телевидении, по сути, используется только одна технология (MPEG-2). На компьютерах и сетях распространены три технологии сжатия видеоизображений:

- Audio Video Interleave (AVI);
- Motion Pictures Experts Group (MPEG);
- фрактальное сжатие изображений.

Каждая из технологий подробно рассматривается в следующих разделах.

Audio Video Interleave (AVI)

Audio Video Interleave (AVI) это метод форматирования комбинирования аудио- и видеофайлов, предложенный компанией Microsoft для использования в системах Windows версии 3.1 и выше. AVI на самом деле является подмножеством формата Resource Interchange File Format (RIFF) (Формат файлов для обмена ресурсами), разработанного совместно компаниями Microsoft и для воспроизведения коротких аудио- и видеоклипов. В файлах этого формата видео- и аудиоданные чередуются: сначала идет

видеоклип, затем сопровождающий его аудиоклип, затем снова видеоклип и т. д. Стандарт AVI имеет недостатки, относящиеся к качеству воспроизведения и транспортировке по сети. Кроме того, файлы получаются относительно большими.

Motion Pictures Experts Group (MPEG)

Motion Pictures Experts Group – это группа в составе ISO, разработавшая стандарт сжатия *Motion Pictures Experts Group (MPEG),* который часто применяется на компьютерах, в средствах мультимедиа и Интернете. MPEG версий

(MPEG-2) предусматривает также методы доставки комбинированных аудио- и видеосигналов в системах цифрового телевидения. Цифровой телевизор воспроизводит передаваемый сигнал MPEG-2 так, как это происходит на компьютере.

Согласно стандарту MPEG-2, существуют три уровня разрешения:

1. 704 x 480 пикселов с построчной разверткой (также обозначается 480p);
2. 1280 x 720 пикселов с построчной разверткой (также обозначается 720p);
3. 1920 x 1080 пикселов с чересстрочной разверткой (также обозначается I080p)

Примечание

На экране компьютерного монитора или цифрового телевизора *пиксель* (pixel) представляет собой маленькую точку света. *Построчная* (progressive) развертка означает, что за секунду передается до 60 кадров, а при *чересстрочной,*(interlaced) развертке за секунду передается до 30 кадров. Уровни 720p и 1080p относятся к высококачественному воспроизведению, отсюда и идет название *цифровое телевидение высокой четкости* (High-definition digital TV (HDTV). Для сжатия видеоизображений стандарт MPEG использует комбинацию трех методов:

1. сжатие с потерями (как в изображениях JPEG), прогностическое кодирование и двунаправленную интерполяцию.

2. *Сжатие с потерями* (lossy compression) учитывает тот факт, что человеческий глаз не различает небольших изменений цвета. Таким образом, при сжатии некоторые разряды в кадрах отбрасываются. При распаковке получается изображение, близкое к оригиналу, при этом некоторые изменения цветов не заметны для человеческого глаза. Недостаток сжатия с потерями заключается в следующем: чем больше удаляется разрядов, тем более заметными становятся изменения цветов при распаковке кадра. При использовании этого метода существует предел приемлемого сжатия, приблизительно равный 24:1.

Метод сжатия с потерями, примененный в MPEG, первоначально использовался в распространенном стандарте сжатия *Joint Photographic Experts Group (JPEG),* созданном ISO и ITUT. В этом стандарте для сжатия также задействуется кодирование по методу Хаффмана, которое чаще всего встречающиеся фрагменты изображения представляет короткими двоичными последовательностями, а реже встречающиеся – более длинными последовательностями. В результате этого сокращается общее число использованных двоичных разрядов. Сжатие JPEG предназначается для неподвижных изображений и не обеспечивает такой коэффициент сжатия, который требуется для передачи последовательности кадров через сеть или модемы. Поэтому MPEG объединяет сжатие JPEG с прогностическим кодированием и двунаправленной интерполяцией. При такой комбинации методов достигается больший коэффициент сжатия, чем тот, который возможен при использовании одного сжатия JPEG.

3. При *прогностическом кодировании* (predicted encoding) предполагается, что часть кадра содержит некоторый фрагмент, который присутствует также и в предыдущем кадре. Вместо того чтобы использовать сжатие JPEG для всего кадра, создаются указатели на блоки пикселов из предыдущего кадра. Это позволяет избежать дублирования той части изображения, которое не менялось. При прогностическом кодировании кадр делится на блоки размером 16 x 16 пикселов и на их основе создаются указатели на соответствующие блоки (рис. 10.1).

4. *Двунаправленная интерполяция* (bidirectional interpolation) напоминает прогностическое кодирование, однако указатели строятся на идентичные блоки пикселов, которые располагаются как в предыдущем, так и в последующем кадрах (рис. 10.2). В стандарте MPEG применение всех

рассмотренных методов сжатия кадров видеоизображения позволяет достигнуть скорости передачи 1,5 Мбит/с. Это довольно впечатляющая скорость, если учесть сложность передаваемой информации и сложность математических алгоритмов, использованных при сжатии и распаковке.

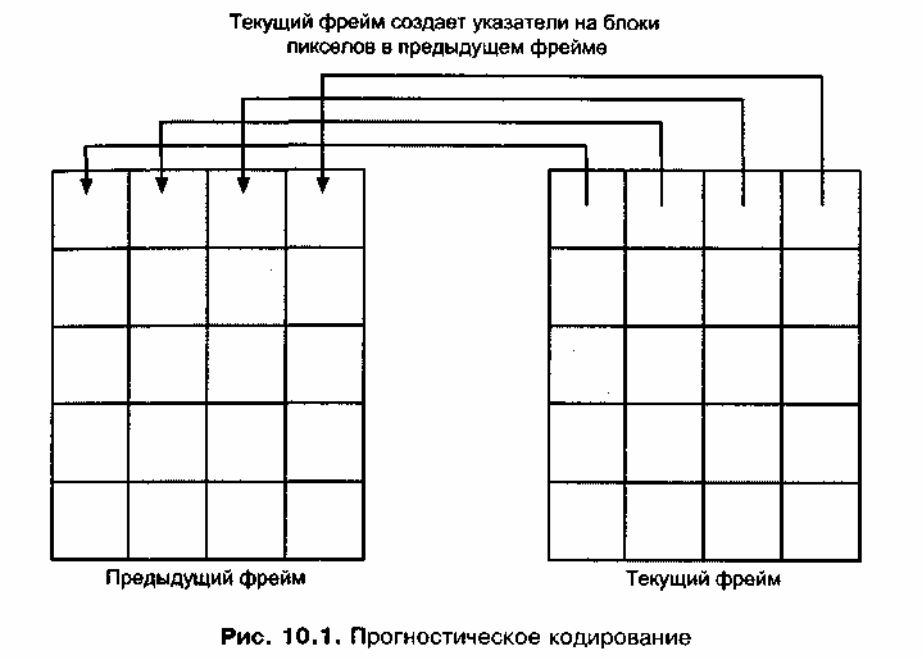


Рис. 10.1. Прогностическое кодирование

Рис. 10.2. Двунаправленная интерполяция

На момент написания книги существовали различные уровни MPEG, которые уже были утверждены или находились в разработке. Перечень этих ровней содержится в табл. 10.1.

Таблица 10.1. *Уровни MPEG*

Уровень	Описание MPEG
MPEG-1	Используется для воспроизведения видеоизображений и музыки на компакт-дисках, а также при передаче через сети и в воздушной среде (например, в беспроводных сетях)
MPEG-2	Совместим с MPEG-1 и распространяет этот формат на цифровое телевидение, высококачественное цифровое телевидение и цифровые видеодиски (DVD)

MPEG-4	Обеспечивает более высокую скорость передачи, что позволяет повысить разрешение, улучшить коррекцию ошибок передачи, а также создавать описания контента (содержимого видео- и аудиопотоков) (это особо важно для передачи информации в веб-сети)
MPEG-7	Совместим с MPEG-4 и расширяет его возможности по созданию описаний контента. Позволяет пользователям находить и получать необходимый им контент
MPEG-21	Перспективная инициатива, направленная на расширение всех возможностей MPEG. Этот разрабатываемый стандарт направлен на улучшение MPEG в плане объединения существующих и, новых видео- и аудио-технологий (музыкальных, стерео, телевизионных, компьютерных, интернетовских, радио, микроволновых, кабельных) в единую совместимую среду

Фрактальное сжатие изображений

При *фрактальном сжатии изображений* (fractal image compression) в кадрах выполняется поиск повторяющихся структур (pattern), даже если эти структуры имеют разную ориентацию или размер. Математики называют такие структуры аффинными преобразованиями. Для уменьшения размера общих аффинных преобразований используется математическое сжимающее отображение. Достоинством фрактального сжатия является высокий коэффициент сжатия, достигающий значения 80:1 и выше. Недостаток заключается в том, что из-за математической сложности этот метод требует заметно больше времени на сжатие и распаковку изображений по сравнению с MPEG или JPEG. Поэтому в значительной степени фрактальное сжатие изображений до сих пор является экспериментальной технологией.

Режимы воспроизведения видеоизображений формата MPEG

Один из способов воспроизведения видеоклипа в формате MPEG состоит в том, что его можно сохранить на некотором сервере и позволить клиентам обращаться к нему. Весь видеоклип копируется как файл, после чего он воспроизводится с помощью программного MPEG-плеера. Такой способ воспроизведения является предсказуемым в смысле получаемого качества изображения и времени, необходимого для полного проигрывания клипа; Он напоминает воспроизведение видеоклипа с компакт-диска.

Другим способом воспроизведения MPEG-файла является его потоковая передача по сети. При *потоковой передаче* (streaming) воспроизведение видеоклипа начинается, как только будет получен первый фрагмент файла при этом не нужно ждать, пока этот файл будет загружен полностью. Потоковое воспроизведение особенно удобно при организации видеоконференций или при просмотре длинного учебного материала, который может состоять из множества MPEG-файлов. Недостатком потокового видео является то, что воспроизведение может быть неровным из-за изменений состояния сети (например, при неоднородном сетевом трафике), при этом кадры могут теряться для обеспечения более равномерного воспроизведения, достигаемого за счет качества и непрерывности изображения.

Примечание

Наличие приложений с потоковой передачей видеоизображений является одной из причин реализации QoS в сети. Для этого, например, можно использовать технологию ATM (подробно она рассматривалась в *главе 8).*

Технологии создания аудиофайлов

Технологии создания аудиофайлов различаются в значительно большей степени, чем видеотехнологии. Кроме того, передаваемые файлы могут быть относительно короткими или очень большими. Существует множество технологий создания аудио-файлов, некоторые из наиболее

используемых перечислены в табл. 10.2.

Для передачи по сетям чаще всего используются три перечисленных ниже технологии создания аудиофайлов:

1.ACELP – применяется, например, в медиа- и аудиоплеерах;

2.MPEG – используется для передачи через Интернет любых комбинированных видео- и аудиосигналов;

3.WAV (особенно PCM U-law) – применяется для воспроизведения музыкальных файлов через Интернет.

Все три технологии оказали чрезвычайное влияние на развитие сетей, поскольку аудио-файлы зачастую имеют большой размер и передаются как через Интернет, так и по локальным сетям.

Таблица 10.2. *Технологии создания аудиофайлов*

Технология	**Описание**	**Область применения**	**Стандартизующая(ие) организация(и)**
Algebraic-Code-Excited Linear Prediction (ACELP)	Обрабатывает и сжимает аудиосигнал используя дискретизацию с частотой 8 или 16 кГц. Также применяет метод широкополосного сжатия, что позволяет ускорить передачу информации за счет уменьшения длины файлов	Voice over IP, голосовая почта, интернет-телефония, программы интерактивного общения в сети, медиаплееры и аудио-плееры	Не стандарт. Разрабатывается компанией VoiceAge в качестве собственного продукта на основе нескольких стандартов, включая стандарт ITU-T G.729 для смежной структуры ACELP
Audio Code Number 3 (AC-3), называемая также Dolby digital surround sound (Цифровая система объемного звучания Долби)	Использует шесть каналов для передачи звука (2 правых, центральный и 2 левых). Воспроизведение звука по пяти основным каналам осуществляется в диапазоне 3 - 20000 Гц, а по шестому (басовому) каналу в диапазоне 3-120 Гц	Саундтреки кинофильмов на ленте и DVD, а также в цифровом телевидении	Не стандарт. Разрабатывается компанией Dolby Laboratories Inc
Adaptive Differential Pulse Code Modulation, ADPCM (Адаптивная дифференциальная импульсно кодовая модуляция)	Использует импульсно-кодовую модуляцию (см. PCM), преобразует 64-килобитные аудиоканалы в каналы с меньшей скоростью (например, 24 и 16 Кбит/с) для передачи в телекоммуникационных	Передача аудио-сигнала через модемы	ITU-T

Технология	Описание	Область применения	Стандартизующая(ие) организация(и)
	системах		
Audio Interchange File Format, AIFF	Дискретизирует информацию и представляет ее в виде небольших блоков для хранения различных звуков (моно, стерео и объемных), а также для синхронизации аудио-сигналов. AIFF-файлы нередко имеют большие размеры, поэтому для их сжатия был создан стандарт AIFF-C	Сети на базе компьютеров Apple Macintosh и аудиокомпакт-диски	Apple Computer, Inc. и American Interactive Media Group (стандарт CD-I IFF)
Global System for Mobile Communications, GSM (Глобальная система мобильной связи)	Кодирует цифровые аудиосигналы для передачи со скоростью 1650 бит/с	Передача аудиосигналов через спутники	European Telecommunications Standards Institute (ETSI)
Interchange File Format, IFF	Напоминает стандарт AIFF, однако использует методы дискретизации с меньшими возможностями	Компьютеры Amiga (устаревшие компьютеры для персонального использования)	Не стандарт. Используется компанией Amiga Computers
Musical Instrument Digital Interface, MIDI (Цифровой интерфейс музыкальных инструментов)	Передает звук по 16 каналам, которые воспроизводят звуки реальных инструментов, звуки голоса, а также синтезированные звуки	Передача звуков между музыкальными синтезаторами и MIDI-совместимыми компьютерами	International MIDI Assocoation
MPEG-1 Audio	Использует импульсно-кодовую модуляцию для синхронизации звуков в одном или двух каналах или в стереоканалах с видеокадрами. Обеспечивает коэффициент сжатия аудиосигналов до	Мультимедийные компьютерные коммуникации и обмен информацией между компьютерами (в частности, с использованием значения 6:1 компакт-дисков)	ISO и ITU-T
MPEG-2 Audio	Расширяет возможности MPEG-1. Использует импульсно-кодовую модуляцию для одно- и многоканального звука, поддерживает больше	Мультимедийные компьютерные коммуникации и обмен информацией между компьютерами (в частности, с использованием	ISO и ITU-T

Технология	Описание	Область применения	Стандартизующая(ие) организация(и)
	форматов, чем MPEG-1	компакт-дисков и DVD). Также применяется в цифровом телевидении и телевидении высокой четкости, а также для воспроизведения стереозвука во фронтальных и тыловых акустических системах	
MPEG-4 Audio	Стандарт основан на MPEG-2, добавляет к нему описания контента (содержимого)	Мультимедийные компьютерные коммуникации, обмен информацией между компьютерами, компакт-диски, DVD-диски и веб-приложения	ISO и ITU-T
MPEG-7 Audio	Стандарт основан на MPEG-4, добавляет к нему возможность поиска по описаниям контента, благодаря чему можно воспроизвести некоторый фрагмент аудиоклипа	Те же области, что и для MPEG-4	ISO и ITU-T
Open Document Architecture Audio Content Architecture, ODA ACA (Открытая структура документов – Структура аудиоданных)	Использует кодирование с помощью импульсно-кодовой модуля например, ADPCM или MPEG для интеграции звуков в документы, отвечающие стандарту Open Document Architecture (ODA) и содержащие текст и графику ODA – это стандарт ISO для специальным образом отформатированных документов, содержащих текст, графику, звуки и другие презентационные данные	ODA-документы на компьютерах и документы, передаваемые по сети	ISO и ITU-T
Pulse Code Modulation, PCM	Используется для преобразования	Преобразование аналоговых аудио-	ITU-T

Технология	Описание	Область применения	Стандартизующая(ие) организация(и)
(Импульсно-кодовая модуляция)	аналогового аудио-сигнала в 8-разрядный цифровой сигнал, который можно передавать со скоростью 64 Кбит/с. Существуют два субстандарта PCM: U-law (для США и Канады) и A-law (для Европы)	сигналов в цифровые для Интернета и телекоммуникаций (например, через терминальные адаптеры по сети ISDN)	
Sub-band Adaptive Differential Pulse Code Modulation, SB-ADPCM (Адаптивная дифференциальная импульсно-кодовая модуляция с поддиапазонами)	Предназначается для ISDN-коммуникаций и использует ADPCM для передачи аудиосигналов по ISDN-каналам	Кодирование аудио-сигналов для терминальных адаптеров при передаче через сети ISDN и frame relay	ITU-T
Waveform audio file format (WAV)	Часто применяется на персональных компьютерах, работающих под управлением операционных систем компании Microsoft. Стандарт был разработан для использования с форматом Resource Interchange File Format (RIFF), принятым в системах Windows версии 3.1 и выше. WAV-файлы могут кодироваться с помощью ADPCM, PCM U-law, PCM A-law и других методов	Компьютеры, работающие под управлением Windows версии 3.1 и выше, передача сигналов по сетям и в Интернете	Не стандарт. Разработан и используется компаниями Microsoft и IBM

Дискретизация аудио- и видеосигналов

Во многих аудио- и видеотехнологиях для преобразования аналогового сигнала в цифровой используются методы дискретизации (sampling). Это означает, что для получения цифрового сигнала в определенные моменты времени снимаются значения амплитуды аналогового сигнала, частота которого изменяется в герцах. Чем выше частота дискретизации, тем выше будет качество воспроизведения звука, полученного из цифрового сигнала. Таким образом, качество звука при частоте дискретизации, равной 8 кГц, будет выше, чем при дискретизации с частотой 2 кГц. Кроме того, реальная частота дискретизации для многоканального сигнала будет равна количеству каналов, умноженному на частоту дискретизации. Например, для одноканального монофонического аудио-сигнала, оцифрованного с частотой 2 кГц, общая

частота дискретизации будет равна 2 кГц, однако для двухканального стерео сигнала общая частота дискретизации составит 4 кГц.

Распространение аудио- и видеотехнологий

Аудио- и видеотехнологии используются организациями и частными лицами для многих целей. Важной областью применения технологий создания аудиофайлов стали Интернет-радио и музыкальные файлы, загружаемые из Интернета. (Следует, однако, заметить, что загрузка музыкальных файлов может являться нарушением авторских прав исполнителей.)

Аудио- и видеоконференции являются еще одной областью применения, которая расширяется по мере того, как компании ищут пути снижения расходов на командировки. Кроме этого, многие учебные заведения предлагают учебные курсы или целые образовательные программы, с которыми можно познакомиться в онлайновом режиме через Интернет, а некоторые производители предлагают интернет-семинары.

Индивидуальные пользователи компьютеров во всем мире посылают по электронной почте письма с вложениями, содержащими речь или видеосообщения. Также электронная почта может использоваться для пересылки презентаций с аудио- и видеоклипами.

Примечание

Производители компьютеров и сетевого оборудования предлагают аудио и видео учебные курсы для знакомства с новыми технологиями. Например, компания Microsoft предлагает технические дискуссии **(www.microsoft.com/technet/treeview/ default.asp?url=/technet/itcommunity/chats/default.asp)** и онлайновые семинары **(www.microsoft.com/technet/treeview/default.asp?url=/technet/tcevents/ olseminars/default.asp).** Компания Network World предлагает веб-семинары на своем сайте Network World Fusion **(www.nwnetsmart.com/ns/webcast/index.html]** Компания Red Hat также предлагает веб-семинары по вопросам, касающимся операционной системы Linux **(www.redhat.com/solutions/info/webcasts/).**

Местные и национальные информационные службы предлагают аудио- видеоклипы, иллюстрирующие новости и последние события. Некоторые люди используют сети или Интернет для телефонных переговоров, а другие пересылают отснятые видеосюжеты.

Примечание

Все большее применение аудио- и видеоприложений уже повлияло на развитие компьютерных систем и сетей. Первые компьютеры предъявляли весьма скромные требования к памяти и жесткому диску (например, хватало нескольку сот килобайт ОЗУ и 10 –20-мегабайтного диска). В настоящее время компьютерам необходимо 64, 128 и более мегабайт памяти, несколько гигабайт дискового пространства и привод CD-ROM. Аналогичный рост можно наблюдать и в отношении требований к сетевым ресурсам. В первых сетях скорость 10 Мбит была более чем достаточной, однако в наше время даже для небольших сети требуется скорость не ниже 100 Мбит/с, чтобы справиться с возросшей нагрузкой, создаваемой при передаче голоса, видео и данных.

Тенденции развития аудио- и видеотехнологий

Аудио- и видеотехнологии составляют быстро растущий сектор сетевых коммуникаций. Например, в области мультимедийных средств развивают средства проведения аудио- и видеоконференций. Программа NetMeeting компании Microsoft позволяет проводить интерактивные конференции нескольких человек, находящихся на удалении друг от друга. В процессе конференции может передаваться звук и изображение или только звук Другим средством для организации конференций является технология IP/TV, предлагаемая компанией Cisco. С ее помощью можно, оставаясь за компьютером, участвовать в конференциях, проводить корпоративные собрания и совещания рабочих групп. Реализация IP/TV достигается за счет координации коммуникаций между группами устройств с помощью процедуры, называемой многоточечными (многосторонними) коммуникациями.

Совет

Дополнительную информацию о программе NetMeeting или технологии IP/TV можно получить на веб-сайтах **www.microsoft.com** (выполните поиск елок NetMeeting) и **www.cisco.com** (выполните поиск строки IPTV).

Если говорить о перспективах и областях развития аудио- и видеотехнологий, то можно привести следующие примеры:

- все больше людей будет использовать сетевую и Интернет-телефонию, а также почтовые службы, передающие голос и видео; благодаря этому люди смогут видеть собеседников и упростится конференц-связь;
- все больше семинаров будет передаваться по сетям и через Интернет, обеспечивая живое, интерактивное общение;
- большинство кинотеатров будут получать фильмы через Интернет, и практически каждый, кто хочет посмотреть фильм дома, сможет воспользоваться такой возможностью с помощью цифрового телевидения высокой четкости и кабельных сетей или Интернета;
- все больше учащихся будут получать внеклассную помощь от учителей и преподавателей, используя голосовую и видеосвязь через Интернет;
- собеседования для поступления в учебные заведения, для получения ученой степени, а также при приеме на работу будут проводиться в онлайновом режиме, что позволит сократить расходы на поездки и расширить количество претендентов;
- медицинские и фармацевтические компании получат больше возможности для обучения врачей и распространения информации о своей продукции (например, о том, как применять новые лекарства или вживлять имплантаты), при этом обучение будет осуществляться исключительно через Интернет с использованием аудио- и видеотехнологий;
- телефоны, телевизоры, компьютеры и стереосистемы будут все больше и больше интегрироваться и выпускаться в виде единого аудио/видео-устройства, легко подключающегося к сетям с помощью беспроводных технологий;
- туристы смогут пользоваться ручными беспроводными аудио/видео-устройствами для быстрого поиска достопримечательностей и знакомства *с* ними, для ориентации на местности, для поиска знакомых и визуального общения с ними.

Выполните практическое задание 10-1 для прослушивания демонстрационных ACELP-файлов. Затем выполните задание 10-2 для определения размера различных типов аудиофайлов. В практическом задании 10-3 вы попробуете воспроизвести потоковый видеоклип формата MPEG через сеть или Интернет. И, наконец, в задании 10-4 вы узнаете о том, как пользоваться средством воспроизведения аудио/видеофайлов (например, MPEG-файлов) в системе Red Hat Linux *7.x*.

Примечание

Ориентируйтесь на стандарты MPEG-7 и MPEG-21, которые идут на смену многим другим стандартам, поскольку MPEG является наиболее распространенным методом кодирования звука и может обеспечить очень высокое его воспроизведение. К тому же область совместного использования звуковых и видеосигналов все больше расширяется.

Передача голоса по IP-протоколу Voice over IP, VoIP)

Voice over IP (VoIP – это сетевая технология, позволяющая осуществлять телефонные коммуникации по IP-сети. С ее помощью организация может создать собственную телефонную систему с использованием IP-сети и VoIP устройств. При таком подходе можно отказаться от разнообразных частных телефонных систем, описанных в *главе 4,* и сэкономить деньги, поскольку доля внутренней телефонной службы можно использовать уже существующую сеть.

VoIP-сеть обычно состоит из устройств трех типов (как минимум). Телефонный модуль (или компьютер, оборудованный микрофоном и акустическими системами) используется для преобразования речи в двоичный код, затем – в IP-пакеты. Этот модуль обменивается информацией с другим устройством, называемым обработчиком вызовов (или сервером вызовов), который может выполнять следующие функции:

- устанавливать и разрывать телефонные соединения; перенаправлять вызовы;
- управлять телефонными соединениями;
- преобразовывать телефонные номера или идентификаторы в IP-адреса.

Телефонная система на базе VoIP требует подключения к внешнему миру, применяется специальный шлюз, преобразующий речевые сигналы, передаваемые IP-пакетами, в сигнал, который можно направлять в обычные телефонные системы (местные или междугородные). Этот же шлюз используется также для подключения VoIP-системы к частной телефонной системе PBX, PAX или PABX).

Примечание

Для преобразования IP-адресов в телефонные номера (и наоборот) используется стандарт ITU E. 164.

В области VoIP существует несколько конкурирующих стандартов, и многие производители реализуют их одновременно. Чаще всего используются следующие стандарты:

- ITU H.323;
- Session Initiation Protocol (SIP);
- Media Gateway Control Protocol (MGCP)/MENAGO/H.248.

Далее они рассматриваются более подробно.

Стандарт ITU H.323

Стандарт ITU H.323 изначально был ориентирован на проведение сетевых конференций, однако в нем имеются многие элементы, которые применимы для реализации VoIP-коммуникаций. Этим стандартом предусмотрено несколько типов устройств для голосовой связи. Например, телефонные устройства (терминалы) могут представлять собой комбинацию аппаратных и программных средств, которые вызывающая сторона использует для преобразования речи в IP-пакеты. Модуль многосторонних конференций – это устройство, позволяющее двум или нескольким участникам общаться друг с другом. Диспетчер шлюза используется для управления сеансами и преобразования телефонных идентификаторов или номеров в IP-адреса. И, наконец, сам шлюз служит для подключения IP-сети к аналоговой телефонной системе.

Стандарт ITU H.323 применяется в сочетании с несколькими сопутствующими стандартами для *компрессора-декомпрессора (кодека)* (compression/ decompression, codec) и методов управления голосовыми коммуникациями. Кодек – это программный алгоритм для сжатия речи, видео или комбинированной информации и записи в файл, а также для выполнения обратного преобразования. Примером кодека является стандарт MPEG. Для стандарта ITU H.323 определены следующие кодеки:

- *G. 711* – предусматривает четкое воспроизведение переговоров, использует PCM (см. табл. 10.2) и обычно предназначается для голосовых коммуникаций;
- *G.729a* – обеспечивает более низкое качество речи по сравнению с G.711, однако создает относительно небольшие файлы (т. е. меньше нагружает сеть) и подходит для голосовой почты; использует разновидность ACELP (см. табл. 10.2);
- *G.726* – обеспечивает почти такое же качество речи, как и G.729a, однако файлы получаются большего размера;
- *G.723.1* – обеспечивает более низкое качество речи по сравнению с G.729a и G.726, предназначен для мультимедийных коммуникаций.

Помимо кодеков, стандарт ITU H.323 использует несколько других стандартов для управления голосовыми коммуникациями:

- *H.225* – устанавливает и разрывает телефонные соединения, управляет соединениями и часто реализуется в обработчик вызовов (сервер вызовов);
- *H.245* – устанавливает уникальный канал для каждого вызова;]
- *И.450* – (на самом деле представляет собой набор протоколов от H.45 до H.450.9) обеспечивает дополнительные функции (например, ожидание вызова, удержание вызова или переадресацию вызова).

Совет

Узнать больше о стандартах, связанных со стандартом H.323, можно на **веб-**сайте ITU по адресу **www.itu.int.**

Session Initiation Protocol (SIP)

Session Initialization Protocol (SIP) (Протокол инициализации сеансов) представляет собой созданный группой IETF протокол обмена сигналами, работающий на Прикладном уровне. Он служит для

инициализации и завершения сеанса VoIP-коммуникаций (аналогично стандарту H.225 в составе ГШ H.323). Протокол SIP использует команды, похожие на те, которые применяются в протоколе HTTP. Для адресации используется формат URL. Протокол SIP быстро находит применение в коммуникационных устройствах VoIP, поскольку он может применяться как в Интернете, так и в локальных, региональных и глобальных IP-сетях. Другим достоинством этого протокола является то, что он может использоваться вместе с системами стандарта H.323. 1

Помимо служебных сигналов, в работе SIP-протокола обычно принимают участие несколько следующих компонентов:

- агент пользователя (например, телефон или компьютер);
- сервер размещения, связывающий IP-адреса с конкретными агентами пользователя;
- один или несколько прокси-серверов, позволяющих определить, какие VoIP-службы имеются на других серверах или сетевых устройствах (когда агент пользователя посылает запрос к конкретной службе, прокси-сервер пересылает этот запрос к соответствующему серверу или устройству);
- один или несколько серверов переназначения, которые позволяют агент пользователя, инициировавшему вызов, определить IP-адрес целевого агента.

Совет

Дополнительную информацию о протоколе SIP можно найти на веб-сайте **www.sipcenter.com.**

Media Gateway Control Protocol (MGCP)/MENAGO/H.248

Протокол *Media Gateway Control Protocol (MGCP)* предназначен для управления преобразованиями аудиосигнала для передачи в VoIP-сеть. Он может применяться в телефонном устройстве или в шлюзе, расположенном, например, между VoIP-сетью и обычной телефонной службой. Протокол MGCP использует сравнительно мало служебной информации, поскольку работает с протоколом UDP, обеспечивая передачу аудиосигналов в IP-сети. Достоинством MGCP является его совместимость с сетями, где применяется протокол SIP.

Примечание

Протокол MGCP описан в RFC 2705.

Стандарты MENAGO и H.248 являются расширениями протокола MGCP. Стандарт MENAGO обеспечивает протокол MGCP возможностью передачи видеоизображений • (например, вызывающая сторона может видеть своего собеседника). Стандарт H.248 является протоколом ITU для MGCP и обеспечивает его совместимость с H.323.

Определение полосы пропускания и производительности сети

Применение аудио- и видеотехнологий в сети требует расширения полосы пропускания и увеличения производительности сети. *Полоса пропускания* (bandwidth) характеризует скорость передачи данных в коммуникационной среде, она измеряется в битах за секунду (при передаче данных) и может определяться как разность между максимальной и минимальной передающими частотами. Таким образом, полоса пропускания определяет скорость информационной магистрали. Другим показателем, который следует учитывать, является реальная производительность сети, ее *пропускная способность* (throughput) при передаче всех типов данных. Она зависит от возможностей серверов и количества рабочих станций, работающих в сети с определенной полосой пропускания. Пропускную способность можно рассматривать как объем трафика, передаваемого через определенную точку сети (например, через сервер) за определенный отрезок времени. При подключении большого числа рабочих станций (или если сервер работает медленно) производительность сети понижается, даже если полоса пропускания относительно высокая. Многие сети не полностью используют максимальную полосу пропускания, поскольку не все элементы в них работают с наибольшей эффективностью. Однако максимальная производительность не может превышать общую полосу пропускания.

При проектировании сети вы реализуете ту полосу пропускания, которую обеспечивает выбранная технология (например, 100-мегабитный или 1-гига-байтный Ethernet). Для измерения реальной пропускной способности в некоторой точке сети можно использовать следующие показатели:

- величину загрузки сети, которая представляет собой процент использования сети в конкретный момент времени;
- количество байтов, переданных за секунду;
- количество фреймов, пакетов и датаграмм, переданных за секунду;
- количество файлов, переданных за секунду (или за определенное время);
- количество однонаправленных, широковещательных или групповых посылок, осуществленных за секунду.

После определения сетевой нагрузки, создаваемой некоторым приложением проверьте значения всех перечисленных показателей. Чтобы наиболее полно оценить текущую производительность сети, определите тестовые показатели также называемые базовыми нагрузками, baseline). *Тестовый показатель* benchmark) для сети представляет собой оценку производительности этой сети при различной нагрузке и в разных условиях. Используйте показатели пропускной способности, предложенные выше, и определите следующие тестовые показатели:

- минимальная, средняя и пиковая активность в сети при выполнении задач, типичных для вашей организации;
- минимальная, средняя и пиковая активность в различных точках сети(например, в разных подсетях);
- типовая сетевая активность сервера, обеспечивающего работу аудио/видеоприложений в сети (когда он не передает речь или видео);
- сетевая активность в тот момент, когда только одна рабочая станция получает аудио- или видеоинформацию от сервера;
- сетевая активность в то время, когда максимальное количество рабочим станций (которые, как ожидается, действительно будут работать с аудио/видеоприложением или файлом) получают информацию от сервера.

Нет точной формулы для определения полосы пропускания, достаточной для обеспечения требуемой производительности, поскольку конфигурации сетей различаются. В какой-то сети серверы могут быть плохо настроенными или недостаточно мощными, в результате чего они будут работать медленнее, чем в другой сети. В какой-то сети устройства (например, коммутаторы) могут иметь буферы большего размера, чем аналогичные устройства другой сети. В одной сети все операционные системы могут быть настроены оптимально для достижения максимальной производительности, а в другой сети такого может не быть. Поэтому для получения наилучшего результата нужно тщательно подготовить и обновлять тестовые показатели, которые измеряют пропускную способность и производительность вашей сети. Чем больше времени вы потратите на сбор и изучение показателей конкретной сети, тем лучше будете знать эту сеть. Если вы разобрались с производительностью сети, то вам будет проще судить о том, где потребуется большая полоса пропускания, или как работа некоторых приложений и передача определенных файлов повлияет на пропускную способность сети.

Когда вы получили данные о пропускной способности сети и сопоставили их с требуемой полосой пропускания, убедитесь в том, что выполнены уже знакомые вам основные шаги по улучшению производительности сети. Проверьте, чтобы рабочие станции были настроены должным образом (например, порядок привязки протоколов). Используйте только самые подходящие протоколы в сети и удалите все ненужные. Для управления сетевым трафиком применяйте подсети и соответствующие сетевые устройства.

Совет

Выполните практическое задание 10-5, в котором вы с помощью Сетевого монитора системы Windows 2000 будете определять степень использования сети некоторыми мультимедийными приложениями. Аналогичная задача ставится в практическом задании 10-6, где определяется нагрузка на сеть в системе Red Hat Linux *7.x*.

Перед тем как установить в сети некоторое мультимедийное приложение, доступное всем, необходимо проверить его в лабораторной среде и определить тестовые показатели производительности для этого приложения. Кроме того, поинтересуйтесь у производителя, какая полоса пропускания требуется данному приложению. Вся эта информация позволит вам сравнить запрашиваемые ресурсы с

текущей конфигурацией сети. При этом нужно учитывать:

- мощность сервера и его быстродействие, включая скорость шины и сетевых адаптеров;
- мощность и быстродействие клиентских рабочих станций, включая скорость шины и сетевых адаптеров;
- специальные требования к каналам связи (например, возможность создания групп, транков, из двух или нескольких каналов);
- параметры межсетевых устройств (например, возможности буферизации и создания подсетей и виртуальных локальных сетей, VLAN);
- полосы пропускания подключения к Интернету, а также каналов связи локальной и VPN-сети (т. е. возможности каналов ISDN, DSL, frame relay, SONET и ATM).

Определение времени загрузки отдельного файла

Иногда полезно знать, сколько времени потребуется для загрузки или для передачи отдельного файла (например, файла MPEG). Когда вам известна это время, вы сможете оценить общий эффект, который появится в том *слу*чае, когда к файлу обратится множество людей. Например, если файл передается за две секунды, то вы знаете, что если к файлу обратятся восемь человек, время передачи файла будет, по меньшей мере, равняться 16 секундам. Следует учитывать, что это значение получено для идеальных условий поскольку на самом деле в любой сети существует и другой трафик и конфликты. Общая формула для определения времени, необходимого для загрузки файла, выглядит так: загрузки = файла * 10 / Скорость соединения в бит/с j в секундах в байтах Например, если MPEG-файл имеет размер 4,48 Мбайт (на самом деле 4 697 620 байт) и вы загружаете его по линии T-3, то приблизительное время загрузки этого файла (при наилучших условиях) равно 1,05 с:

1,05 = (4697620) * (10 / 44736000)

Практическое задание 10-7 позволит вам попрактиковаться в определении времени загрузки файла.

Факторы, влияющие на полосу пропускания и пропускную способность

Когда в одной локальной или глобальной сети совместно передаются речи видео и данные (например, при работе мультимедийных приложений), существует несколько важных для сетевых администраторов факторов, влияющих на полосу пропускания и производительность, а именно:

- сжатие файлов и совместимость файловых форматов;
- синхронизация;
- время ожидания;
- джиттер.

Каждый из факторов рассматривается в следующих разделах.

Сжатие файлов и совместимость файловых форматов

Сжатие файлов (file compression) – это процесс, используемый для уменьшения размера обычного файла с помощью методов, рассмотренных выше (например, при помощи сжатия с потерями или двунаправленной интерполяции). Методы сжатия важны потому, что при уменьшении размера файла уменьшается время передачи файла в точку назначения, что влияет на производительность сети. Одни данные (особенно аудио- и видеофайлы, сжатые в MPEG-формат) имеют довольно большой размер, несмотря на то, что они сжаты. Другие данные (например, неподвижные изображения, сжатые в JPEG- или GIF-формат) имеют меньшую длину. Формат GIF (Graphics Interchange Format) был разработан компанией CompuServe, в нем используется метод сжатия файлов без потерь, при котором в процессе обработки никакие данные не удаляются.

Для файлов потокового мультимедиа (например, MPEG-файлов) необходима широкая полоса пропускания, поскольку эти файлы имеют достаточно большой размер и их содержимое не допускает задержек при передаче. Поэтому существует вероятность того, что мультимедийные коммуникации могут прерываться или отдельные фрагменты данных могут теряться при нехватке полосы пропускания или при наличии задержек в сети. В значительной степени это относится к передаче

MPEG-файлов, т. к. в них используется прогностическое кодирование и двунаправленная интерполяция. Если предыдущий или последующий кадры потеряны, то указатели в текущем кадре будут ссылаться на отсутствующую информацию, т. е. один или несколько потерянных кадров сделают бесполезным воспроизведение многих других кадров. Такое свойство интегрированных сетей для передачи речи, видео и данных делают чрезвычайно важным требование наличия достаточной полосы пропускания сети несмотря на то, что мультимедийные программы и плееры могут компенсировать некоторые потери кадров.

Примечание

Область применения стандарта MPEG продолжает расширяться, а с ней растут и требования к полосе пропускания, поскольку MPEG-файлы требуют большей полосы, чем многие другие файлы. Зато MPEG-файлы обеспечивают высококачественное воспроизведение видео- и аудиосигналов, которые к тому же можно редактировать.

Синхронизация

При совместной передаче речи, видео и данных по сети вся эта информация должна быть синхронизирована программами у получателя, т. е. нужно, чтобы все последовательные фрагменты были собраны и воспроизведены в правильном порядке. Синхронизация надежнее всего в тех случаях, когда имеется полоса пропускания, достаточная для приложения, благодаря чему отсутствуют потери разрядов или кадров, а также нет слишком больших задержек, вызванных перегрузкой сети. Синхронизация полученной информации становится еще сложнее, если часть информации или все данные сжаты и должны быть распакованы и синхронизированы одновременно.

В потоковых мультимедийных приложениях это нужно делать сразу же при получении информации. Иногда аудиосигналы смешиваются из разных источников, и получаемый сигнал требует дополнительной синхронизации.

На рис. 10.3 показаны операции, которые выполняются у получателя мультимедийной информации при потоковом

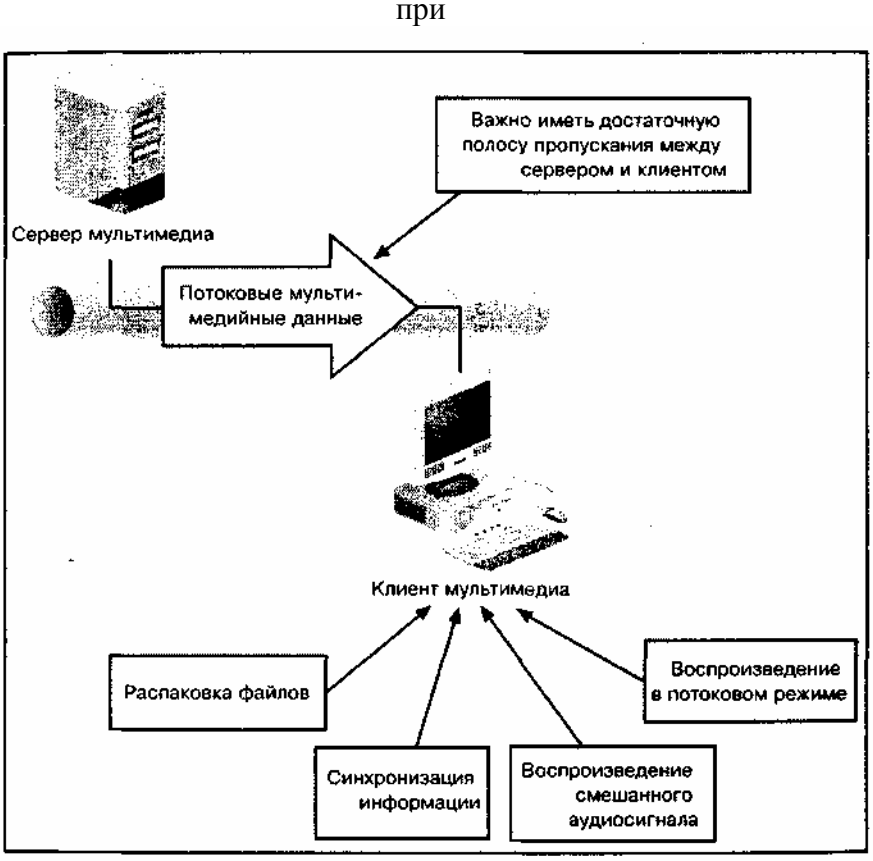


Рис. 10.3. Разнообразные действия клиента мультимедийного потока

воспроизведении.

Время ожидания

Интефированные приложения (например, аудио- и видеоконференция предполагают равномерную скорость доставки данных по сети, чтобы движения и звук были синхронизированы и не было бы подергиваний и при воспроизведении. Время, необходимое для передачи информации

передающего устройства к принимающему, называется временем ожидания (latency). Если полоса пропускания сети недостаточна, время ожидания увеличивается. Задача хорошо спроектированной сети для интегрирования мультимедийных приложений – обеспечить минимальное время ожидания и минимальное его изменение. Например, глобальные сети на основе телекоммуникационных каналов должны иметь время ожидания не более 400 мс. Большинство локальных сетей рассчитаны на такое же время ожидания.

На время ожидания в сети влияют следующие факторы:

- *задержка передачи* (transmission delay), т. е. время, в течение которого пакет перемещается в сетевой среде (например, в кабеле 10BaseT с максимальной скоростью передачи 10 Мбит/с или в кабеле 100BaseTX с максимальной скоростью 100 Мбит/с). Помимо скорости коммуникационной среды, на задержку передачи также влияет размер пакета;
- *задержка при распространении* (propagation delay), представляющая собой время, необходимое пакету для прохождения всего сегмента или всей сети. Такие задержки обычно относятся к оптоволоконной среде и скорости светового сигнала в этой среде;
- задержка на обработку (processing delay);
- задержка промежуточного хранения (store-and-forward delay) или задержка коммутации (switching delay).

Джиггер

Джиггер (jitter) – флуктуации (разброс значений) времени ожидания в сети, вызывающие заметные ошибки в доставке мультимедийного сигнала (например, щелчки и треск при воспроизведении аудиосигнала или подергивания и паузы при воспроизведении видеоизображений).

Величина джиггера определяется путем вычитания минимального значения времени ожидания из максимального значения. Например, если минимальное время ожидания составляет 200 мс, а максимальное – 520 мс, то величина джиггера составит 320 мс, что довольно много. Мультимедийные приложения могут в некоторой степени компенсировать джиттер, запоминая данные в буферах как на передающем, так и на принимающем компьютере, и подстраивая синхронизацию при воспроизведении. Буферы в межсетевых устройствах (например, в коммутаторах) также помогают уменьшить потери кадров при высоком джиггере. Если большой джиттер возникает часто, необходимо проверить, нет ли в мультимедийном приложении ошибок разработчиков, а также правильно ли сконфигурированы межсетевые устройства. Для знакомства с джиттером выполните практическое задание 10-8.

Передача мультимедийной информации в локальных и глобальных сетях

Мультимедийные коммуникации (т. е. передача речи и видеоизображений) обычно осуществляются между двумя устройствами (отправителем и получателем) в локальной или глобальной сети, а также в смешанных сетях. Существуют различные способы доставки мультимедийной информации в сети. При выборе некоторых способов сетевые ресурсы (например, маршрутизаторы) используются весьма эффективно, благодаря чему уменьшается нагрузка на сеть, вызванная наличием мультимедийных коммуникаций. Другие способы (особенно те, которые применяются в устаревших мультимедийных программах) создают довольно высокий сетевой трафик. В следующих разделах будет рассказано о трех методах пересылки данных в сети которые могут использоваться мультимедийными программами, и вы сможете сравнить влияние каждого из методов на работу сети.

Методы пересылки информации

В том случае, когда в локальной или глобальной сети развернуты мультимедийные приложения, важно определить, является ли создаваемый ими трафик однонаправленным, широковещательным и/или многоадресным (групповым). Некоторые приложения могут использовать только один тип пересылки информации, а другие программы могут работать в нескольких режимах. Если вы знаете, какой тип трафика генерируется некоторым приложением, то вам будет легче планировать полосу пропускания, необходимую для развертывания этого приложения в сети.

В табл. 10.3 перечислены и описаны все три типа пересылки данных. Рис. 10.4 служит в качестве иллюстрации.

Таблица 10.3. *Методы пересылки мультимедийных данныц*

Тип передачи	Описание	Ограничения
Однонаправленная передача (Unicast)	При однонаправленной передаче данных одна копия каждого фрейма или пакета передается в каждый целевой узел, обратившийся за информацией к мультимедийному приложению. Например, если к приложению обращаются четыре рабочих станции, посылаются четыре копии каждого фрейма или пакета: по одной копии для каждой станции. Приложения с однонаправленным вещанием не требуют реализации специальных сетевых протоколов, поэтому они относительно просты в разработке. Кроме того, однонаправленный трафик является двухточечным, поскольку отправитель передает один пакет каждой рабочей станции, принимающей данные от приложения.	Мультимедийные приложения, использующие однонаправленную передачу, трудно масштабировать при увеличении числа пользователей. Если пользователей много, создается высокий трафик, что требует увеличения полосы пропускания
Широковещание (Broadcast)	При широковещательных посылках одна копия каждого фрейма или пакета рассылается всем узлам сети вне зависимости от того, запрашивала или нет некоторая рабочая станция эту информацию. Например, если в сети 100 рабочих станций, компьютер-отправитель передает один фрейм или пакет, который размножается концентраторами, коммутаторами и мостами для всех станций, включая те, которые и не обращались к приложению. Если сеть содержит мосты или коммутаторы, широковещательный трафик можно контролировать, создавая фильтры, ограничивающие распространение широковещательных фреймов или пакетов. Широковещательные рассылки являются примером многоточечного трафика, поскольку отправитель генерирует один фрейм или пакет, передаваемый всем узлам	Широковещательный мультимедийный трафик (если он не фильтруется межсетевыми устройствами) может быть даже больше, чем однонаправленный, поскольку он может распространяться на большее количество целевых узлов
Многоадресное (групповое) вещание (мультивещание многоабонентская доставка-(Multicast)	Многоадресное вещание является еще одним примером многоточечного трафика, при котором отправитель генерирует один фрейм или пакет для передачи всем клиентам. При мультивещании создаются группы, в которые включаются те рабочие станции, которые запросили доступ к мультимедийному приложению, сообщений). Один пакет передается одной или нескольким группам, для чего совместно используется MAC- и IP-адресация, Группы идентифицируются и образуются с учетом MAC- и IP-адресов компьютеров. Многоадресный трафик	Оценивая три перечисленных метода, труднее всего разработать приложения, использующие многоадресное вещание однако такие усилия в полной мере оправдываются за счет улучшенной управляемости сети и более оптимального распределения

Тип передачи	Описание	Ограничения
	распространяется только на те рабочие станции, которые входят в группы станций, запросивших информацию от приложения	трафика

Рис. 10.4. Однонаправленная передача, широковещание и многоадресное вещание

Применение различных методов вещания для одного и того же приложения

Сервер видеоизображений, передающий клиентам MPEG-файлы в протокольном режиме, требует полосы пропускания приблизительно 1,5 Мбит/с в расчете НЗ одного клиента. Если приложение рассчитано на однонаправленную передачу, сервер генерирует трафик, объем которого равен значению 1,5 Мбит/с, умноженному на число клиентов (например, для пяти клиентов трафик составит 7,5 Мбит/с). Если сервер подключен по 10-мегабитному каналу, шесть или семь клиентов полностью займут полосу пропускания сети. При широковещании степень использования полосы пропускания будет не меньше или даже выше.

Если это же приложение будет работать в режиме многоадресного вещания, степень использования полосы пропускания уменьшится до 1,5 Мбит/с вне зависимости от числа клиентов. Рассмотрим, к примеру, сеть, в которой имеются четыре маршрутизатора. Две станции, подключенные к одному маршрутизатору, входят в одну группу клиентов мультимедийного приложения, а пять станций, подключенных к одному из оставшихся маршрутизаторов, входят во вторую группу. При мультивещании один отправленный пакет достигает обоих маршрутизаторов, а

они, в свою очередь, передают информацию так, что она будет получена только теми клиентами, которые входят в соответствующие группы, подключенные к конкретному маршрутизатору (т. е. двумя клиентами для первого маршрутизатора и пятью клиентами – для второго).

Наличие средств для многоадресной групповой адресации на Уровнях 2 и 3 модели OSI означает, что вы можете использовать этот метод передачи данных для того, чтобы учесть топологию сети. Например, если топология представляет собой отдельную локальную сеть, то, скорее всего, будет достаточно MAC-адресации Уровня 2. Если в сети используются несколько сегментов, маршрутизация и подключения к глобальным сетям, то адресация Уровня 3 позволит задействовать все преимущества маршрутизации. Это особенно важно в развитых интрасетях, VPN-сетях и при наличии подключений к Интернету, при этом могут использоваться любые комбинации технологий Ethernet, Token Ring, FDDI и ATM.

Назначение протокола IGMP

Internet Group Management Protocol (IGMP) (Межсетевой протокол управления группами) представляет собой протокол Уровня 3, используемый для определения клиентов, которые входят в группы многоадресных рассылок, и для передачи этой информации сетевым маршрутизаторам.

Протокол IGMP устанавливается на сервере и клиентах мультимедиа, а также на маршрутизаторах и коммутаторах. Он позволяет клиентам посылать и отзывать заявки на обслуживание некоторым мультимедийным приложением, для этого используются запросы на подписку и на прекращение подписки (также называемые запросами на вступление в группу и на выход из группы). Для пересылки этих запросов служит *сообщение о членстве хоста* (HostMembership Report), отправляемое с помощью протокола IGMP. Согласно стандарту IPv4, это сообщение имеет IP-адрес Класса D *(см. главу 6)* в форма-1 те 244.0.XX. Клиент может отказаться от подписки в любой момент, это не влияет на текущие передачи информации другим клиентам, относящимся к этой же группе или к другим группам. Маршрутизаторы периодически посылают клиентам IGMP-запросы, чтобы удостовериться в том, что этот клиент по-прежнему подписан на обслуживание. Если клиент не отвечает, маршрутизатор обновляет свои таблицы, где указывается на то, что данный клиент более не входит в группу, принимающую информацию.

Дополнительные протоколы, обеспечивающие многоадресное вещание

Помимо IGMP, для поддержки многоадресного вещания маршрутизаторы используют один из трех других протоколов маршрутизации:

- Distance Vector Multicast Routing Protocol (DVMRP);
- Multicast Open Shortest Path First Protocol (MOSPF);
- Protocol Independent Multicast (PIM).

Протокол *Distance Vector Multicast Routing Protocol (DVMRP)* (Протокол дистанционной маршрутизации сообщений с использованием векторной многоканальной трансляции) работает вместе с протоколами IGMP и RIP *(см. главу 4Ш* и служит для определения принадлежности рабочих станций к некоторой группе мультивещания. Сначала он предполагает, что все станции подписаны, а затем постепенно удаляет их из группы, если те не отвечают. Если оказывается, что целый сегмент не содержит членов группы, протокол останавливает пересылку многоадресных пакетов в этот сегмент.

Протокол DVMRP также выполняет следующие операции:

- каждые 60 секунд проверяет наличие новых подписчиков;
- с помощью алгоритма Бельмана–Форда (Bellman–Ford) позволяет маршрутизаторам определять количество ретрансляций (расстояние между конкретным маршрутизатором и другими маршрутизаторами) ко всем другим маршрутизаторам сети;
- позволяет маршрутизатору определить, в каком направлении (называемом вектором) посылать по сети пакет, чтобы тот мог достигнуть определенного маршрутизатора с минимальным количеством ретрансляций.

Протокол *Multicast Open Shortest Path First Protocol (MOSPF)* в работе напоминает протокол OSPF *(см. главу 4)*. Используя информацию, переданную! по протоколу IGMP между сервером и подписанным клиентом, он определяет, какие рабочие станции являются членами группы многоадресной рассылки. Он постоянно следит за сетью и находит кратчайшие маршруты между сервером и членами каждой группы. MOSPF не совместим с RIP и должен применяться только в тех сетях, где в качестве основного протокола маршрутизации используется OSPF.

Протокол *Protocol Independent Multicast (PIM)* (Многоадресное вещание, не зависящее от протокола) существует в двух разновидностях: Dense-mode PIM и Sparse-mode PIM. Обе разновидности работают вместе с протоколом IGMP.

Протокол Dense-mode PIM (PIM в "плотном" режиме) совместим как с RIP, так и с OSPF. Подобно протоколу DVMRP, он собирает информацию о подписанных рабочих станциях, опрашивая все сетевые станции и постепенно удаляя те из них, которые не отвечают. Dense-mode PIM используется в тех случаях, когда в некоторой части сети располагается много членов группы и когда имеется широкая полоса пропускания.

Протокол Sparse-mode PIM (PIM в "разряженном" режиме) рассматривает маршрутизаторы как промежуточные точки для определения кратчайших маршрутов между сервером мультимедиа и членами группы. Затем он посылает многоадресные пакеты только тем маршрутизаторам, которые выбраны в качестве промежуточных точек, и с их помощью пересылает пакеты подписанным рабочим станциям. Sparse-mode PIM предназначен для использования в тех сетях, где члены группы разбросаны по удаленным подсетям (например, по Интернету).

Совет

Многоадресные рассылки в сетях, где используются коммутаторы и нет маршрутизаторов, полностью зависят от протокола IGMP. На каждом коммутаторе при наличии IGMP-пакетов строятся фильтры. Если коммутатор обнаруживает IGMP-пакет в одном из своих исходящих портов, он добавляет эту информацию в фильтр, а затем просто пересылает многоадресный трафик через этот порт.

Примечание

В зависимости от возможностей конкретного коммутатора может оказаться так, что фильтры для многоадресных рассылок нужно будет строить вручную. Если в коммутаторе нет возможности фильтрации, то многоадресные пакеты будут обычным образом проходить в каждый порт.

Протоколы для многоадресного потокового вещания в реальном масштабе времени

Описанный в RFC 1889 протокол *Real Time Protocol (RTP)* (Протокол реального времени) был создан для лучшего управления многоадресным потоковым вещанием в реальном масштабе времени, которое применяется при проведении видеоконференций и в аналогичных приложениях. Для передачи потоковых данных заголовки пакета RTP пересылаются с помощью протокола UDP (а не при помощи протокола TCP, входящего в стек TCP/IP).

Работа поверх UDP означает, что UDP-пакет содержит заголовок RTP и полезную нагрузку. В заголовке находится информация о последовательных пакетах, данные для синхронизации видео- и аудиофреймов, а также указание на то, как данные закодированы или сжаты для передачи по сети полезной нагрузки).

Совет

В RFC 1890 описано свыше 120 типов полезной нагрузки, представляющей собой аудио- и видеоинформацию.

Другой протокол, *Real Time Transport Control Protocol (RTCP)* (Протокол управления доставкой в реальном времени), был создан для того, чтобы позволить сетевым администраторам и разработчикам применять методы компенсации искажений в тех случаях, когда сетевые проблемы влияют на качество работы мультимедийных приложений реального времени.

С помощью многоадресных пакетов протокол RTCP позволяет устанавливать качество обслуживания (QoS) для сеансов связи по протоколу RTP RTCP собирает сообщения о членстве от получателей и обеспечивает отправителя обратной связью, сообщающей о заданном качестве обслуживания и о состоянии сети (например, о перегрузке или джиггере). Рассмотрим, к примеру, приложение, которому для передачи цветного видеосигнала и стереофонического аудиосигнала требуется полоса пропускания глобальной сети, построенной на базе линий T-1. Когда канал T-1 недоступен и используется резервный канал со скоростью 56 Кбит/с, протокол RTCP может

предоставить средства для передачи черно-белого видеосигнала и монофонического аудиосигнала. Также этот протокол позволяет сетевым администраторам использовать средства для анализа производительности сети с мультивещанием и для определения количества подписанных рабочих станций.

Приложения и межсетевые устройства

В Интернете или в корпоративных сетях мультимедийные приложения должны передавать данные через разнообразные межсетевые устройства; настроенные по-разному для пересылки различного типа трафика. Неоднородность сетевых настроек создает проблемы для мультимедийных коммуникаций, которым требуется минимальный набор определенных ресурсов.

С этой задачей помогает справиться протокол *Resource Reservation Protocol*[2] *(RSVP)* (Протокол резервирования ресурсов).

Протокол RSVP позволяет некоторому приложению зарезервировать нужные ему ресурсы (например, полосу пропускания, буферы и класс обслуживания) (рис. 10.5). С помощью RSVP мультимедийные приложения с потоковым воспроизведением могут сосуществовать с приложениями, передающими данные в виде блоков, однако мультимедийным приложениям дается более высокий приоритет доставки, поскольку они в меньшей степени допускают задержку передачи. Также протокол RSVP удобен для динамического выделения ресурсов при добавлении рабочих станций в группу многоадресного вещания. В некоторых случаях он позволяет просто включить новых подписчиков в группу и использовать ресурсы, уже назначенные этой группе (т. е. не менять распределение ресурсов). Более того, отдельные клиентские рабочие станции, входящие в группу, могут запросить другие ресурсы. Например, клиент может пожелать отключить звук или изображение в передаваемом потоке.

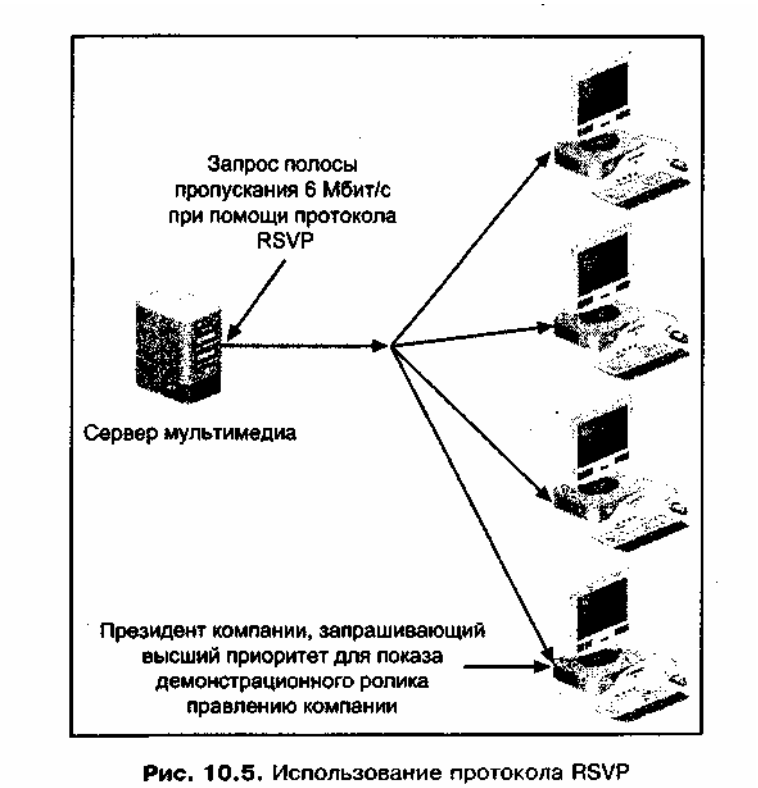


Рис. 10.5. Использование протокола RSVP

Примечание

Протокол RSVP динамически выделяет ресурсы по мере увеличения или уменьшения потребностей. Однако при этом он использует параметры, тщательно подобранные сетевым администратором и гарантирующие минимум полосы пропускания и других ресурсов.

Подготовка локальных и глобальных сетей к развертыванию мультимедийных приложений

При проектировании локальных и глобальных сетей для мультимедийных приложений следует учитывать множество факторов. Например, в некоторых случаях вам может встретиться сеть на базе устаревшего оборудований (с концентраторами и коаксиальным кабелем), которое нужно обновить перед тем как развертывать приложения. В других случаях для существующей сети могут

понадобиться дополнительные устройства, такие как маршрута, заторы и коммутаторы, позволяющие повысить производительность сети.

Следующие разделы главы помогут вам понять, как модернизировать существующие сети для развертывания мультимедийных приложений, как реализовать высокоскоростные технологии Ethernet в мультимедийных локальных сетях и как спроектировать глобальную сеть, которая без проблем смогла бы поддерживать мультимедийные программы.

Модернизация существующей сети для развертывания мультимедийных приложений

В некоторых существующих офисных и кампусных локальных сетях полоса пропускания не отвечает требованиям мультимедийных приложений, таких как средства организации видеоконференций или интерактивные мультимедийные классы. Зачастую проблема заключается не в самой коммуникационной среде, а в неэффективной реализации и сегментации локальной сети. Например, в существующей локальной сети можно значительно расширить полосу пропускания, заменив концентраторы (рис. 10.6) на коммутаторы (рис. 10.7) и заменив старый "тонкий" коаксиал и повторители на витую пару Категории 5 и коммутаторы 100BaseTX. Маршрутизатор, помещенный между серверами мультимедиа и областью коллизий, где располагаются рабочие станции, также является эффективным средством сегментации трафика и повышения сетевой безопасности. Кроме того, он позволяет конфигурировать различные протоколы, используемые для многоадресного

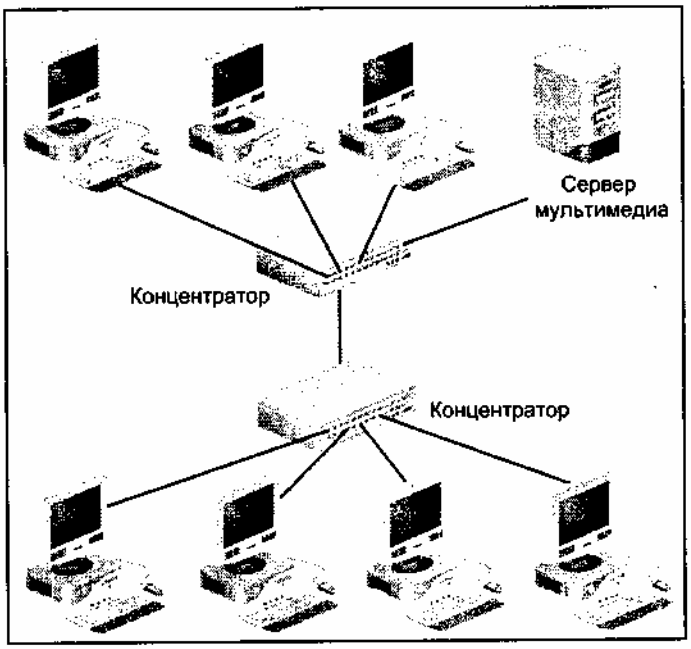


Рис. 10.6. Существующая сеть на основе концентраторов

вещания.

При выборе коммутаторов для локальной сети следует обращать внимание на такие устройства, которые имеют возможность многоадресной фильтрации и буферизации, а также обеспечивающие малое время ожидания (например, такие, в которых используются специализированные интегральные схемы (ASIC) и коммутация без буферизации пакетов). Наличие многоадресной фильтрации особенно важно, т. к. без нее многоадресные пакеты могут заполнить сеть подобно широковещательным пакетам. Кроме того, коммутаторы должны иметь настройки для организации виртуальных локальных сетей (VLAN), что позволит контролировать размер и область охвата домена многоадресного вещания.

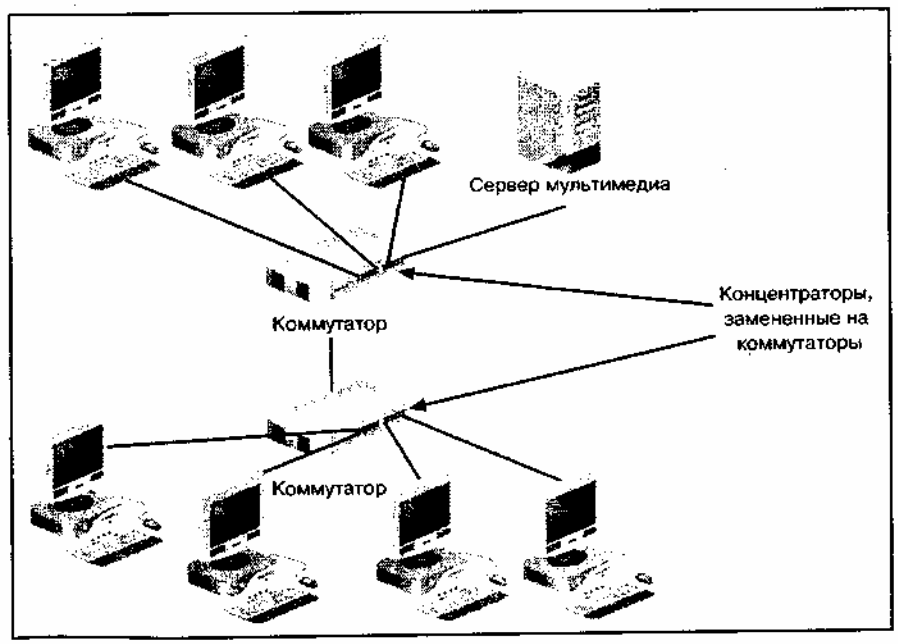


Рис. 10.7. Замена концентраторов на коммутаторы

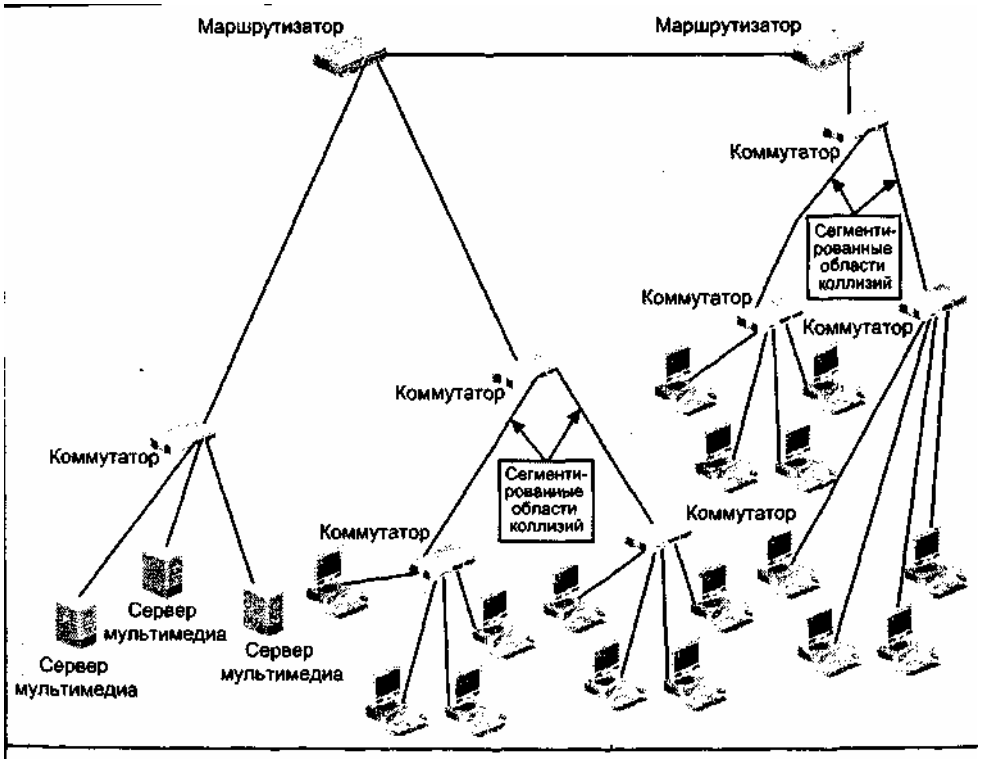


Рис. 10.8. Использование маршрутизаторов в мультимедийных сетях

где одним способом увеличения производительности и безопасности существующей сети, в которой развертываются мультимедийные средства, является включение в нее маршрутизаторов, совместимых с протоколами многоадресной (групповой) маршрутизации. Маршрутизаторы можно использовать для сегментации трафика и для изолирования областей коллизий. В тех случаях, когда нужны VLAN-сети, маршрутизаторы позволят им взаимодействовать друг с другом для улучшения контроля за многоадресными пакетами. Как показано на рис. 10.8, маршрутизаторы являются важным средством распределения трафика по мере роста сети и увеличения объема пересылаемых мультимедийных данных.

Совместное использование Fast Ethernet и Gigabit Ethernet в мультимедийных локальных сетях

Для многих локальных сетей, в которых развернуты мультимедийные приложения, одним из самых эффективных (в плане рентабельности решений и надежности технологий) будет сочетание Fast Ethernet и Gigabit Ethernet. В такой архитектуре предполагается, что технология Fast Ethernet будет использоваться для подключения пользователей, а технология Gigabit Ethernet (или даже 10 Gigabit Ethernet в очень загруженных сетях) послужит для создания магистрали. Подобное решение позволит избежать перегрузки магистрали и обеспечить достаточную полосу пропускания для рабочих станций, получающих информацию от мультимедийных приложений.

Примечание

Технология FDDI *(см. главу 2)* также обеспечивает передачу данных со скоростью 100 Мбит/с, используя архитектуру двойного кольца с избыточностью. Обычно эта технология обходится дороже, чем Fast Ethernet, однако ее вполне можно рассматривать как альтернативное решение (в некоторых случаях), особенно в тех организациях, где она уже применяется для создания магистрали, а серверы собраны в одном месте (в серверную группу).

Fast Ethernet обеспечивает полосу пропускания не ниже 100 Мбит/с по неэкранированной витой паре (UTP) или одно/многомодовому оптоволоконному кабелю. В зависимости от типа выбранного сетевого коммутатора эту полосу можно увеличить до 200 Мбит/с, для чего используется дуплексный режим.

Достоинством каналов Gigabit Ethernet является то, что их можно группировать (объединять в транки), т. е. между устройствами магистрали Gigabit Ethernet (например, маршрутизаторами или

коммутаторами) можно проложить два или три кабеля. Например, если сгруппировать два кабеля между двумя коммутаторами Gigabit Ethernet, можно получить суммарную полосу пропускания в 2 Гбит/с. При группировке трех каналов полоса будет 3 Гбит/с. При этом достигается избыточность (резервирование), поскольку в случае отказа одного из каналов группы другой кабель сможет обеспечивать скорость 1 Гбит/с (в случае двух каналов). Еще одно достоинство сгруппированных каналов Gigabit Ethernet заключается в том, что для повышения производительности и во избежание конфликтов можно использовать дуплексные коммуникации.

Комбинированная архитектура Fast Ethernet и Gigabit Ethernet обеспечит полосу пропускания, которая позволит в полной мере использовать многие особенности структуры сети, включая высокоскоростную связь между клиентами и серверами (а также между коммутаторами) и дуплексные коммуникации (отсутствие конфликтов), что фактически удваивает полосу пропускания и, следовательно, значительно увеличивает производительность сети.

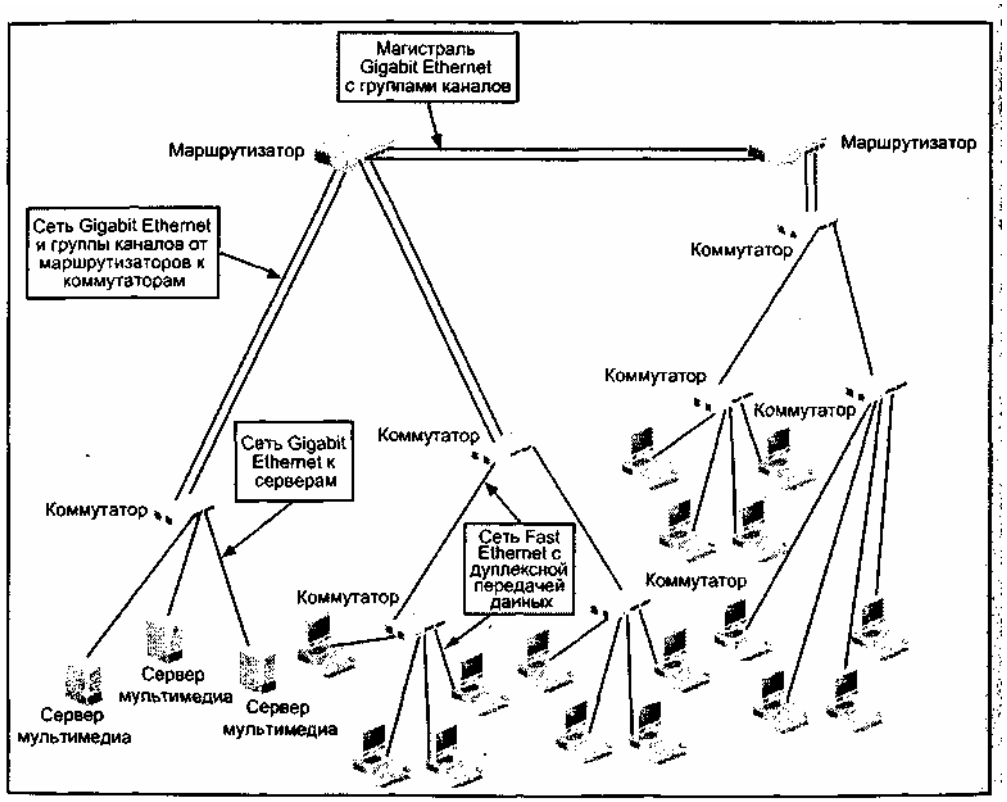


Рис. 10.9. Использование Fast Ethernet и Gigabit Ethernet для мультимедийных коммуникаций

Другим способом расширения полосы пропускания является непосредственное подключение серверов мультимедиа к каналам Gigabit Ethernet (если используются быстродействующие серверы с быстрыми шинами, например, на базе процессоров RISC или Itanium). Такое решение особенно хорошо работает при осуществлении комбинированных аудио/видеокоммуникаций, когда сервер должен обеспечивать доставку множества мультимедийных потоков. Насколько полно сервер сможет использовать высокоскоростные подключения к Gigabit Ethernet – зависит от процессора этого сервера и архитектуры шины, а также от установленной операционной системы. Например, для подключения к Gigabit Ethernet вполне подойдет сервер с процессором RISC или Itanium, работающий под управлением UNIX или Windows 2000.

При использовании сетевой архитектуры, изображенной на рис. 10.8, для реализации мультимедийных коммуникаций можно выбрать каналы Gigabit Ethernet между магистральными маршрутизаторами, а также между коммутаторами и подключенными к ним коммутаторами. Для подключения серверов также можно использовать каналы Gigabit Ethernet, а для подключения станций – каналы Fast Ethernet. При этом следует использовать коммутаторы и сетевые адаптеры, обеспечивающие дуплексные коммуникации. Структура такой сети показана на рис. 10.9. (Более подробно об общих принципах проектирования сетей и группировании каналов рассказывается в *главе 11.)*

Существуют и другие топологии, альтернативные комбинации Fast Ethernet и Gigabit Ethernet, такие как ATM, однако они дороже и сложнее в реализации. Например, можно вместо Gigabit Ethernet

использовать ATM-сеть в качестве магистрали локальной сети. Более того, можно с помощью глобальной ATM-сети или сети на базе SONET соединить две локальных ATM-сети, в которых интенсивно передаются потоковые видеоизображения.

Примечание

Дополнительная информация о реализациях сетей ATM и SONET имеется на веб-сайтах **www.atmforum.com и www.atis.org.**

Проектирование глобальных сетей, поддерживающих мультимедийные приложения

Если две локальные сети связываются с помощью глобальной сети для доставки речи, видео и данных на большие расстояния, то используемая глобальная сеть должна быть согласована со скоростью соединенных локальных сетей и требованиями приложений, в них работающих. При выборе поставщика услуг глобальной связи следуйте перечисленным рекомендациям:

- согласуйте полосу пропускания глобальной сети с той полосой, которая требуется локальными сетями и прикладными программами;
- выбирайте службу глобальной связи, пригодную для передачи речи, видео и данных, а также для проведения конференций и работы мультимедийных приложений;
- ищите поставщика услуг, который может предоставить вам соглашение об уровне сервиса (service level agreement, SLA), гарантирующее соответствие глобальной сети потребностям вашей организации;
- для ответственных глобальных коммуникаций используйте службу, которая может предложить качество обслуживания (QoS).

Для больших организаций, выходящих за рамки территориальной сети, службы глобальных коммуникаций, которые вероятнее всего будут соответствовать перечисленным критериям, включают сети ATM, SONET и B-ISDN. Для организаций, которые нужно связать в пределах города, чаще предлагаются региональные сети на базе Optical Ethernet (Gigabit Ethernet и 10 Gigabit Ethernet). Для небольших организаций и индивидуальных пользователей можно использовать линии DSL и кабельные модемы.

Все перечисленные службы глобальных коммуникаций могут обеспечить скорость свыше 100 Мбит/с и совместимы с мультимедиа. ATM-сети также предоставляют качество обслуживания (QoS), т. е. они выделяют свою полосу пропускания для каждой прикладной задачи, такой как передача мультимедиа *(см. главу 8).* Физические линии глобальных сетей, которые могут обеспечить высокоскоростные коммуникации, реализованы с использованием технологий коммутации каналов (коммутируемые каналы 56 Кбит/с, коммутируемые линии T-1, T-3, а также B-ISDN). Другая альтернатива – сеть frame relay, подключенная к каналам T-3. Она обеспечивает скорость 45 Мбит/с.

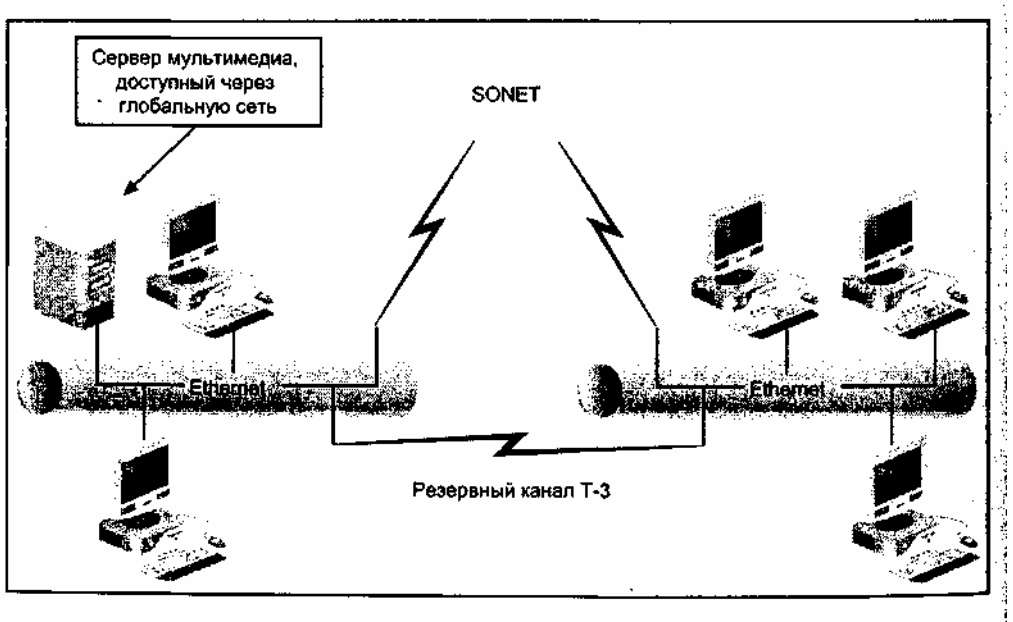


Рис. 10.10. Структура глобальной сети с резервным каналом

В первую очередь необходимо тщательно изучить технологии глобальных сетей, имеющиеся в вашем регионе, и провести сравнение услуг и цен. Цены могут различаться не только в зависимости от типа услуг, но в зависимости от используемых каналов, качества обслуживания (QoS) и соглашения об уровне сервиса. Кроме того, в некоторых случаях вам могут потребоваться несколько типов услуг, особенно для резервных служб при осуществлении ответственных глобальных коммуникаций. Например, для основной службы может использоваться SONET, а резервной линией может служить выделенная линия Т-3, как показано на рис. 10.10.

Уменьшение стоимости глобальной сети и увеличение ее производительности

Одним из способов уменьшения стоимости и увеличения эффективности использования соединений с глобальными сетями является планирование глобальных коммуникаций и времени работы приложений.

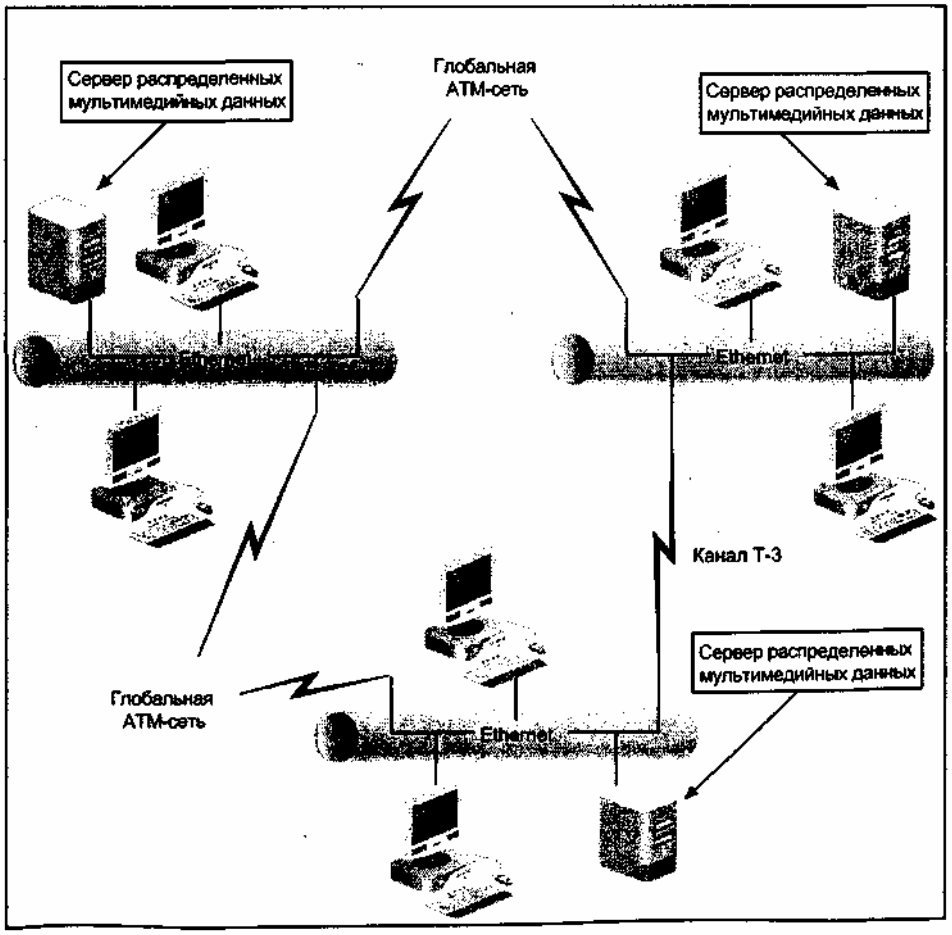


Рис. 10.11. Распределение серверов мультимедиа по глобальной сети

Ответственные приложения (например, проведение видеоконференций) обычно используются в дневные часы (когда издержки велики), однако работа других приложений (например, передача видеоклипов для тренинга и обучения) может быть запланирована на нерабочее время.

Другим решением является размещение нескольких серверов видеоинформации в разных точках локальной или глобальной сети (рис. 10.11). В течение дня пользователи будут обращаться к локальным серверам за мультимедийной информацией, а по ночам (когда трафик в глобальной сети меньше) серверы смогут обновлять видеоинформацию, т. е. если новый курс или!; учебный модуль будет установлен на одном сервере, он будет копироваться; по глобальной сети на другие серверы. Система Windows 2000 Server, например, имеет программно реализуемую распределенную файловую систему, (Distributed File System, DPS), которая может автоматически копировать (реплицировать) файлы и каталоги с одного сервера на другой.

Возможности устройств, позволяющие увеличить производительность глобальной сети

Устройства некоторых производителей позволяют увеличить производительность глобальной сети, для чего в них реализуются специальные функции, в т. ч. "моментальная" маршрутизация, спуфинг IPX/SPX и полоса пропускания по запросу. "Моментальная" маршрутизация (маршрутизация

с вызовом по требованию) представляет собой технологию, при использовании которой интерфейсы маршрутизатора фактически находятся в выключенном состоянии до тех пор, пока в интерфейсе не появится трафик. При возникновении трафика маршрутизатор обращается к удаленным маршрутизаторам (или дозванивается до них) и обновляет свои таблицы маршрутизации, после чего передает пакеты на линию связи. Такой способ маршрутизации применяется для того, чтобы уменьшить время активности линии, благодаря чему каналы, связанные с этой линией, могут использоваться другими службами владельца каналов или другими клиентами.

Примечание

При наличии таких подключений к глобальной сети, когда маршрутизаторы связаны между собой коммутируемыми линиями и модемами, маршрутизатор инициирует процесс установление связи.

Другой полезной функцией является спуфинг IPX/SPX, который используется в глобальных сетях, передающий трафик серверов NetWare старых моделей. Эти серверы рассылают клиентам специальные тестовые пакеты (watchdogs), которые поддерживают соединение активным в течение заданного интервала времени. Когда клиент неактивен (например, когда он зарегистрирован на сервере, но в данный момент не обменивается с ним данными), такие пакеты передаются каждые несколько минут. Если множество клиентов сети подключается к серверу удаленно, такие пакеты могут создать значительный трафик в локальной и глобальной сетях. Спуфинг IPX/SPX позволяет маршрутизатору глобальной сети посылать ответы серверу для поддержания соединения в активном состоянии, уменьшая таким образом трафик от всех подключенных клиентов.

Примечание

На клиентских компьютерах, работающих под управлением Windows 98, Windows 2000 или Windows XP, можно также увеличить интервал посылки тестовых IPX-пакетов, изменив его значение в системном реестре.

Совет

Для повышения производительности глобальной сети лучше всего установить новые версии системы NetWare, которые поддерживают протокол TCP/IP и делают ненужным использование протокола IPX/SPX в глобальной сети.

Еще одной функцией, которую используют поставщики услуг глобальных сетей, является выделение полосы пропускания в соответствии с текущими требованиями приложения или трафика. Эта функция называется "полоса пропускания по запросу". Например, некоторые поставщики услуг могут располагать оборудованием, которое может увеличивать или уменьшать количество используемых ресурсов в зависимости от текущего трафика. Другие поставщики услуг могут использовать маршрутизаторы, поддерживающие списки доступа, согласно которым ресурсы глобальной сети выделяются в соответствии с тем, кто к этой сети обращается. Адрес клиента определяет тип и величину задействованных ресурсов.

Другим механизмом, напоминающим функцию "полоса пропускания по запросу", является маршрутизация на основе политик, используемая в тех случаях, когда имеется несколько линий (в том числе резервные линии). Политики использования ресурсов могут быть заданы такими, что трафик с низким приоритетом (например, передача файлов) передается через медленные резервные линии (скажем, через линии T-1). Трафик с высоким приоритетом или не допускающий задержек по времени (например, мультимедийный) будет пересылаться по быстрым ATM- или SONET-каналам. Помимо оптимизации полосы пропускания, политики можно также применять для обеспечения безопасности. Например, исследовательский университет, имеющий каналы глобальной сети с Национальным центром атмосферных исследований США, может использовать низкоприоритетную линию T-3 для обычного и менее важного трафика (например, для передачи электронной почты), а высокоприоритетный канал SONET может применяться для передачи секретных исследовательских данных на суперкомпьютеры.

Службы каталогов, такие как Active Directory, могут генерировать значительный трафик в глобальной сети при репликации данных каталога между серверами Windows 2000 или Windows Server 2003. При использовании Active Directory проверьте настройку периодов репликации и выберите связи сайтов для репликации так, чтобы минимизировать излишний трафик, возникающий при репликации.

Перспективы развития мультимедийных средств

Мультимедийные коммуникации стали значительно сложнее, они постепенно и незаметно сливаются с традиционными операциями передачи данных. Кроме того, объединяются телефония, телевидение и компьютерные технологии, в результате чего появляются такие средства, как интернет-телефония, цифровое телевидение и операционные системы (например, Red Hat Linux *7.x* и Windows XP) с мультимедийными возможностями. Многие из нас уже встречались с интегрированными технологиями в следующих областях:

- аудио- и видеоконференции;
- компьютерная профессиональная подготовка;
- цифровое и интерактивное телевидение;
- промышленное роботостроение и управление механизмами;
- компьютерные киоски для информационных служб;
- интерактивные игры.

По всей видимости, в один прекрасный день обычные телефонные переговоры превратятся в небольшие видеоконференции, проводимые с помощью, устройств наподобие обычных сотовых телефонов, которые соединят в себе возможности персонального компьютера, телевизора и телефона. Обычные технологии быстро интегрируются, порождая новые коммуникационные средства: голосовую почту, технологии PC/TV и IP/TV, Интернет-телевидение, Интернет-телефонию и т. д.

Для того чтобы быть готовыми к новым технологиям, производители оборудования и организации по стандартам должны предпринимать следующие действия:

- поставлять на рынок новые устройства с приемлемыми ценами;
- разрабатывать новые протоколы для передачи информации и управления ею;
- совершенствовать методы сжатия и синхронизации;
- предоставлять доступные по цене высокоскоростные каналы во все дома и компании;
- продолжать разработку новых межсетевых устройств и физических передающих сред, обеспечивающих требования высокоскоростных коммуникаций;
- создавать простые в использовании комбинированные устройства (а также "прозрачные" для пользователя программные средства), соединяющие в себе возможности персонального компьютера, телевизора, аудиосистемы и коммуникационного оборудования;
- продолжить разработку общих и международных стандартов, обеспечивающих совместимость оборудования;
- обучать монтажников, эксплуатационников и пользователей.

Резюме

Видеотехнологии (в т. ч. и используемые на компьютерах) берут свое начало от аналогового телевидения. В настоящее время цифровые технологии являются привычными в компьютерах и компьютерных сетях, с их помощью происходит переход от обычного телевидения к высококачественному цифровому. Широко распространена передача неподвижных изображений через Интернет, для чего применяется сжатие JPEG. Стандарт MPEG стал одним из самых важных форматов сжатия файлов при передаче мультимедийной информации (включая видео- и аудиосигналы) по компьютерным сетям и в системах цифрового телевидения.

Существует множество форматов аудиофайлов и методов их сжатия, что зависит от способа передачи аудиосигнала и программных средств, при этом применяемых. Примерами таких форматов являются ACELP (используется в медиаплеерах), MPEG (применяется в самых разнообразных приложениях) и WAV (используется для передачи музыки через Интернет).

Методы дискретизации применяются во многих аудио- и видеотехнологиях, выбранный метод заметно влияет на качество сигнала.

Технология Voice over IP (VoIP) используется некоторыми компаниями как альтернатива частным и офисным телефонным системам. Она обеспечивает телефонные услуги в сети.

При развертывании мультимедийных приложений в сети следует оценивать ее полосу пропускания и производительность, сопоставляя их с потребностями данных приложений.

Возможности передачи аудио- и видеосигналов по сети зависят от таких факторов, как методы сжатия, форматы файлов, синхронизация, время ожидания и джиттер.

Для передачи информации в локальных и глобальных сетях используются однонаправленные, широковещательные и групповые пакеты. Производительность сети для некоторых приложений, нуждающихся в большой полосе пропускания, можно увеличить, если разрешить этим приложениям использовать многоадресное (групповое) вещание.

Устаревшие и существующие локальные сети можно модернизировать, увеличив их полосу пропускания для развертывания мультимедийных приложений (например, добавив коммутаторы и маршрутизаторы). Для сетей, предназначенных для передачи мультимедийного трафика, многие сетевые администраторы в настоящее время выбирают комбинированную архитектуру Gigabit Ethernet и Fast Ethernet.

При создании глобальной сети для передачи речи, видеоизображений и данных следует выбирать технологии, обеспечивающие полосу пропускания, достаточную для совместимости с теми локальными сетями, которые глобальная сеть объединяет, а также поддерживающие все три метода передачи пакетов и фреймов, существующих в мультимедийных сетях. Также необходимо использовать имеющиеся методы повышения производительности и распределения ресурсов, обеспечивающие удовлетворение растущих потребностей.

В ближайшие годы у мультимедийных средств и интегрированных сетевых служб появится множество новых привлекательных возможностей. Эти возможности можно уже сейчас наблюдать в таких областях, как компьютерная профессиональная подготовка, проведение видеоконференций и потоковое воспроизведение информации.. Мультимедийные приложения лишь только сейчас позволили в полной мере увидеть потенциал персональных компьютеров и сетей в области коммуникаций, стимулируя общение людей, находящихся на больших расстояниях, реализуя возможности удаленного обучения и предоставляя средства коллективной работы при решении задач.

Глава 11

Базовые принципы проектирования локальных и глобальных сетей

По прочтении этой главы и после выполнения практических заданий вы сможете:

- обсудить основные аспекты проектирования локальных и глобальных сетей, включая применение структурированных кабельных систем и структурированных сетей;
- описать и реализовать методы построения локальных сетей;
- объяснить и реализовать методы построения глобальных сетей.

Одни сети начинают работать вполне успешно, однако впоследствии становятся перегруженными трафиком. Другие сети безупречно работают с самого начала и быстро адаптируются к изменениям и новым технологиям. Третьи сети с момента запуска испытывают сложности с передачей трафика и никогда не раскрывают свой потенциал полностью. Зачастую различие между всеми этими сетями определяется тем, как они спроектированы. Правильно разработанная сеть должна работать так, чтобы ее присутствие было почти незаметно для пользователей.

В этой главе будет показано, как на базе передающего оборудования, с которым вы познакомились в *главе 4,* построить хорошо работающую локальную сеть. Вы узнаете об основных принципах проектирования локальных сетей, в т. ч. с методами обеспечения масштабируемости и безопасности, со способами реализации кабельного хозяйства, с технологиями структурированных кабельных систем и структурированных сетей. Будут рассмотрены вопросы применения полнодуплексных коммуникаций, особенности использования коммутаторов и маршрутизаторов, а также методика составления запросов информации (RFI) и заявок на предложение (RFP). Затем вы познакомитесь с некоторыми методами организации локальных сетей на примере простой сетевой структуры. Вы узнаете, где нужно располагать хосты и серверы, а также как подготовить развертывание мультимедийных приложений. Также будет рассказано о структурах беспроводных сетей и задачах эксплуатации и поддержки. В разделе, посвященном принципам проектирования глобальных сетей, описываются модели беспроводных региональных и глобальных сетей, топологии, предлагаемые поставщиками услуг глобальных сетей, структура расходов, вопросы выбора полосы пропускания и оборудования.

Общие вопросы проектирования локальных и глобальных сетей

Как только появляются новые версии программных средств, так пользователи сразу желают работать с ними. Пользователи системы Windows 2000 Professional хотят перейти на Windows XP Professional, пользователи веб-браузеров хотят получить последние, наиболее безопасные версии, а пользователи систем UNIX стремятся немедленно применить в работе функциональные возможности, появляющиеся в новейших версиях продукта. Требует обновления клиент-серверное программное обеспечение, поскольку в нем могут учитываться постоянно меняющиеся значения налогов и другие показатели. Для поддержания новых функциональных возможностей многих обновленных программ необходимы дополнительные серверы, рабочие станции или сетевые ресурсы. Эти и многие другие причины вызывают необходимость создания локальных и глобальных сетей. После анализа и оценки возникающих потребностей следует учитывать некоторые факторы, влияющие на проект локальной или глобальной сети.

Факторы, влияющие на структуру локальных и глобальных сетей

Когда возникает задача развертывания или модернизации локальной или; глобальной сети, можно определить факторы, влияющие на сетевую модель, в том числе:

- ожидаемый сетевой трафик;
- требования по избыточности;
- перемещения пользователей;
- перспективное развитие;

- требования безопасности;
- подключение к глобальным сетям;
- стоимость.

Далее мы подробно рассмотрим каждый из перечисленных факторов.

Ожидаемый сетевой трафик

При установке или обновлении сети необходимо хорошо представлять себе объем трафика, предполагаемого в сети. В новых сетях нужно учитывать количество пользователей и тип серверов или хостов, которые будут работать в сети. При обновлении некоторой сети получите тестовые показатели (benchmarks) для текущей загрузки сети и проанализируйте трафик от определенных устройств, включая серверы и хост-компьютеры. Например, если в локальной сети имеется мэйнфрейм, то значительный трафик может создавать *пакетная* (batch) *обработка* заданий. В одной известный авторам компании, весьма успешно торгующей по почтовым заказам, операторы вводили заказы на мэйнфрейме IBM, причем каждый заказ оформлялся дважды. После ввода 20 новых заказов они передавались в виде пакета. Повторное оформление заказов осуществлялось для того, чтобы избежать ошибок ввода. Проект новой сети для этой компании должен был учитывать появляющийся трафик и местоположение операторов ввода данных для того, чтобы создаваемый ими высокий трафик не влиял бы на работу всей сети.

Электронная почта может быть еще одним источником значительного трафика, например, в тех случаях, когда все члены некоторой рабочей группы часто посылают большие электронные таблицы в виде вложений почтовых сообщений. Особенно часто такое может случаться, если не совсем квалифицированные пользователи вкладывают в сообщение целую книгу формата Microsoft Excel, а не отдельные ее страницы.

Требования по избыточности

Другим определяющим фактором является необходимость в избыточных (резервных) сетевых путях для передачи данных. Иногда наличие локальной сети важно для пользователей, однако в силу характера их деятельности они могут некоторое время обходиться без сети, если, например, часть сети выйдет из строя из-за неисправности коммутатора. В других ситуациях требуются резервные сетевые маршруты для перераспределения трафика – чтобы пользователи никогда не замечали неисправностей оборудования (рис. 1.1.1). Наличие *избыточности* (redundancy) – это требование тех организаций, которые могут потерять тысячи долларов за каждую минуту простоя части сети.

Перемещения пользователей

Еще один фактор, учитываемый в сетевом проектировании, – необходимость поддержки пользователей, которые постоянно меняют свое местоположение. В некоторых областях бизнеса типичными являются частые реорганизации, необходимые для отслеживания состояния рынка. Для других организаций может быть высокой вероятность их слияния. В таких ситуациях рабочие места в офисах часто перемещаются, что нужно учитывать в структуре сети.

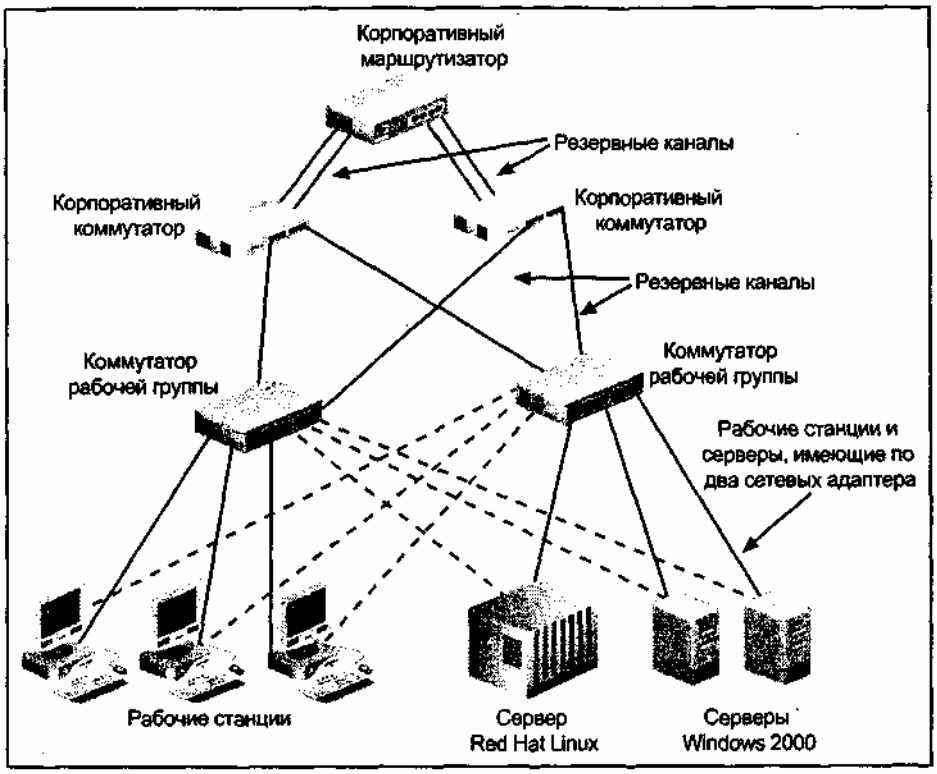


Рис. 11.1. Методы обеспечение избыточности

В некоторых организациях пользователям нужно физически перемещаться по зданию (например, по складу или больнице), имея при себе карманное вычислительное устройство или портативный компьютер. Подобные ситуации также следует учитывать для правильного выбора топологии беспроводной сети, позволяющей таким пользователям получать полный доступ ко всем сетевым ресурсам.

Перспективное развитие

Все перспективные сети должны предусматривать возможность роста, для чего в них необходимо заложить соответствующие проектные решения. При соблюдении этого условия средства, вложенные в сеть, окупаются в течение многих лет. Например, существующую звездообразную сеть 10BaseT модернизировать проще, чем обычную шинную сеть 10Base2. Кроме того, возможности развития проще заложить в сеть, созданную на базе маршрутизаторов и коммутаторов, чем в сеть, построенную на основе устаревших топологий с использованием мостов, где следует учитывать ограничения IEEE на число мостов, соединяемых друг с другом.

Требования безопасности

Хотя некоторые средства безопасности нужны для большинства сетей, не для всего сетевого трафика требуется одинаковый уровень зашиты. Например, сеть, используемая аудиторской компанией при обработке счетов и зарплат для других компаний, должна обеспечивать высокую степень защиты. Для этого могут использоваться маршрутизаторы и соответствующие инструменты, а также защищенная кабельная проводка. Однако для компании, поддерживающей общедоступную базу данных медицинской статистики, не требуется такой же уровень безопасности, как для аудиторской фирмы.

Подключение к глобальным сетям

Подключение к глобальным сетям также является важным фактором, учитываемым при проектировании локальной сети. Для некоторых локальных сетей необходимы лишь базовые возможности глобальной связи, для чего достаточно иметь подключение к Интернету по DSL- или ISDN-каналам. Для других локальных сетей требуются разнообразные средства глобальных коммуникаций: например, спутниковые каналы для связи с другими странами, сети frame relay для подключения к локальным сетям в соседних городах, и линии T-3 для всеобщего доступа к веб-сайту, анонсирующему выпускаемую продукцию.

Стоимость сети

При осуществлении любого проекта локальной и глобальной сети необходимо учитывать расходы. В

большинстве организаций расходы на развертывание новой сети или на модернизацию существующей сети определяются некоторым бюджетом или определенной суммой денег, выделенных на проект. Вам нужно учитывать в проекте стоимость различных составляющих, включая следующие:

- коммуникационный кабель;
- сетевые устройства;
- дополнительные компьютеры, необходимые в сети;
- программные и аппаратные средства управления сетью и ее анализа;
- монтажные работы;
- обучение;
- консультации поставщиков;
- плата за услуги глобальной сети или за выделенные линии.

Анализ существующей топологии и ресурсов

Для уже используемой сети необходимо периодически анализировать топологию локальной сети и использование ее ресурсов. Глубина анализа может варьироваться от простого осмотра кабельной структуры до сбора тестовых показателей степени использования полосы пропускания сети с применением сетевого анализатора и получения оценки о соответствии сети существующим запросам и о возможностях ее развития. Кроме того, нужно следить за использованием ресурсов (какие ресурсы используются, а какие нет), поскольку нет смысла в существовании коммутаторов или соединений, если те более не задействуются. Необходимо учитывать следующие вопросы.

- Наблюдается ли значительное увеличение числа пользователей сети?
- Имеются ли изменения в типах пользовательских рабочих станций и приложений?
- Нужны ли пользователям дополнительные сетевые службы?
- Легко ли управлять сетью?
- Существуют ли новые требования по повышению надежности сети и обеспечению дополнительной избыточности?
- Можно ли модернизировать имеющееся сетевое оборудование или оно окончательно устарело?

Два первых вопроса касаются трафика, и за ними нужно следить постоянно. Некоторые сетевые администраторы контролируют производительность сети подобно тому, как администраторы серверов или хостов контролируют дисковое пространство. Этот процесс планирования включает в себя необходимый для распределения нагрузки по сегментам сети анализ текущих и будущих потребностей: сюда входит количество пользователей, необходимость в новых программах, мощность сетевых серверов, соответствие рабочих станций потребностям пользователей и прикладных программ, полоса пропускания сети. Для определения сетевой нагрузки в сегменте выполните практическое задание 11-1.

Управление сетью

Во всех сетевых проектах необходимо пристальное внимание уделять вопросам управления сетью. Например, важно, чтобы при установке новых сетевых программных продуктов администратор сети тесно взаимодействовал с администратором сервера. Это дает гарантию того, что сеть соответствует новым потребностям. Сетевое управление тесно связано с моделью и топологией сети, поскольку одними топологиями проще управлять, чем другими. Во многих случаях звездообразная топология обеспечивает более быстрое обнаружение проблемы, чем обычная шина. Кроме того, сетевая структура, в которой использованы коммутаторы и маршрутизаторы, проще для мониторинга, диагностики и перенастройки в случае возникновения узких мест, чем сеть, построенная на базе устаревших неуправляемых концентраторов или многопортовых повторителей.

Нередко к развертываемой сети не предъявляется никаких требований по обеспечению избыточности или надежности, поскольку пользователи не размещают в сети ответственных приложений до тех пор, пока не привыкнут к сети. Постепенно развертывается все больше и больше приложений, и этот процесс продолжается до тех пор, пока сеть не станет столь же важной, как пользовательские рабочие станции. К этому моменту сеть должна иметь избыточные маршруты и отвечать требованиям надежности.

Как и персональные компьютеры, сетевое оборудование быстро устаревает из-за изменений технологий или пожеланий производителей. В некоторых устройствах совмещаются старые и новые технологии (например, коммутатор может иметь порты на 10 Мбит/с, 100 Мбит/с и 1 Гбит/с). Другие устройства можно модернизировать за счет обновления соответствующих программных средств. Однако некоторые устройства модернизировать нельзя, поэтому их нужно либо переместить в другую точку сети, либо заменить.

Прокладка и замена кабеля

Кабельная структура определяет время жизни сети – все другие компоненты зависят от нее. В качестве проектировщика сетей вас могут пригласить для аудита существующих кабелей с целью обнаружения устаревших кабелей и разработки плана модернизации кабельного хозяйства, что позволило бы обеспечить расширение сети, реализовать высокоскоростные коммуникации и разнообразные возможности глобальной связи. Кабель может оказаться не просто устаревшим, он может также не соответствовать существующим на данный момент спецификациям ШЕЕ или требованиям пожарной безопасности, которые со временем меняются.

Для новых и существующих сетей кабельная структура (кабельный участок) является основой для соединения локальной сети с глобальной. В 1970– 80-х годах в локальных сетях для горизонтальной разводки по рабочим местам широко использовался тонкий коаксиал, а толстый коаксиал применялся в качестве вертикального *восходящего кабеля* (riser cable), проложенного между этажами здания. На рис. 11.2 изображена эта старая, традиционная шинная топология, в которой для расширения сети сначала используются многопортовые повторители, а затем – мосты.

Традиционные кабельные структуры с использованием тонкого и толстого коаксиалов имеют существенные ограничения. Во-первых, их полоса пропускания не отвечает высоким требованиям трафика, создаваемого современными программами. Во-вторых, эти сети (где применяется негибкий коаксиальный кабель, не выдерживающий многократные перегибы) очень дороги при эксплуатации и ремонте.

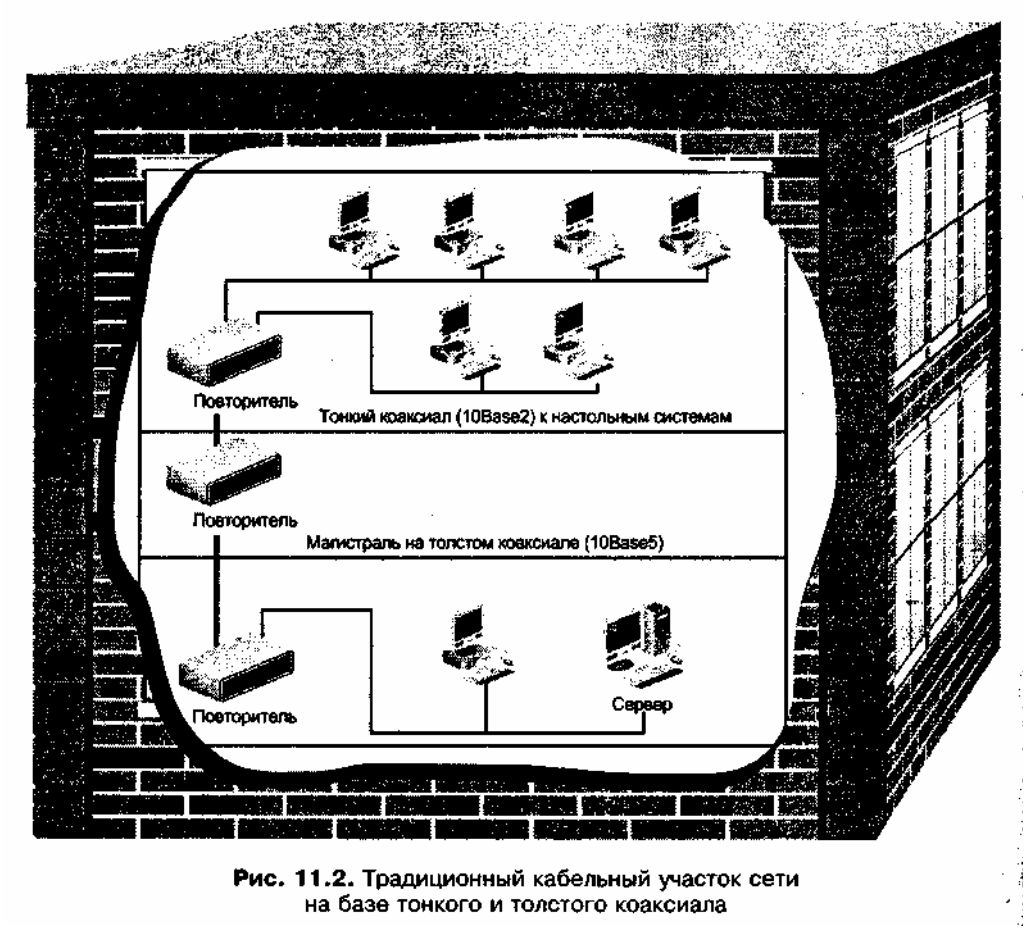


Рис. 11.2. Традиционный кабельный участок сети на базе тонкого и толстого коаксиала

BNC-коннекторы для коаксиальных кабелей стоят больше, чем коннекторы RJ-45, используемые для витой пары. Их сложнее устанавливать, они менее надежны после нескольких подключений/отключений. Кроме того, неисправный трансивер для тонкого коаксиала сложнее обнаружить в случае отказа сети,

поскольку для реализации сетевого подключения используются несколько различных компонентов с BMC-разъемами.

Еще одна проблема заключается в том, что целый сегмент сети легко вывести из строя, если с него (случайно или намеренно) снять терминатор или если в нем появится всего лишь одно неисправное устройство (или откажет компонент кабельной разводки). Может оказаться так, что устаревшие сети на базе тонкого и толстого коаксиалов будет сложно расширить, поскольку в настоящее время мало необходимого оборудования, и переход от традиционной шинной топологии к новой звездообразной может потребовать полной переделки кабельной структуры. Неудачно выбранная топология сети может сделать практически невозможным ее расширение.

Если вы планируете замену кабелей, учитывайте следующие факторы:

- возможность замены устаревшего кабеля (например, тонкого и толстого коаксиала, а также кабеля Категории 3);
- стоимость кабеля и коннекторов;
- монтажные расходы;
- условия среды (например, наличие коробов и источников радио- и электромагнитных помех);
- дополнительные требования к кабелю;
- создание и перестройка помещений для монтажных шкафов.

В любом случае создайте план замены старого кабеля существующей сети. Например, в здании вместо толстого магистрального коаксиала проложите многомодовый оптоволоконный кабель, а повторители замените на коммутаторы. Замените идущий к рабочим станциям тонкий коаксиал или кабель Категории 3 на кабель Категории 5 (или лучший), однако имейте в виду, что вам потребуется также заменить установленные сетевые адаптеры под тонкий коаксиал на адаптеры, обеспечивающие подключение витой пары. Для проложенных между зданиями сегментов региональной сети подмените толстый коаксиал или кабель Категории 3 на одно- или многомодовый (в зависимости от расстояния) оптоволоконный кабель.

Во многих случаях стоимость современного кабеля и коннекторов будет ниже, чем затраты на старый кабель из-за существующего массового спроса. Определяя расходы на замену старого кабеля сравните их с теми суммами, которые будут сэкономлены при эксплуатации и сопровождении. Прокладка нового кабеля может оказаться дорогой с точки зрения трудозатрат (в зависимости от степени сложности работ по удалению старого кабеля и наличия осложняющих моментов, например, если при этом нужно убрать или нейтрализовать опасные строительные материалы). Стоимость кабеля может увеличиться, если из-за строительных нормативов и/или условий среды необходимо приобрести специальный кабель для прокладки в вентиляционной зоне или экранированный кабель, защищенный от радио- и электромагнитных помех). Кроме того, во всех случаях имеет смысл оставлять запас кабеля от 20% до 50% для упрощения и удешевления подключения новых рабочих станций, т. к. расходы на оплату труда по прокладке кабеля больше стоимости самого кабеля. Всегда дешевле установить кабель *"с* нуля", чем прокладывать дополнительные отрезки кабеля. Организации расширяются, и в помещении, где сегодня сидят пять человек, завтра может оказаться восемь. Еще одной
причиной для прокладки дополнительного кабеля является необходимость создания избыточных коммуникационных магистралей.

Совет

Как вы уже знаете из *главы 9,* если расходы на прокладывание кабеля слишком высоки из-за необходимости удаления опасных материалов или применения специального кабеля, рассмотрите в качестве альтернативы беспроводные технологии.

Рекомендации по прокладке кабелей

Для любой ситуации – заменяете ли вы существующий кабель или прокладываете новый – имеется множество проверенных рекомендаций. Если вы будете следовать указанным рекомендациям, то реализованная кабельная структура с большей вероятностью справится с ожидаемым сетевым трафиком и сможет быть модернизирована в будущем. Никто не хочет прокладывать кабель так,

чтобы он с самого начала работал неправильно. Однако ошибки случались, и для их исправления требовались дорогостоящие переделки или полная замена разведенного кабеля, в результате чего напрасно тратилось время и возникали неоправданные расходы.

Чтобы сеть работала нормально, при монтаже кабельного участка пользуйтесь следующими рекомендациями:

- используйте принципы построения структурированных кабельных систем и структурированных сетей (будут описаны позже);
- устанавливайте кабельную систему, полоса пропускания которой соответствует или превосходит полосу, необходимую в конкретной зоне (с учетом предполагаемых прикладных программ, используемых компьютеров и сетевых ресурсов);
- для горизонтальной разводки (для подключения настольных систем) используйте витую пару (UTP) Категории 5 (или выше);
- для восходящего кабеля между этажами применяйте многомодовое оптоволокно;
- проверьте, соответствуют ли по длине все отрезки кабеля спецификация IEEE для выбранной коммуникационной среды;
- на больших расстояниях (например, между зданиями) используйте одномодовый оптоволоконный кабель;
- устанавливайте беспроводные сети стандарта 802.11 в тех случаях, когда прокладка кабеля обходится слишком дорого или для этого имеется очень много препятствий. При выборе такого решения убедитесь в том,) что соблюдены все стандарты, и что вы тщательно выбрали оборудование, соответствующее имеющимся или разрабатываемым стандартам;
- прокладывайте звездообразные кабельные участки;
- используйте только высококачественный кабель;
- следуйте всем строительным нормативам (например, на прокладку специального кабеля для монтажа в вентиляционной зоне);
- избегайте больших усилий при прокладке кабелей на основе витой пары;
- точно соблюдайте требования к радиусу изгиба кабеля (чтобы не повредить кабель монтажными клещами или многократными перегибами);
- в конечных точках оставляйте достаточный запас кабеля, что обеспечит гибкость при последующих изменениях, переделках или перемещениях компьютеров;
- если для проведения работ выбран подрядчик, проверьте у него наличие необходимых сертификатов и лицензий, а также убедитесь в том, что он предоставил на кабельный участок документацию и результаты тестирования;
- убедитесь, что кабель и монтаж сертифицированы на соответствие спецификациям IEEE;
- промаркируйте все кабели в соответствии со стандартом EIA/TIA-606 (например, пометьте все выходы и терминаторы);
- правильно заземлите все кабельные участки в соответствии со стандартом EIA/TIA-607.

Примечание

Сертификация кабеля проходит в два этапа. Сначала производитель кабеля сертифицирует его на соответствие стандартам EIA/TIA, IEEE и UL. Затем с помощью специального оборудования тестируются все смонтированные сегменты кабеля и проверяется их соответствие стандартам EIA/TIA и IEEE.

Совет

В качестве общего правила следует запомнить, что минимальный радиус изгиба для кабеля на основе четырех витых пар приблизительно в четыре раза больше длины окружности кабеля, а если число пар больше четырех – то в 10 раз.

Структурированная кабельная система

В настоящее время многие сети создаются с использованием идеологии *структурированных кабельных систем* (структурированная разводка, structured wiring), которым в книге уделено особое внимание. Это понятие может по-разному трактоваться теми, кто прокладывает кабель, и проектировщиками сетей. Мы будем так называть способ прокладки кабеля, при котором он расходится по горизонтали в виде звезды, в центре которой находится один или несколько стоечных концентраторов или коммутаторов, расположенных в телекоммуникационных комнатах или монтажных шкафах (телекоммуникационные комнаты, telecommunication rooms, описаны в стандарте EIA/TIA-569-A). Зачастую стоечные концентраторы или коммутаторы находятся на одном этаже и помещаются в монтажном шкафу, как показано на рис. 11.3.

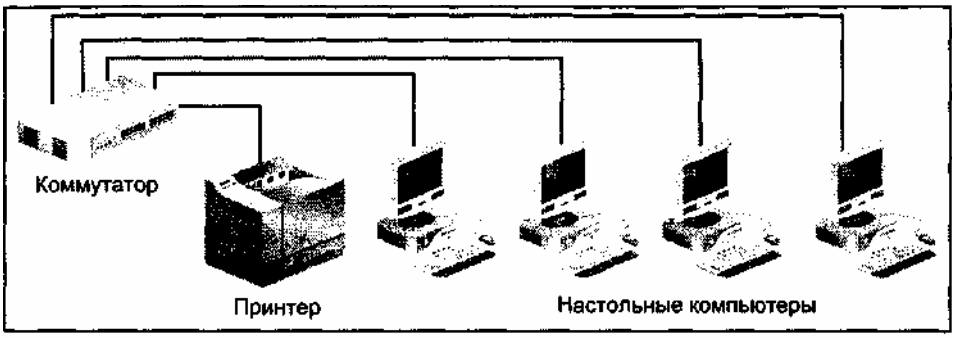


Рис. 11.3. Структурированная кабельная система

Для реализации структурированной кабельной системы необходимы следующие компоненты и условия:

- гибкий кабель (например, на основе витой пары);
- разводка в виде физической звезды;
- соответствие стандартам EIA/TIA-568-A и EIA/TIA-568-B на горизонтальную разводку;
- централизованное подключение кабельного участка к стоечным концентраторам или коммутаторам;
- наличие "интеллектуальных способностей" у концентраторов и коммутаторов для обнаружения неисправностей в узлах;
- возможность изолирования хостов и серверов в своем кабельном сегменте;
- наличие высокоскоростных каналов к хостам и серверам, а также к другим сетевым устройствам.

Обычно горизонтальная разводка охватывает отдельный этаж здания, Веерообразно расходясь по различным комнатам и зонам офиса. Если в здании несколько этажей, то существует несколько уровней горизонтальной разводки, соединенных вертикальными кабелями, что в совокупности образует структурированную сеть. Одним из достоинств принципа горизонтальной разводки является то, что она упрощает проектирование, разделяя кабельную структуру на отдельные модули (подобно тому, как программист создает в программе подпрограммы и связывает их в целый функциональный модуль). В здании каждый этаж представляет собой самостоятельную единицу кабельного участка.

Вертикальная разводка и структурированные сети

Соедините структурированную проводку каждого этажа в многоэтажном здании, используя тщательно продуманную схему вертикальных кабелей, и вы получите структурированную сеть. Компоненты вертикальной разводки такой сети включают в себя кабели и сетевое оборудование, используемое между этажами здания и зачастую физически связывающее телекоммуникационные комнаты смежных этажей. Вертикальная разводка используется как логическая магистраль, к которой подключаются горизонтальные кабели всех этажей здания.

При реализации вертикальной разводки сети нужно руководствоваться следующими принципами:

- для связи устройств используйте расширенную звездообразную топологию (монтажные шкафы, расположенные на этажах, иногда можно соединять в цепочку);
- применяйте высокоскоростной кабель, лучше всего многомодовое оптоволокно, чтобы уменьшить вероятность перегрузки магистрали и для защиты от радио- и электромагнитных

помех;

- соблюдайте стандарты EIA/TIA-568-A и EIA/TIA-568-B на вертикальную и магистральную разводку;
- используйте сертифицированный восходящий кабель (кабель, пригодный для прокладки между этажами) для сегментов, проходящих по кабельным каналам и вертикальным шахтам; этот кабель должен отвечать стандартам Underwriters Laboritories, Inc. (UL) и National Electric Code (NEC) на огнестойкость;
- применяйте огнестойкие материалы для защиты отрезков кабеля между этажами (если имеется более двух этажей или в соответствии со стандартами UL и NEC, а также с учетом местных строительных нормативов).

Для двух первых пунктов приведенного списка необходимы дополнительные комментарии. Во-первых, применение расширенной звездообразной топологии между этажами соответствует спецификациям EIA/TIA-568-A и EIA/TIA-568-B. Достоинство такого подхода заключается в том, что он упрощает управление соединениями с использованием повторителей, через которые сигнал должен передаваться. Недостатком является то, что центральный стоечный концентратор или коммутатор может стать единственной точкой отказа. Эту проблему можно решить, приобретая устройства с избыточностью (например, с резервными задними панелями и источниками питания). Кроме того, такие устройства можно подключить к *источнику бесперебойного питания* (uninterruptible power supply, UPS), представляющему собой систему резервного батарейного питания, включающуюся при нарушении энергоснабжения, а также в случае всплесков или падений напряжения.

Во-вторых, применение оптоволокна для вертикальной разводки не только позволит вам повысить скорость магистрали для реализации высокоскоростных коммуникаций, но и защитит магистраль от радио- и электромагнитных помех. Это означает, что вы можете проложить кабель возле линий силового напряжения, электрических кабелей, источников света и лифтов. Кроме того, на оптоволоконный кабель не распространяются требования заземления, чего не скажешь о медном кабеле.

Объединяя структурированную кабельную систему с надежной вертикальной разводкой, вы получаете *структурированную сеть* (structured network), концепциям которой в книге уделяется особое внимание. Элементы такой сети сосредоточены в стратегических точках. Например, коммутаторы помещаются в монтажных шкафах, которые подключаются с помощью высокоскоростных каналов к главному стоечному коммутатору, расположенному в машинном зале или в некоторой узловой точке кабельной структуры здания. Не редко серверы непосредственно соединяются с главным или центральным коммутатором по скоростному каналу (например, по 1-гигабитному каналу, как показано на рис. 11.4). Для реализации структурированной сети в главных точках устанавливаются стоечные коммутаторы или концентраторы, которые могут централизовать кабельную структуру, а также модули мостов, маршрутизаторов и коммутаторов. (Чтобы нарисовать общий план структурированной сети, выполните практическое задание 11-2.)

Структурированные сети позволяют сетевому администратору решать следующие задачи:

- централизовать или распределять управление сетью;
- объединять вертикальные и горизонтальные сетевые структуры с помощью высокоскоростной магистрали;
- перестраивать физическую и логическую топологию сети;
- сегментировать сеть, используя модель групп и виртуальные локальные сети (VLAN);
- обеспечивать избыточность;
- быстро расширять сеть и создавать новые высокоскоростные каналы;
- осуществлять профилактический мониторинг сети, а также быстро находить и устранять возникающие проблемы.

Помимо того что в структурированной сети главные сетевые устройства расположены централизованно, другим достоинством такой сети является возможность централизованного сетевого управления. Для этого выбираются базовые точки, в которых реализуются важные сетевые функции. Например, сетевой мониторинг может осуществляться на станции управления сетью с использованием протокола SNMP и подключений к интеллектуальному стоечному коммутатору или концентратору.

SNMP-совместимые коммутаторы (сетевые агенты по сбору информации) размещаются на каждом этаже и снабжают станцию управления непрерывными данными о всех элементах сети. При централизованном управлении сетью многие операции по конфигурированию сети можно выполнять из одной точки. Это особенно важно для крупных сетей.

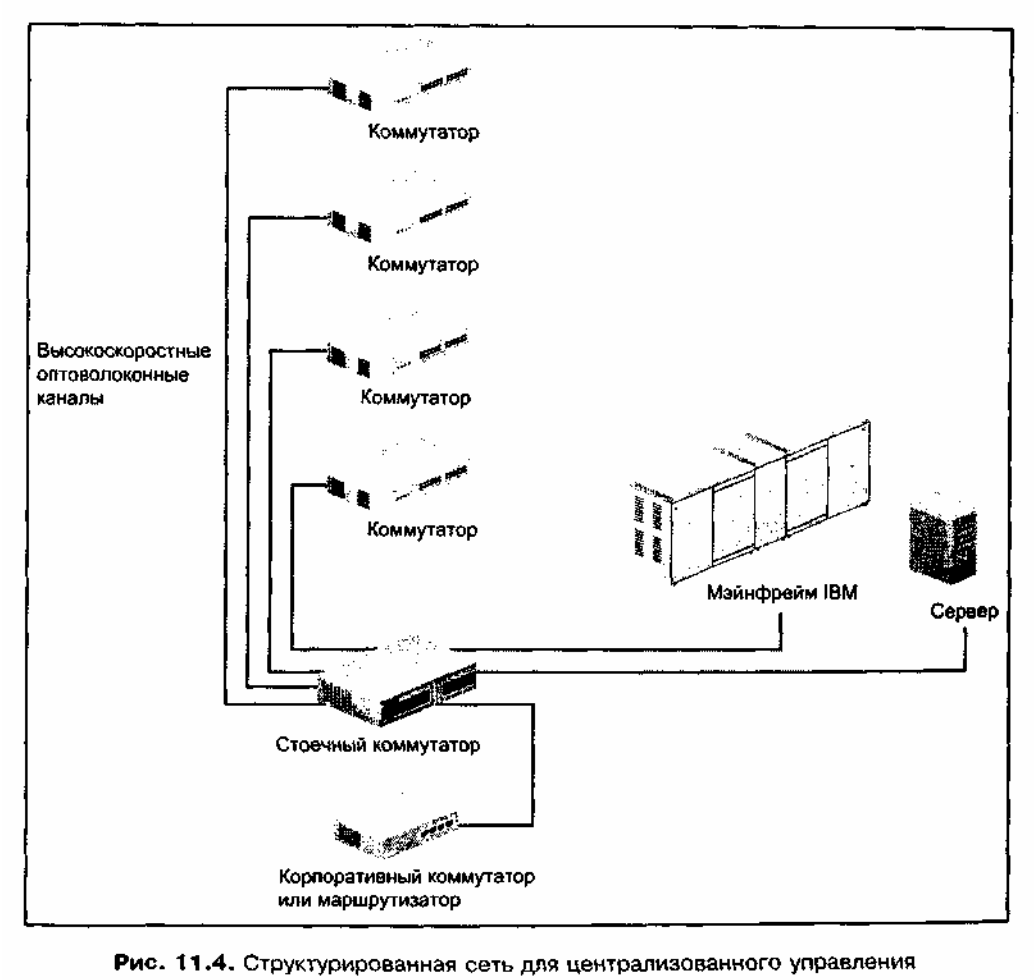


Рис. 11.4. Структурированная сеть для централизованного управления

При централизованном управлении сетью также упрощаются такие операции, как мониторинг серверов и хостов, которые могут размещаться в таких зонах, где их легко обслуживать (например, рядом с главными стоечными коммутаторами). В этом случае резервирование информации и обновление программных средств можно проводить на одной площадке, а не на нескольких, что нередко позволяет снизить трафик.

Серверы и хосты могут быть подключены к одному источнику бесперебойного питания и к *источнику фильтрованного питания* (conditioned power source), замена которых обходится дешевле, чем при их размещении по разным помещениям. Источник фильтрованного питания представляет собой § устройство, иногда встраиваемое в источники бесперебойного питания (UPS), которое сглаживает как небольшие, так и заметные изменения мощности силового напряжения, получаемого от энергетических компаний, и обеспечивает некоторый заданный диапазон мощностей. Благодаря такому устройству колебания мощности силового напряжения сглаживаются и не могут повредить устройства или создать помехи в компонентах.

Совет

Один из производителей источников фильтрованного питания – компания Powercom – называет фильтрованной такую мощность, которая содержит не более 10% шума, а согласованной "землей" – линию, колебания напряжения в которой не превышают 0,5 В.

Для компьютерного оборудования, расположенного централизованно, необходимо также соблюдать требования к температуре, влажности и количеству пыли в помещении. Некоторые организации не обращают достаточного внимания на внешние условия в помещениях, где установлены компьютеры, до тех пор, пока не начнутся проблемы. Это касается и качества силовой проводки.

Применение дуплексных коммуникаций

В дуплексном (полнодуплексном) режиме данные передаются и принимаются одновременно. Этот режим следует использовать в той части сети, где имеются высокоскоростные каналы (например, между коммутаторами или между коммутатором и маршрутизатором). Дуплексные коммуникации позволяют снизить вероятность конфликтов, поскольку входящие и исходящие) фреймы никогда не сталкиваются в проводе. При этом значительно увеличивается производительность сети, т. к. если конфликты отсутствуют, то нет пауз, в течение которых станции ожидают передачи после возникновения некоторого конфликта. Кроме того, уменьшается число потерянных пакетов.

Совет

10-гигабитные устройства работают только в дуплексном режиме.
Другой причиной для применения дуплексного режима в высокоскоростных каналах является то, что большинство коммутаторов используют один из двух способов управления потоком: режим создания помех и буферизацию. Коммутатор, работающий в полудуплексном режиме, использует режим создания помех, который может сигнализировать о том, что один из узлов коммутатора перегружен. Попросту говоря, *создание помех* (jamming) – это процесс усиления несущего сигнала для имитации конфликта. Недостатком режима создания помех является то, что он останавливает сетевой трафик, при этом передаваемые в данный момент фреймы могут быть потеряны. *Буферизация* (buffering) – это хранение фреймов в памяти до тех пор, пока они не будут отосланы по адресу назначения. Буферизация используется в дуплексном режиме (в этом режиме нет конфликтов, поэтому режим создания помех применять нельзя). В этом режиме коммутатор посылает специальный фрейм, инициирующий уменьшение скорости передачи данных. Благодаря этому появляется время, достаточное для буферизации активных фреймов, поэтому они не теряются и коммуникации продолжаются без перерыва (только с меньшей скоростью).

Примечание

При покупке коммутатора убедитесь в том, что размеры буферов в нем достаточно велики для хранения данных, передаваемых по всем интерфейсам.

Особенности использования мостов, маршрутизаторов и концентраторов

В течение многих лет мосты и маршрутизаторы используются для повышения производительности и безопасности сетей. Старые крупные сети нередко строились на базе "прозрачных" локальных мостов, а при необходимости подключения к локальной сети применялись удаленные маршрутизаторы. Ограниченность мостов заключается в их неспособности маршрутизировать трафик. Маршрутизаторы стоят дорого и ими сложно управлять. Их недостатком является то, что они не могут обрабатывать пакеты с такой же скоростью, с какой мосты обрабатывают фреймы, хотя в настоящее время в маршрутизаторах используются микропрограммные, аппаратные и программные средства, позволяющие им сравниться по быстродействию с мостами.

Примечание

Мосты (и коммутаторы Уровня 2) обрабатывают фреймы приблизительно *в* три раза быстрее, чем обычные маршрутизаторы могут обрабатывать пакеты (при этом нужно учитывать метод доступа, тип передающей среды и другие факторы). Это объясняется тем, что мостам не нужно анализировать информацию о маршрутизации и принимать решение о том, куда перенаправлять каждый фрейм. Современные мосты (на самом деле являющиеся коммутаторами)можно настраивать на различные способы обработки фреймов: с промежуточным хранением (базовый режим моста) или без буферизации пакетов (коммутация). Однако разность в быстродействии при маршрутизации или пересылке значительно уменьшилась. Фактически если маршрутизатор на некотором интерфейсе настроен на работу в режиме моста, он на самом деле тормозит этот интерфейс, поскольку процессор маршрутизатора выполняет дополнительные операции.

Некоторые существующие сети построены на базе наращиваемых и старых стоечных концентраторов, в которых возможности коммутации (модули коммутаторов) отсутствуют. Достоинство таких сетей состоит в централизации процессов управления сетью и обнаружения неисправностей, которые могут выполняться через концентраторы при условии наличия у них "интеллектуальных способностей". Недостатком является то, что концентраторы транслируют сетевой трафик по всем сегментам, что может

привести к возникновению в сети узких мест и уменьшению максимальной скорости передачи данных. (В современных сетях применяются не концентраторы, а коммутаторы.)

Подготовка запросов информации (RFI) и заявок на предложения (RFP)

Многие организации, планирующие масштабную модернизацию сети или развертывание новой сети, составляют плановые документы, отсылаемые поставщикам. Эти документы носят названия *Request for Information (RFI)* (Запрос информации) и *Request for Proposals (RFP)* (Заявка на предложения), RFI-запрос является первой попыткой общими словами описать потребности. В нем обычно описывается сама организация, имеющиеся ресурсы и тип служб (услуг), которые желательно получить у поставщиков. В частности, описание услуг может содержать такую фразу: "Поставщик должен установить сетевой кабель и оборудование в каждой комнате здания". RFP запрос рассылается поставщикам, которые в ответ предоставляют информацию о своих продуктах и о том, как эти продукты позволяют решать задачи определенные в запросе. Организация может выбрать поставщика на основе информации, присланной в ответ на RFI-запрос, а может выслать следующий документ – RFP. RFP-заявка обобщает полученную информацию, и на ее основе формулируются точные спецификации, которые в дальнейшем могут войти в контракт. Точная спецификация может выглядеть так: "Поставщик должен проложить кабель Категории 5 в каждую комнату, предусмотреть по два сетевых подключения на комнату. На каждом этаже здания кабель Категории *5* дол жен подключаться к коммутаторам 100BaseT. По окончании монтажа поставщик тестирует все соединения и коммутаторы и письменно подтверждает работоспособность каждого соединения и коммутатора.

Составление документов RFI и RFP имеет следующие преимущества:

- ваша организация может взвешенно определить свои потребности к новой или модернизированной сети;
- поставщики знакомятся с вашей организацией и понимают ее конкретные потребности;
- создается капитальная основа для обсуждения контрактов между вашей организацией и теми поставщиками, которые будут выбраны;
- появляются рекомендации, которым может следовать персонал компаний-поставщиков и вашей организации в ходе монтажных работ.

Принципы проектирования локальных сетей

В современных локальных сетях применяются маршрутизаторы и коммутаторы. Эти устройства позволяют использовать принципы построения структурированных кабельных систем и сетей. Маршрутизаторы обеспечивают сегментацию сетей и управление трафиком, а коммутаторы позволяют организовать отдельные области коллизий и повысить скорость пересылки сетевого трафика.

Во многих организациях трафик между подразделениями, как правило, меньше, чем внутри них. Рассмотрим исследовательскую сеть компании, которая может быть защищенным сегментом, где маршрутизатор используется в качестве брандмауэра. В смежной, скажем, маркетинговой сети требования к безопасности ниже или вообще могут отсутствовать. В подобных случаях маршрутизатор может уменьшить общий сетевой трафик, ограничивая его тем сегментом, для которого трафик предназначается, при этом он может действовать как брандмауэр, защищающий одну или несколько сетей.

Маршрутизаторы также используются для трансляции двух различных протоколов (например, SNA и IPX) между подразделениями. Во многих современных маршрутизаторах для повышения производительности стоят RISC-процессоры или специализированные интегральные схемы (application-specific integrated circuit, ASIC), представляющие собой заказные интегральные схемы, спроектированные для конкретной задачи, например, для быстрой маршрутизации.

Изначально коммутаторы были, в первую очередь, многопортовыми мостами, но сегодня некоторые типы коммутаторов имеют функции маршрутизации Уровня 3, а некоторые производители предоставляют функции Уровня 4, поскольку их коммутаторы могут проверять очередность полученных пакетов и даже определять тип приложения, отправившего пакет, при помощи идентификатора (ID) порта. В большинстве коммутаторов для обеспечения быстрых алгоритмов обработки применяются аппаратная логика или специализированные интегральные схемы. Коммутаторы не располагают такой гибкостью программирования и настройки, какая имеется у

маршрутизаторов, однако их легче устанавливать и администрировать, а, следовательно, сетевому администратору требуется меньше времени на обучение. Кроме того, в расчете на стоимость порта, коммутаторы дешевле, чем маршрутизаторы. Коммутаторы Уровней 3 и 4 могут выполнять те же функции, что и маршрутизаторы, однако для соответствия сетевой конфигурации требуется их тщательный подбор, поскольку гибкость в конфигурировании таких коммутаторов недостаточна по сравнению с маршрутизаторами.

При создании или обновлении локальной сети реализуйте план поэтапно, выполняя следующие действия:

- замените имеющиеся концентраторы на коммутаторы;
- замените устаревшие коммутаторы, несовместимые с протоколом SNMP,, на новые модели, в которых эта совместимость присутствует;
- подключите быстродействующие рабочие станции к коммутаторам;
- подключите серверы к высокоскоростным коммутируемым портам;
- подключите сгруппированные коммутаторы или коммутаторы рабочих групп к быстродействующим коммутаторам, используя высокоскоростные каналы;
- подключите основные сегменты подразделения или быстродействующие коммутаторы к маршрутизаторам, используя по мере надобности высокоскоростные каналы.

Поэтапная реализация плана сети

Рассмотрим модуль защищенной сети или сегмент рабочей группы, который требуется подключить к другому, незащищенному сегменту. Например, кампусной сети колледжа сегменты коммерческого отдела и бухгалтерий нужно соединить с сегментом биологического факультета, расположенным в другом здании. Сначала создайте сегменты сети для коммерческого отдела бухгалтерии (рис. 11.5), подключите их к отдельными портам маршрутизатора и сформируйте соответствующие правила и/или списки доступа.

Затем, используя один коммутатор, организуйте сегмент биологического факультета и подключите этот коммутатор к отдельному интерфейсу маршрутизатора (рис. 11.6).

Преимуществом такой поэтапной реализации плана является то, что дополнительные сегменты могут добавляться в разных местах. Сегменты можно подключать к маршрутизатору при расширении сети в некотором здании (например, можно добавить сегмент для физического факультета, находящегося в том же здании, что и биологический факультет). Если необходимое защитить сегмент биологического факультета, маршрутизатор может служить брандмауэром, при этом сегмент физического факультета будет доступен для всех. Кроме того, декан, ассистенты и преподаватели биологического факультета могут получить ограниченный доступ к сегменту коммерческого отдела, при этом студенческие лаборатории, подключенные к маршрутизатору через дополнительные коммутаторы и интерфейсы, могут быть заблокированы на уровне MAC-адресов. Эта сеть иллюстрирует преимущества архитектуры на основе маршрутизаторов и коммутаторов, имеющей множество возможностей модернизации для будущих конфигураций.

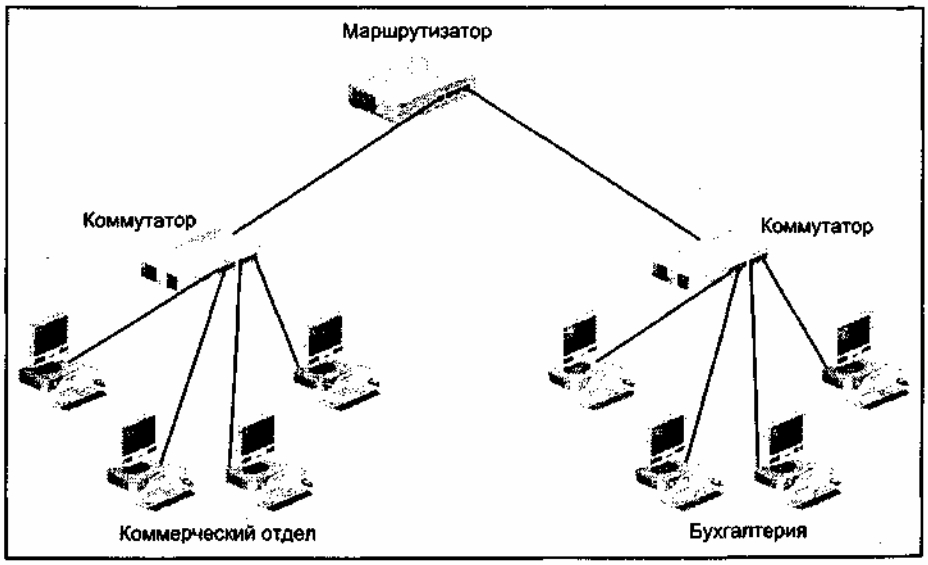


Рис. 11.5. Подключение сегментов двух факультетов к маршрутизатору

При начальной реализации сети, изображенной на рис. 11.6, начинайте с использования коммутаторов 100BaseT. Если вам впоследствии понадобится ее модернизировать, то вы сможете постепенно заменить некоторые коммутаторы на более быстрые 1-гигабитные модели или на комбинированные устройства, имеющие порты на 100 Гбит/с и 1 Гбит/с (при наличии обновленных сетевых адаптеров). Другим шагом может оказаться установка промежуточных 1-гигабитных коммутаторов "ниже" маршрутизаторов (что позволит увеличить пропускную способность подключенных к ним каналов) и размещение в каждом сегменте комбинированных коммутаторов с портами на 100 Гбит/с и 1 Гбит/с (рис. 11.7).

Выигрыш от использования промежуточного коммутатора заключается в том, что в этом случае создается основа для дальнейшего расширения сети.

Зачастую подобные промежуточные коммутаторы являются стоечными, благодаря чему в них можно устанавливать дополнительные модули для новых расширений и технологий. Новые модули можно вставлять по мере подключения новых сегментов. Можно обеспечить избыточность сети, добавив в нее второй промежуточный коммутатор и подключив к нему сегменты коммерческого отдела, бухгалтерии и биологического факультета, а сам; коммутатор соединив с маршрутизатором (или можно связать друг с другом ; оба промежуточных коммутатора).

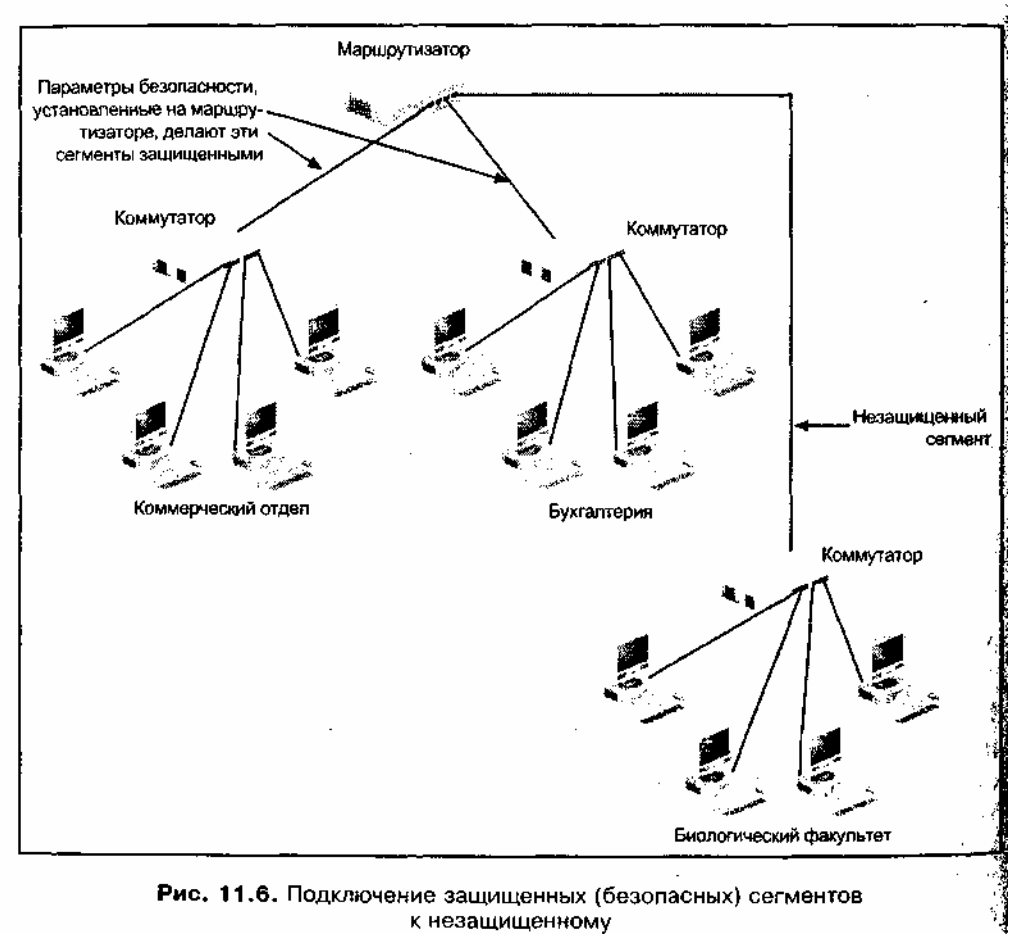


Рис. 11.6. Подключение защищенных (безопасных) сегментов к незащищенному

Еще одним решением является применение коммутаторов, позволяющие агрегировать или группировать каналы связи. *Группировка каналов* (trunking) предполагает объединение дублирующих друг друга каналов в некую совокупность, которую можно рассматривать как один канал, имеющий пропускную способность, равную сумме скоростей каждого канала. Например, три сгруппированных 1-гигабитных канала образуют агрегированный канал со скоростью 3 Гбит/с. Другим достоинством группировки каналов является то, что в случае отказа одного канала оставшиеся будут функционировать, обеспечивая непрерывную работоспособность агрегированного канала, хоть и с меньшей скоростью. На рис. 11.8 показано, как группировка каналов может использоваться в критических точках сети для создания дополнительной полосы пропускания. Выполните практическое задание 11-3 и создайте блок-схему сети с использованием группировки каналов.

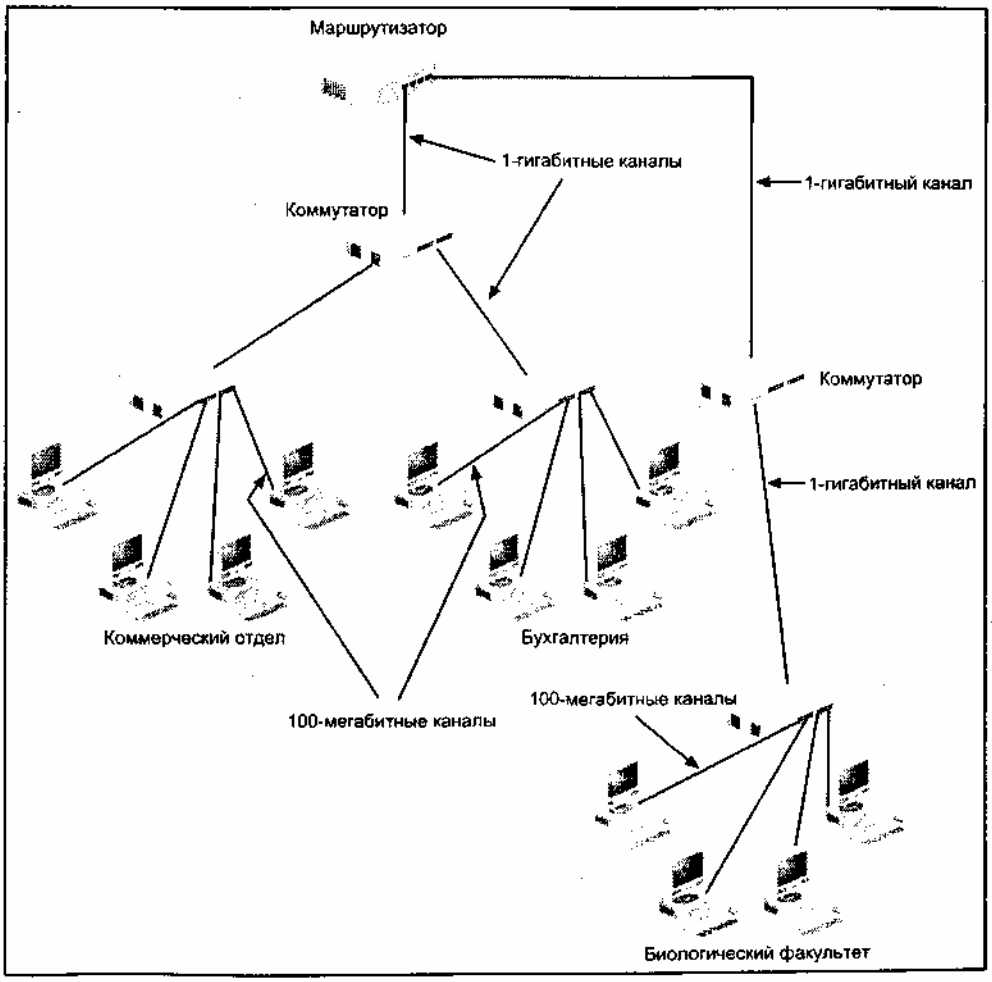


Рис. 11.7. Организация высокоскоростных коммуникаций

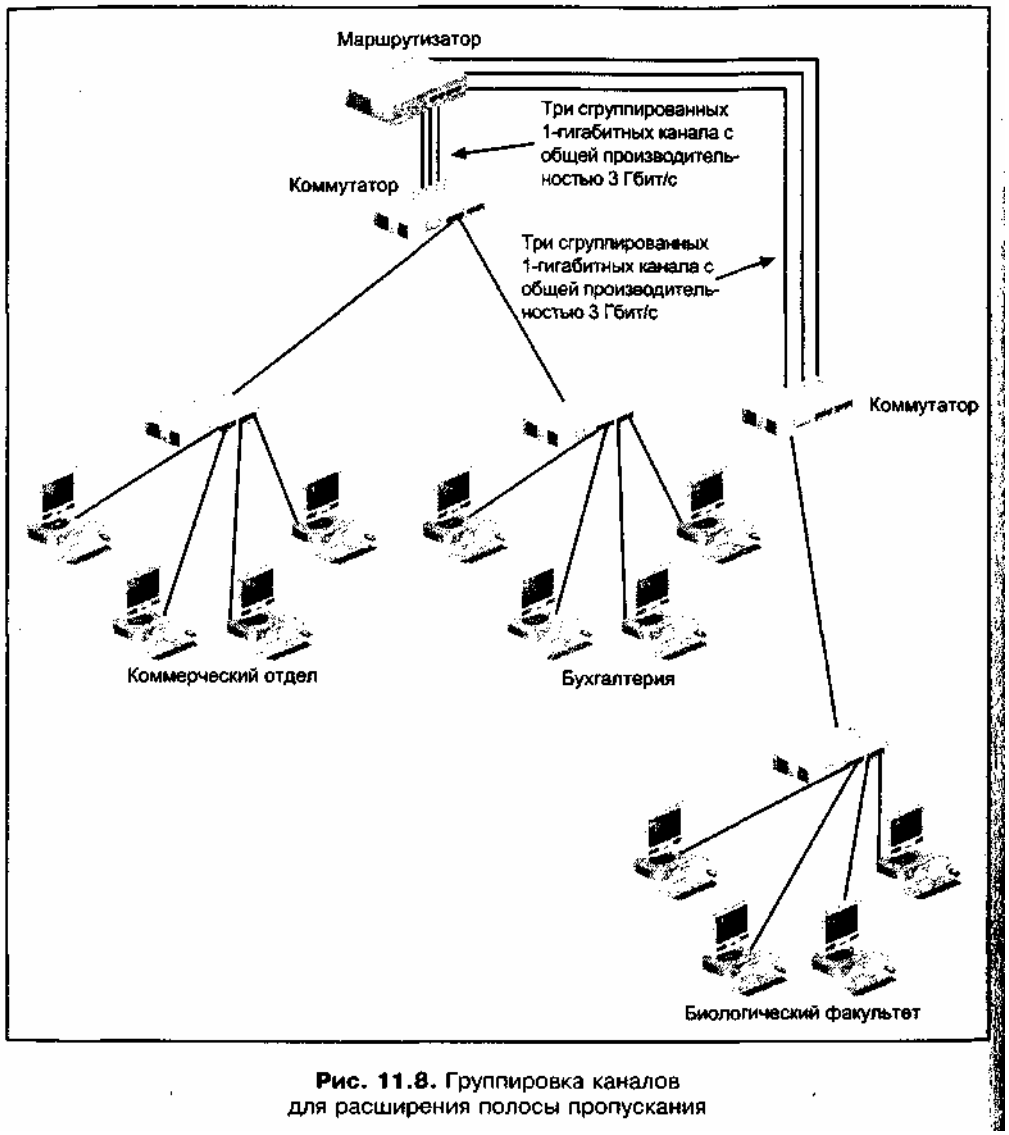


Рис. 11.8. Группировка каналов для расширения полосы пропускания

Примечание

Решения для группировки каналов часто являются частными ("фирменными") и это ограничение нужно учитывать при проектировании сети. Убедитесь, что' во всей структуре сети обеспечивается совместимость используемого оборудования (возможно, от разных производителей).
Далее в главе рассматриваются примеры сетей, иллюстрирующие следующие вопросы:

- выбор местоположения хостов и серверов;
- проектирование сетей для мультимедийных приложений;
- создание беспроводных сетей;
- вопросы эксплуатации и поддержки.

Размещение хостов и серверов

Хосты и серверы можно располагать в сети централизованно или в различных точках сети. *Группа серверов (хостов)* (host farm или server farm) (совокупность этих высокопроизводительных компьютерных систем, расположенных в одном помещении) обычно располагаются в машинном зале с контролируемой средой, т. е. этот зал имеет также специальное оборудование для фильтрации колебаний силового напряжения и поддержания температуры в заданном диапазоне. Кроме того, в зале устанавливаются источники бесперебойного питания и системы архивации, а сам зал закрывается от постороннего доступа.

Примечание

Планируйте поддержание постоянной температуры в помещениях, где стоят компьютеры. Это обеспечит надежную запись информации на магнитные диски и стабильную работу всего компьютерного

оборудования.

Создание группы серверов (хостов) позволяет сэкономить средства, поскольку некоторое оборудование (например, фильтры питания, источники бесперебойного питания и устройства архивации) могут обслуживать целое помещение, и их не нужно покупать отдельно для каждого хоста и сервера. Недостаток такого подхода заключается в наличии высокого трафика в той части сети, где располагается группа серверов.

Примечание

Решение о способе расположения серверов (централизованное размещение или их распределение по разным точкам сети) часто определяется политикой внутри компании. Некоторые фирмы предпочитают централизованное расположение, что позволяет сэкономить средства на управлении и ресурсах. Другие фирмы предпочитают размещать серверы так, чтобы они отражали структуру отделов или подразделений. При таком подходе серверами управляют администраторы, имеющиеся в каждом подразделении, благодаря чему эксплуатация ресурсов может учитывать специфику конкретного подразделения.

Каналы, связывающие серверы и сетевое оборудование, должны быть высокоскоростными, и их следует изолировать от тех сегментов, в которых располагаются рабочие станции. Наличие скоростных каналов обеспечит полосу пропускания, достаточную для всех пользователей, обращающихся к серверам. Изолируя серверы от других сегментов, можно также обеспечить избыточность. Одним из способов подключения хостов является их соединение с отдельными дуплексными интерфейсами коммутатора, как показано на рис. 11.9.

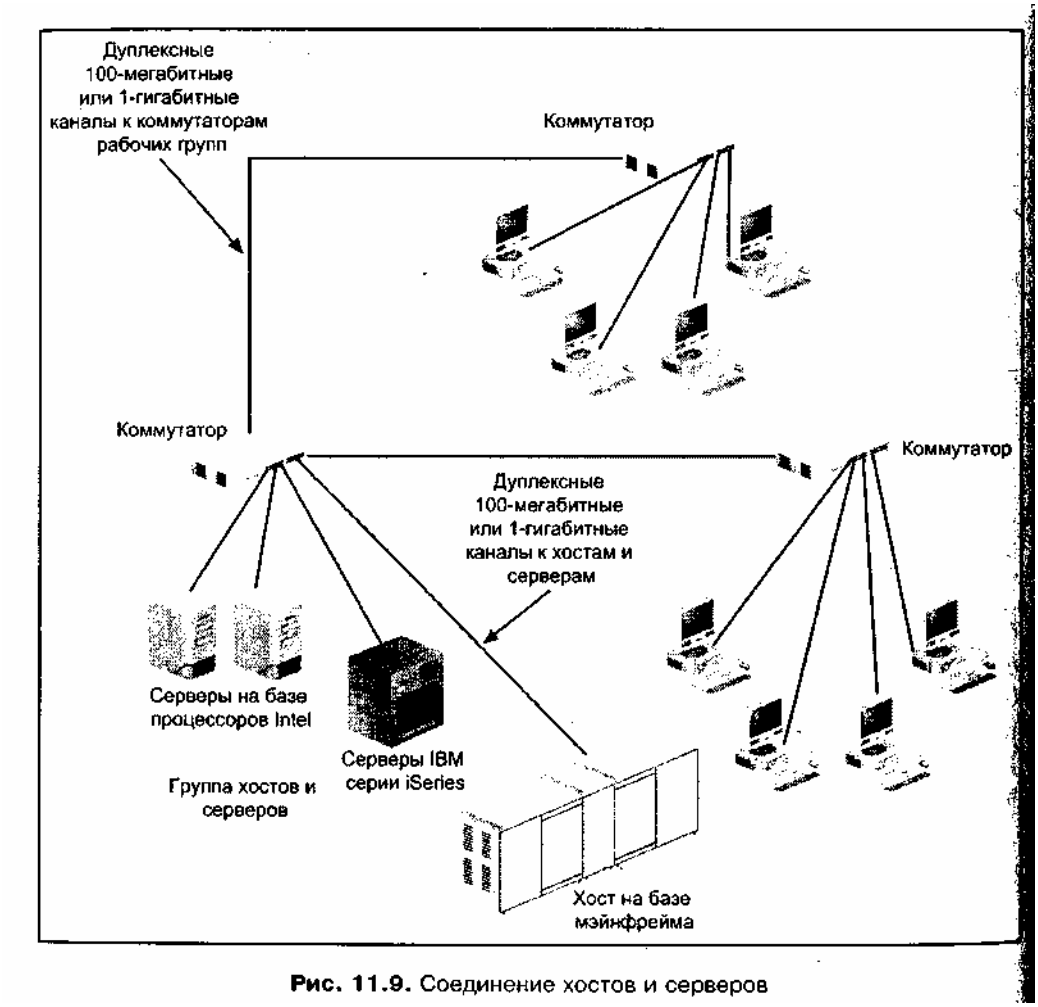


Рис. 11.9. Соединение хостов и серверов

Избыточность можно также создать, установив на серверы как минимум два сетевых адаптера, благодаря чему при отказе одного адаптера сервер сможет взаимодействовать с сетью через другой адаптер. Найдите в документации на серверные операционные системы описание способов установки нескольких сетевых адаптеров и методов привязки протоколов.

Примечание

Как уже говорилось ранее, высокоскоростной канал к серверу эффективен только тогда, когда и сетевой

адаптер, и шина, и процессор этого сервера могут работать с достаточно высокой скоростью. В противном случае сервер окажется узким местом в сети.

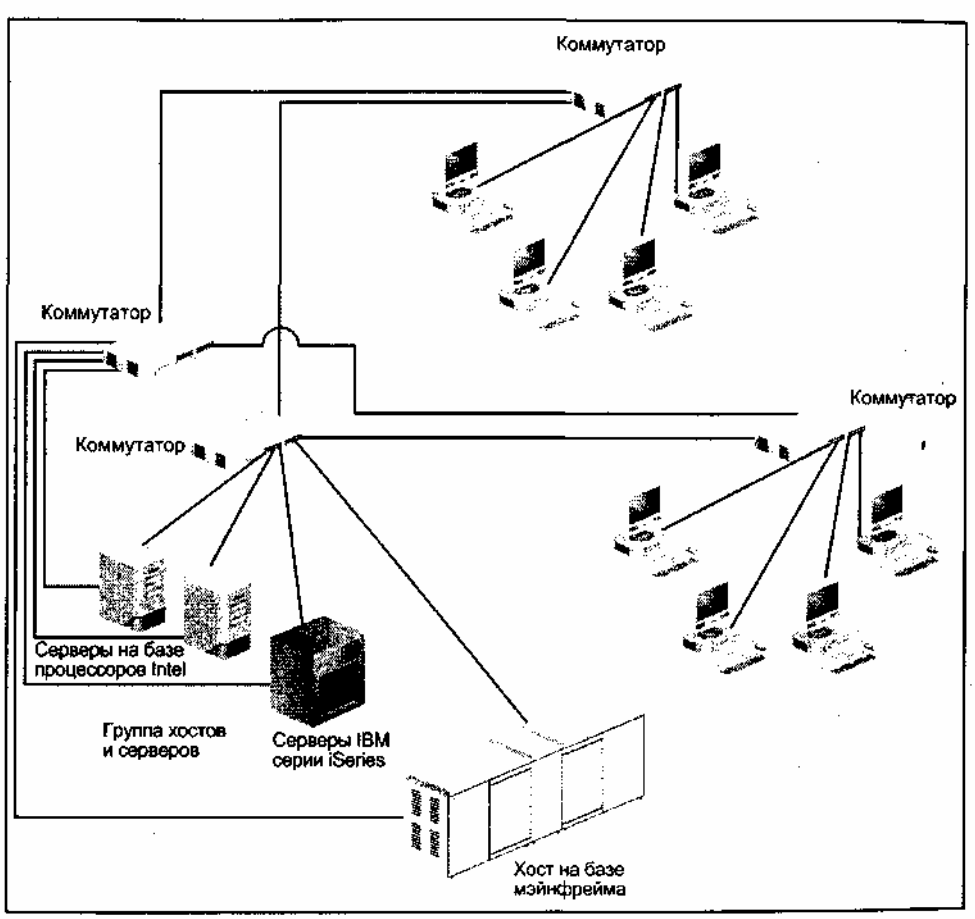


Рис. 11.10. Изолирование группы серверов и хостов, а также обеспечение избыточности

Многие организации предпочитают создавать избыточность, благодаря которой отказ одного сетевого устройства не влияет на работоспособность всей сети. Взяв за основу пример, показанный на рис. 11.9, вы можете построить структуру с избыточностью, добавив второй (резервный) коммутатор между хостом (группой серверов) и теми компьютерами, которые к нему (к ним) обращаются (рис. 11.10). Если главный коммутатор выйдет из строя, то
сетевой администратор сможет включить резервный коммутатор (который также можно настроить таким образом, что он будет работать без вмешательства со стороны администратора).

Хосты и серверы, расположенные по разным точкам сети, также необходимо непосредственно подключать к коммутаторам с помощью высокоскоростных каналов. Преимущество такого подхода заключается в том, что трафик, получается менее концентрированным, чем при создании группы серверов. Двумя другими преимуществами являются гибкость сетевой структуры в случае отказа одного из ответственных серверов и возможность установки резервных хостов на разных площадках (на случай отказа одного из хостов, или его недоступности при возникновении сетевых проблем).

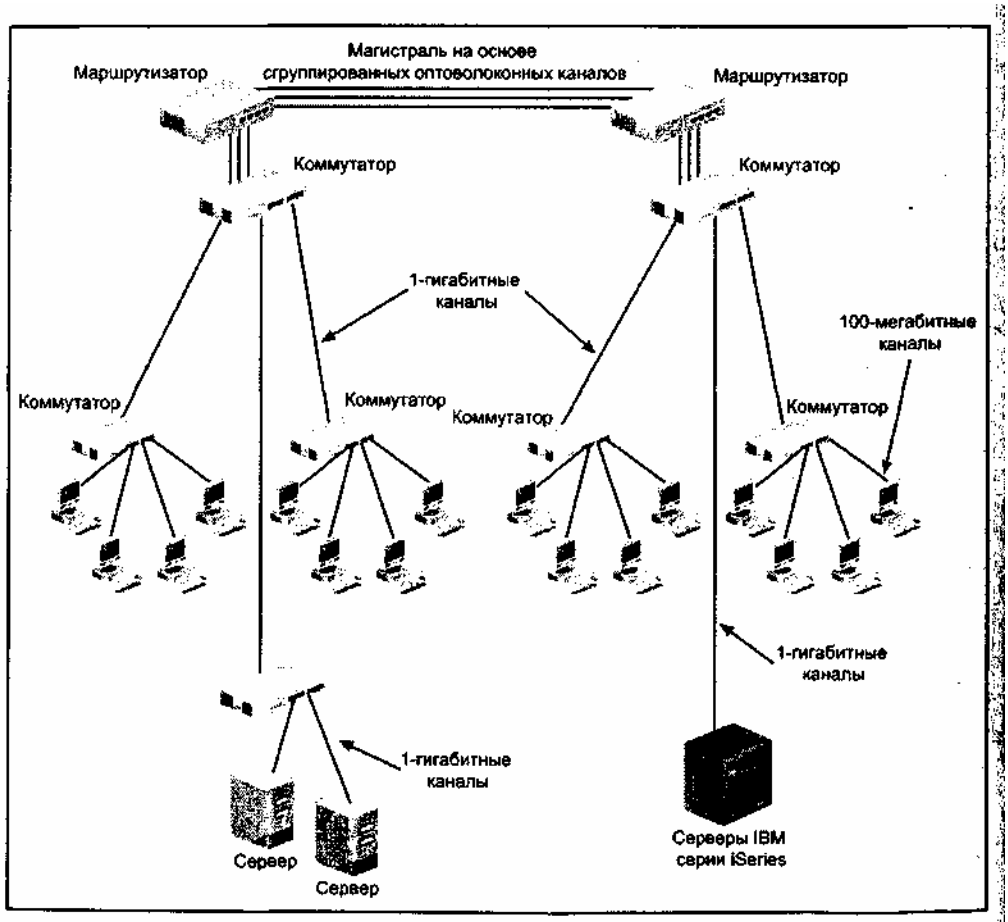


Рис. 11.11. Соединение хостов и серверов, разбросанных по сети

Недостатком рассредоточенного размещения хостов и серверов является то, что в каждой точке их установки требуется дополнительное оборудование (например, источники бесперебойного питания, системы накопителей на компакт-дисках или магнитных лентах). Кроме того, в этом случае будет затруднено централизованное управление хостами и серверами, хотя во многих операционных системах имеются средства удаленного администрирования.

На рис. 11.11 показана структура сети, в которой хосты и серверы распределены по всей сети.

Примечание

На рис. 11.11 обратите внимание на то, что система IBM подключена непосредственно к промежуточному коммутатору с помощью высокоскоростного канала. Поскольку в сети только один хост, то еще один коммутатор между ними не нужен.

Мультимедийные приложения

Мультимедийные приложения могут, в принципе, создавать очень большой трафик, однако его реальная величина зависит от типа конкретного приложения. Мультимедийные коммуникации включают в себя передачу любых типов информации: речи, видеоизображений, интерактивных или "живых" видеопотоков, графики и презентаций. Это могут быть учебная презентация или слайд-шоу, полученные через Интернет, а может быть и видеоконференция между несколькими точками.

Если мультимедийная презентация передается от сервера к одной или нескольким рабочим станциям, загрузка сети будет относительно небольшой. Пусть, к примеру, 15 студентов обращаются к некоторому веб-курсу в университетской сети. Каждое занятие длится три часа, и студенты могут просматривать курс в любое время и день недели. В этом случае нагрузка на сеть распределяется в течение недели, а не сосредотачивается в определенное время. К тому же работа с этим приложением допускает большие временные задержки, чем живая презентация. По этой причине нет смысла задумываться о гарантированном качестве обслуживания (QoS).

Нужна или не нужна мультимедийным приложениям широкая полоса пропускания – зависит от самого приложения и от числа пользователей, к нему обращающихся. Перед тем, как развертывать мультимедийное приложение, получите у разработчика текстовые показатели или определите сами

эти показатели для прогнозирования объема сетевого трафика. Если приложению не требуется широкая полоса пропускания, вполне может оказаться пригодной сетевая модель, изображенная на рис. 11.9.

В другом сценарии все студенты могут приходить в класс одновременно и заниматься в течение трех часов, работая на компьютере, где будет воспроизводиться мультимедийный курс, содержащий звук, слайды Microsoft PowerPoint и анимацию. В данной ситуации потребуется более широкая полоса пропускания и контроль над той частью сети, где будет запускаться мультимедийный курс. В силу этих обстоятельств в структуре сети необходимо предусмотреть подключение сервера к сети через маршрутизатор и сгруппировать каналы, как показано на рис. 11.12.

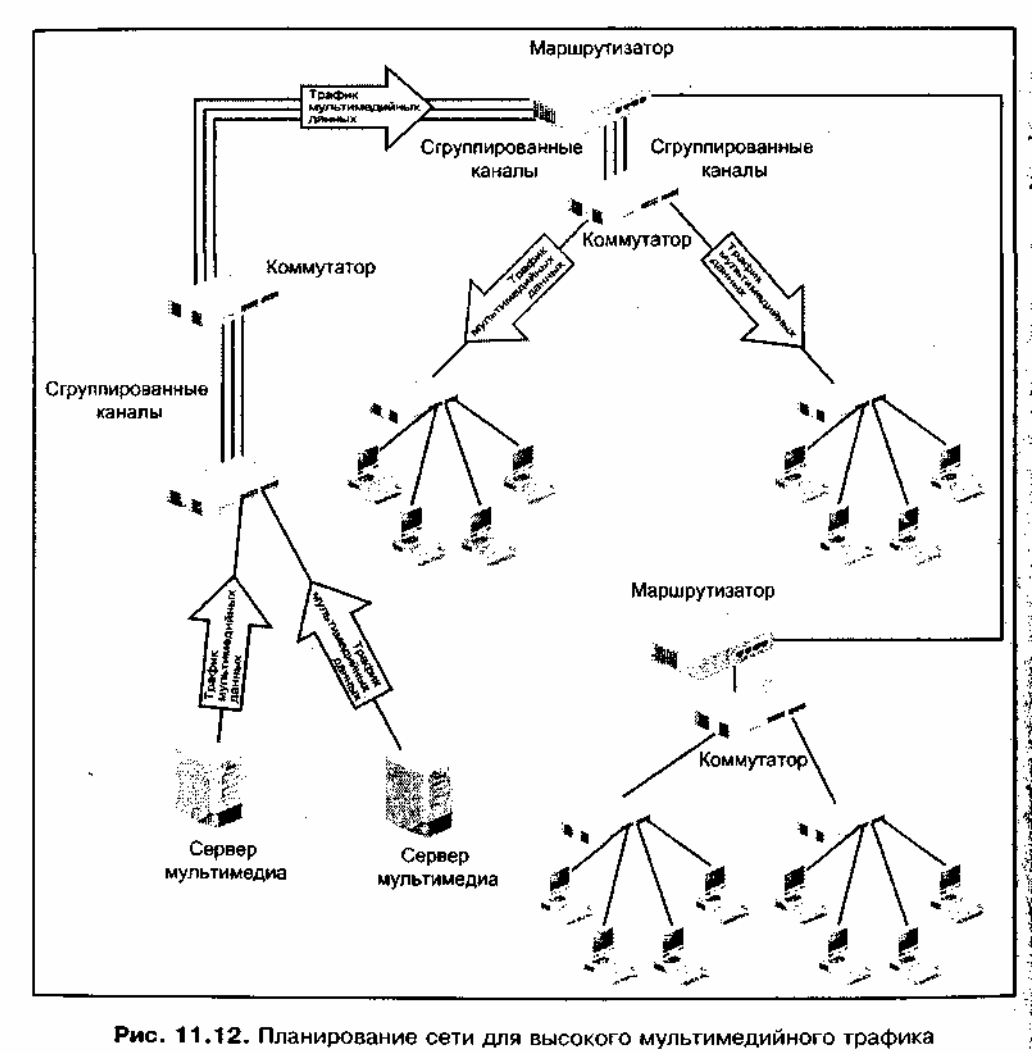


Рис. 11.12. Планирование сети для высокого мультимедийного трафика

Если в приложении предусмотрен режим многоадресного вещания, то участвующие в работе станции делятся на группы подписки. При многоадресном вещании создаются группы пользователей, запросивших определенный
мультимедийный поток, после чего для снижения нагрузки на сеть передача ведется одновременно для всех членов конкретной группы подписки. Любой поток данных состоит из отдельных мультимедийных пакетов, каждый из которых рассылается одновременно по многим адресам (в отличие от ситуации, когда отдельный пакет передается только по определенному адресу). Рассмотрим, например, класс из 12-ти пользователей, которые запускают один и тот же видеокурс с некоторого сервера. За счет мультивещания один передаваемый видеопоток пересылается сразу всем 12-ти пользователям. Сравните эту ситуацию с однонаправленными рассылками, при которых сервер должен один и тот же поток разослать 12 раз (каждому из 12-ти пользователей).

При осуществлении многоадресного вещания и сервер, и каждая клиентская рабочая станция должны быть настроены для выполнения многоадресных операций, что требует установки протокола *Internet Group Management Protocol (IGMP)* (Межсетевой протокол управления группами) и других протоколов многоадресной (групповой) маршрутизации. Протокол IGMP также конфигурируется на маршрутизаторах, связывающих сервер и рабочие станции, поскольку сервер мультимедиа использует его для того, чтобы сообщить маршрутизаторам, какие станции принадлежат к

определенной группе (или группам) мультивещания. На рис. 11.12 показано, как маршрутизаторы обеспечивают управление трафиком, используя протокол IGMP для разделения трафика таким образом, чтобы он передавался только в те сегменты, в которых располагаются станции, подписанные на получение информации от мультимедийного приложения.

Структуры беспроводных локальных сетей

В беспроводных локальных сетях используются две основные топологии: одноранговая (peer-to-peer) и многоячеечная (multiple-cell). Одноранговая архитектура присуща небольшим сетям с числом пользователей, не превышающим 20–25. При использовании устройств стандарта 802.На все взаимодействующие друг с другом станции должны находиться в радиусе 18 м, в случае применения устройств стандарта **802.11b** это расстояние увеличивается до 90 м.

На рис. 11.13 изображена одноранговая топология сети стандарта **802.11b**. В этой структуре фактически имеется только одна ячейка, внутри которой вещают все станции. При этом отсутствует точка доступа, соединенная с кабельной локальной сетью.

В многоячеечной структуре используются точки доступа (например, беспроводные мосты, подключенные к кабельной локальной сети). Вокруг каждой точки доступа образуется ячейка. Если имеются четыре точки доступа, то существуют четыре ячейки. Некоторые станции (например, настольные системы) могут располагаться в ячейке неподвижно. Другие станции (такие, как портативные компьютеры) могут перемещаться от одной ячейки к другой.
Ячейки сконфигурированы так, что можно обеспечить роуминг с использованием какого-нибудь соответствующего протокола (например, Inter-Access Point Protocol, IAPP). Широковещательная область вокруг каждой ячейки имеет радиус 18 м для устройств стандарта **802.11a** и 90 м для устройств стандарта 802.11b. На рис. 11.14 изображена многоячеечная топология на базе устройств **802.11b**.

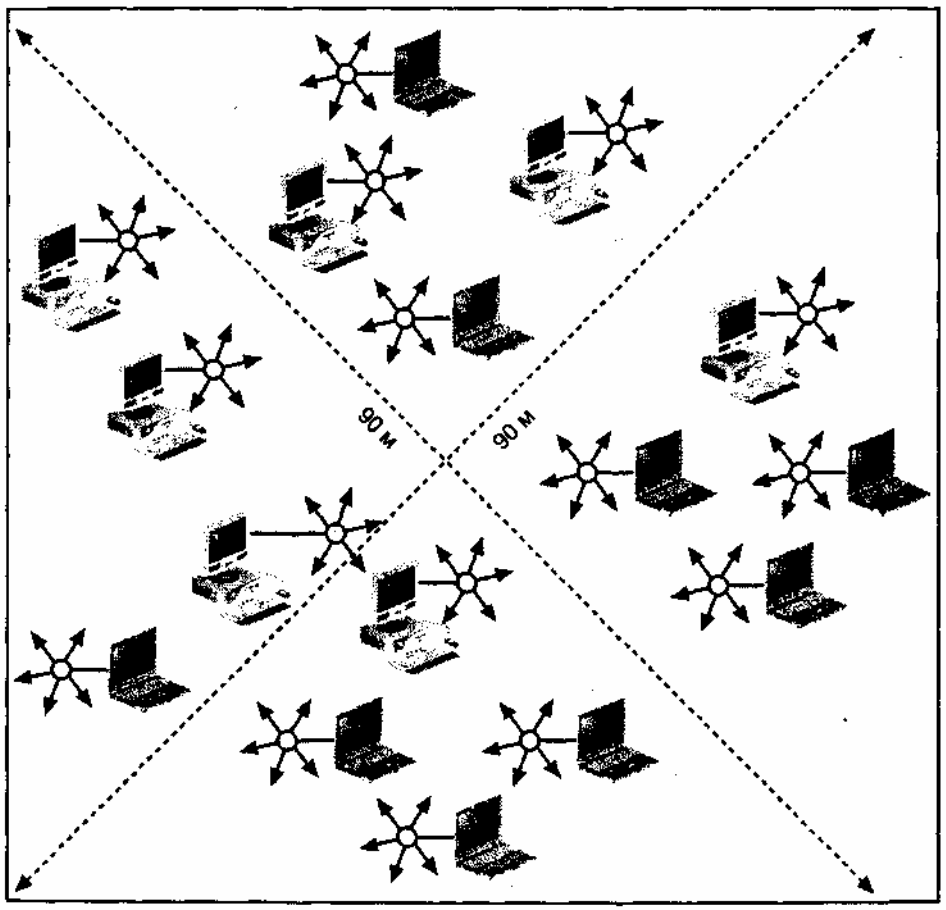


Рис. 11.13. Структура сети стандарта 802.11b с одноранговыми коммуникациями

Совет

Если вы не хотите разрешать роуминг, настройте по-разному каждую точку доступа и связанные

с ней рабочие станции. При этом некоторая станция сможет взаимодействовать только с определенной точкой доступа.

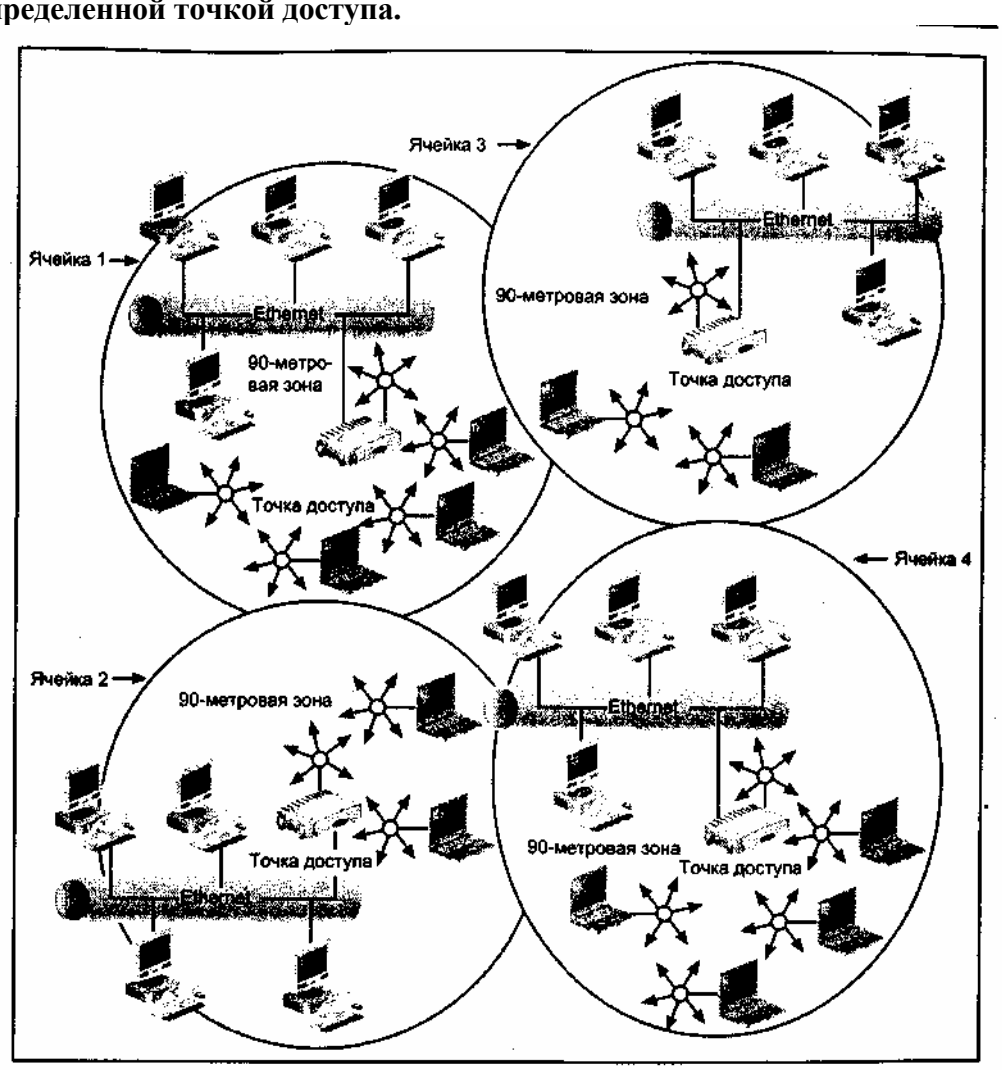


Рис. 11.14. Структура многоячеечной сети стандарта 802.11b

Вопросы эксплуатации и поддержки

Эксплуатация и поддержка имеющегося сетевого оборудования (например, устаревших мостов и маршрутизаторов) могут быть довольно сложными. Нередко поставщики определяют для своего оборудования время конца срока службы (end-of-life, EOL), после которого они прекращают выпускать обновления аппаратных или программных средств. (Иногда это время продлевается для оборудования, используемого в важных правительственных или военных организациях, и оканчивается при его замене.)

Если в оборудовании имеются "интеллектуальные возможности" (например, поддержка протокола SNMP), то возникают специфические проблемы в тех случаях, когда перестают выпускаться обновления программных или микропрограммных средств, поддерживающие совместимость этого оборудования с новыми сетевыми возможностями или с новым сетевым оборудованием. Кроме того, поставщик может отказать в замене неисправных устройств после даты окончания срока службы.

У сравнительно нового сетевого оборудования существует несколько преимуществ. Наиболее очевидное – то, что для этого оборудования имеются все виды обновлений. Новое оборудование можно также отослать изготовителю для ремонта. Некоторые поставщики предлагают программы обновления технологий, позволяющие клиентам заменять стареющее оборудование на новое при минимальных, специально оговоренных затратах. У крупных поставщиков имеются веб-сайты, с которых клиенты могут загрузить обновления программных и микропрограммных средств. На этих сайтах можно оставлять сообщения об ошибках и находить информацию о способах установки, конфигурирования и ремонта оборудования. Также практикуется заключение контрактов со специалистами, помогающими в решении сложных проблем, и поиск обучающих программ для определенных типов оборудования (например, для маршрутизаторов). Вероятнее всего, такие

программы для относительно нового оборудования будут доступнее, чем для устаревшего.

Совет

Перед тем как покупать некоторое устройство, только появившееся на рынке, подождите несколько месяцев, пока другие не обнаружат возможные проблемы, а изготовитель не устранит их.

Принципы проектирования глобальных сетей

Обычно проектирование глобальных сетей включает в себя этап подключения локальной сети или некоторого узла к глобальной сети. Для подключения локального узла к глобальной сети используются следующие устройства:

- маршрутизаторы;
- серверы доступа;
- модемы;
- специализированные адаптеры;
- мультиплексоры;
- беспроводные, микроволновые и спутниковые устройства;
- коммутаторы доступа к глобальной ATM-сети.

Способ подключения к глобальной сети зависит от типа этой сети и спецификаций поставщика сетевых услуг. Распространенным и простым способом подключения локального узла к некоторой глобальной сети является использование модема, терминального адаптера (TA), адаптера DSL или X.25, установленного на сервере, работающим под управлением систем UNIX, Windows 2000 или NetWare. Другим способом, обеспечивающим более широкий спектр возможностей, является установка сервера доступа, имеющего одно или несколько перечисленных устройств (модемов или адаптеров).

Для наиболее оптимального управления сетевым трафиком и для реализации функций брандмауэра сервер или сервер доступа необходимо подключать непосредственно к отдельному интерфейсу маршрутизатора, т. е. нельзя использовать те же интерфейсы, с которыми связаны коммутаторы и сегменты рабочих групп. При такой организации сети сервер или сервер доступа оказывается ближе к сетевой магистрали, в результате чего уменьшается количество ретрансляций несущего сигнала через некоторое сетевое устройство. На рис. 11.15 изображен типовой способ конфигурирования топологии локальной сети для осуществления глобальных коммуникаций.

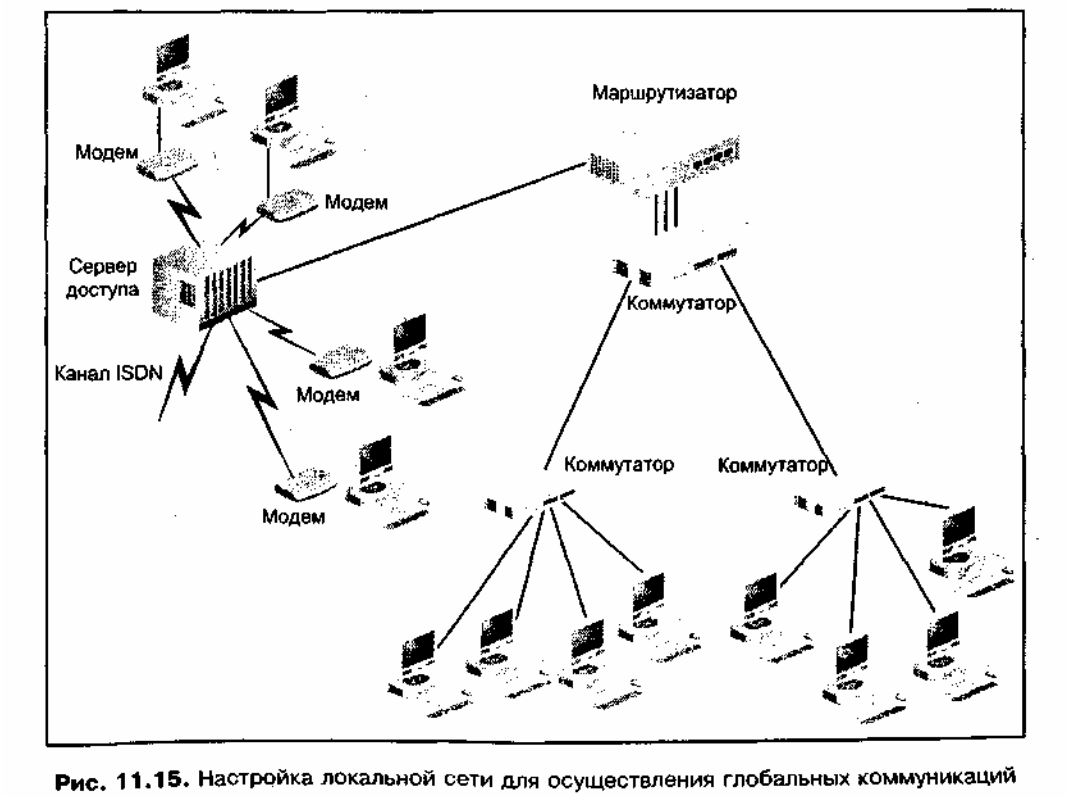


Рис. 11.15. Настройка локальной сети для осуществления глобальных коммуникаций

Другим способом подключения локальной сети к глобальной является применение маршрутизатора и

устройств CSU/DSU (устройство обслуживания канала/устройство обработки данных). Маршрутизатор позволяет контролировать трафик глобальной сети и может выполнять функции брандмауэра для входящего и исходящего трафика. На рис. 11.16 показано, как с помощью маршрутизатора подключить локальную сеть к глобальной.

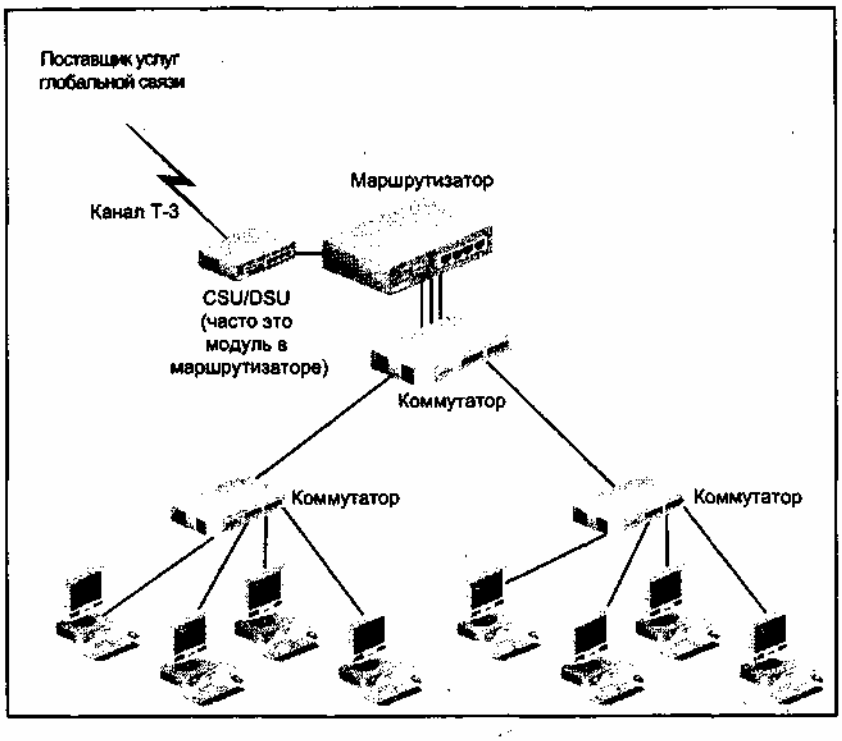


Рис. 11.16. Подключение к глобальной сети через маршрутизатор и устройства CSU/DSU

Для сверхскоростных подключений к глобальным сетям можно применить коммутатор доступа к глобальной ATM-сети или модуль с аналогичными функциями в стоечном сетевом устройстве. Такой коммутатор с одной стороны подключается к локальной сети с использованием топологии, изображенной на рис. 11.15, а с другой – к некоторой ATM-совместимой глобальной сети (например, к SONET).

Беспроводные региональные и глобальные сети

Существует несколько спецификаций беспроводных региональных и глобальных сетей, выбор которых зависит от необходимых расстояний и требуемых технологий. На момент написания этой книги многие их этих спецификаций были частными (не стандартизованными), для их реализации использовались радиоволны, инфракрасное излучение и СВЧ-волны. В следующих разделах кратко описаны имеющиеся возможности для организации беспроводных региональных и глобальных сетей.

Спецификации беспроводных региональных сетей

Небольшую региональную сеть с зоной охвата, равной 90 м, можно построить на базе устройств стандарта **802.11b**. При таком подходе можно соединить два здания, поместив беспроводные мосты (точки доступа) в сетях этих зданий. Беспроводные мосты подключаются к расположенным на крышах зданий направленным антеннам, обеспечивающим двухточечные коммуникации *(см. рис. 9.1 в главе 9)*. Можно выбрать какую-нибудь из частных спецификаций сетей с использованием ИК-излучения, в состав которых входят беспроводные мосты, находящиеся в зданиях, и направленные излучатели, располагающиеся на крышах зданий и создающие узкий лазерный луч. Некоторые из этих частных спецификаций обеспечивают непрерывную передачу данных между мостами со скоростью до 20 Мбит/с.

Частные спецификации сетей с использованием радиоволн можно применять для создания региональных сетей с зоной охвата до 48 км. На коротких расстояниях (до 4,8 км) региональные радиосети могут передавать информацию со скоростью 11 Мбит/с и выше. По мере увеличения расстояния уменьшается скорость передачи: до 1–2 Мбит/с при расстоянии 48 км.

Примечание

В настоящее время разрабатываются радиосети, обеспечивающие передачу данных во всех направлениях

на расстояния до 56 км. Скорости в этих сетях достигают 10 Мбит/с. Имеются две прорабатываемые спецификации: Multichannel Multipoint Distribution Service (MMDS) и Local Multipoint Distribution Service (LMDS).

Также для создания беспроводных региональных сетей можно использовать наземные системы СВЧ-связи, которые обычно обеспечивают скорости передачи до 10 Мбит/с. При этом приходится приглашать организации, имеющие лицензию на использование СВЧ-коммуникаций для организации сетей. Обычно наземные СВЧ-каналы обходятся дороже, чем системы с использованием радиоволн и ИК-излучения, к тому же их сложнее эксплуатировать.

Спецификации беспроводных глобальных сетей

Беспроводные глобальные сети можно создавать на базе геосинхронных и низкоорбитальных (LEO) спутников Земли. Орбиты геосинхронных спутников проходят на высоте 36 000 км. Для работы с ними необходимо приобретать время у поставщиков услуг. Можно запустить собственный спутник, что будет стоить огромных денег. Одна из проблем, возникающих в прошлом при использовании геосинхронных спутников, заключалась в том, что между спутником и Землей возникала 540-миллисекундная задержка передачи данных. Это осложняло коммуникации по протоколу TCP, поскольку требовало настройки скользящего окна, в результате чего реальная скорость коммуникаций оказывалась намного ниже реальных возможностей спутниковой технологии.

Если вы решили для реализации глобальной сети использовать геосинхронные спутники, обсудите с поставщиком услуг возможность установки TCP-шлюзов между вашими передающими узлами и спутником. Этот шлюз используется для такой настройки скользящего окна, чтобы оно соответствовало задержке спутниковых коммуникаций. Кроме того, шлюз обеспечивает специальную синхронизацию подтверждений TCP для принятых пакетов, а также позволяет сжимать данные. Благодаря этим возможностям, TCP-шлюз позволяет значительно, почти на 100 % увеличить скорость TCP/IP-коммуникаций с использованием геосинхронных спутников и приблизиться к скорости 10 Мбит/с, заявленной для этой спутниковой технологии.

Согласно прогнозам, глобальные сети на базе LEO-спутников появятся в 2005 году. Эта технология обещает быть перспективной, т. к. орбиты спутников будут проходить на высоте от 700 до 1600 км от Земли, в результате чего задержки будут намного меньше, чем при использовании геосинхронных спутников. По всей видимости, LEO-спутники смогут обеспечить скорости от 128 Кбит/с до 100 Мбит/с при передаче данных к спутнику и до 700 Мбит/с при передаче информации от спутника. Когда глобальные сети на базе LEO-спутников станут реальностью, они сделают глобальные коммуникации доступными для индивидуальных и корпоративных пользователей в любой точке планеты.

Топологии, предоставляемые поставщиками услуг глобальных сетей

Топологии глобальных сетей обычно реализуются выбранным поставщиком услуг глобальных коммуникаций. Выбираемые вами услуги зависят от требуемой полосы пропускания, от объема выделенных средств, а также от скорости и типа интерфейсов в вашей локальной сети.

Если компания поставщика услуг небольшая или среднего масштаба, то этот поставщик может попросту купить услуги у крупной компании подобно тому, как оператор междугородных телефонных разговоров приобретает телефонные каналы у крупной телекоммуникационной компании. Для обслуживания клиентов мелкие поставщики могут использовать одно устройство (например, маршрутизатор), подключенное к крупной компании через банк коммутируемых модемов или серверы доступа. Некоторые мелкие поставщики предлагают услуги электронной почты и некоторые веб-сервисы (например, персональные веб-страницы). Крупные поставщики могут предлагать и другие службы: веб-хостинг, электронную почту, службы архивации для персональных компьютеров и серверов, а также программные ресурсы и базы данных. Крупные поставщики предлагают комбинированные службы (FDDI, ATM, ISDN, T-линии, SONET и другие), построенные на основе оптоволоконных технологий с использованием различных уровней избыточности.

Структура затрат

Поставщики услуг глобальных сетей предлагают службы с различными возможностями доступа: от неограниченного до ограниченного с поминутной оплатой (с учетом тарифа, выбранного пользователем). Для типовой сети среднего размера, подключенной к глобальной сети, общие расходы на оплату

глобальных коммуникаций составляют приблизительно одну треть от общих расходов на поддержание сети. В отличие от расходов на локальную сеть, которые могут значительно изменяться от месяца к месяцу (в зависимости от стоимости обновлений и новых программ), расходы на услуги глобальной сети остаются относительно стабильными, поскольку определяются ежемесячными выплатами (подобно тому, как ежемесячно оплачиваются телефонные услуги). Иногда на величину расходов влияют стоимость обновлений или расширений оборудования, что временно увеличивает расходы.

Фактические затраты на развертывание и эксплуатацию глобальной сети определить сложно, поскольку имеются как прямые, так и косвенные расходы. Примером прямых расходов является ежемесячная плата за некоторую услугу. Обучение и поддержка пользователей является примером области косвенных расходов. При анализе расходов на глобальную сеть учитывайте следующие факторы:

- ежемесячная плата за услуги;
- стоимость оборудования для подключения локальной сети к глобальной;
- стоимость обучения и поддержки пользователей;
- стоимость обучения сетевого персонала;
- расходы на поддержку сети и устранение неисправностей;
- потери рабочего времени при разрыве соединения;
- затраты на периодическую модернизацию оборудования.

Крупные поставщики услуг глобальных сетей предлагают *соглашение об уровне сервиса* (service level agreement, SLA), представляющее собой некоторое соглашение между поставщиком и клиентом, гарантирующее минимальный уровень обслуживания. В нем обычно оговариваются следующие моменты:

- гарантированное время готовности (например, оговаривается, что линия будет доступна для клиента в течение 95% всего времени);
- максимальная задержка на линии;
- гарантированное или среднее время, в течение которого неисправная линия будет восстановлена *(среднее время ремонта* (mean time to repair, MTTR));
- гарантированная пропускная способность;
- величина издержек, которую поставщик возместит клиенту в случае нарушения соглашения об уровне сервиса.

Выбор полосы пропускания

Ширина необходимой полосы пропускания зависит от используемых приложений и типа полосы, предоставляемой поставщиком услуг глобальных сетей. Большинство поставщиков в определенном регионе предоставляют приблизительно одинаковые службы и полосы пропускания почти по одинаковой цене. Некоторые поставщики предлагают "полосы пропускания по запросу", что означает возможность расширения или сужения полосы в зависимости от потребностей в конкретный момент времени. Такая услуга оплачивается с учетом ширины реально использованной полосы пропускания и часто распространяется на коммутируемые линии со скоростью 56 Кбит/с или линии ISDN.

Многие поставщики предлагают выделенную полосу пропускания со скоростью от 56 Кбит/с до 155 Мбит/с. В этом случае клиенту дается возможность стратегического выбора: например, линия со скоростью 56 Кбит/с может использоваться для отдельных простых файловых пересылок, а по линии со скоростью 155 Мбит/с может передаваться непрерывный мультимедийный трафик. Кроме того, поставщики предлагают гибкие тарификационные планы, так что даже небольшая компания или домашний пользователь могут воспользоваться достоинствами высокоскоростных каналов. Полоса пропускания, доступная в некотором регионе, зависит от того, какие услуги предлагаются в этом регионе. В одних районах (например, в сельских) доступны только традиционные телефонные линии, а в других – спутниковые глобальные службы. В третьих имеются службы T-1 и T-3, а в некоторых городских районах предлагаются сверхскоростные и специализированные оптоволоконные службы.

Выбор поставщика услуг зависит от ширины необходимой полосы пропускания и соглашения об уровне сервиса, предлагаемого конкретным поставщиком. Крупные глобальные поставщики предлагают как минимум магистраль OC-12 (622 Мбит/с) в составе *ячеистой сети* (meshed

architecture). В сети с такой архитектурой существует множество альтернативных информационных магистралей, благодаря чему в случае отказа одной из них коммуникации автоматически перенаправляются по другим магистралям и это происходит незаметно для пользователя. Мелкие поставщики предлагают низкоскоростные соединения со скоростью от 64 Кбит/с до 622 Мбит/с и обычно ограничивают до двух число пересылок ("прыжков") через маршрутизаторы.

Оборудование поставщика услуг и клиентское оборудование

Поставщики услуг глобальных сетей имеют со своей стороны различное оборудование: от банков коммутируемых модемов до групп каналов и интерфейсов маршрутизаторов. Используемое оборудование соответствует размеру компании-поставщика. Кроме того, оборудование поставщика должно располагаться на нескольких площадках. Иногда выполняются подключения к оборудованию, которое находится на спутниковых точках присутствия (point of presence), располагающихся далеко от основной распорядительной станции, а иногда подключения осуществляются непосредственно к оборудованию этой станции. Услуги, приобретаемые у небольших Интернет-провайдеров, могут быть реализованы на оборудовании, находящемся в плохо оборудованных помещениях. Такие ситуации нужно тщательно проанализировать, поскольку от надежности и производительности этого оборудования будет непосредственно зависеть качество предоставляемых вам услуг.

Некоторые поставщики кооперируются и располагают свое коммуникационное оборудование в одних и тех же помещениях. Обычно это делается для того, чтобы организовать специализированные службы, которые они не смогли бы предложить самостоятельно. Такие мероприятия могут быть дорогостоящими и требовать специальных мер безопасности.

С помощью технологий кабельного телевидения обеспечивается передача данных, речи и видео в большинстве районов страны. Слияние компаний кабельного телевидения и телефонных компаний привело к появлению интегрированных услуг почти во всех районах США, для чего используются существующие кабели и точки присутствия. Все, что нужно клиенту, – это кабельный модем и соответствующее периферийное оборудование (например, персональный компьютер и телефон). Такие средства подключения к Интернету быстро распространяются в оставшихся (частично сельских) районах США и в других странах, в которых в настоящее время отсутствуют рентабельные способы подключения к Интернету. Кабельные службы особенно хорошо подходят для совместной передачи речи, видеоизображений и данных. Иногда клиент получает собственное оборудование от поставщика услуг глобальных сетей, а иногда должен приобретать его сам. К тому же, в настоящее время некоторые производители рабочих станций и серверов оборудуют их специализированными устройствами, необходимыми для подключения к глобальной сети: модемами, терминальными адаптерами (TA), адаптерами X.25, DSL и др. Эти же производители также выпускают специализированные серверы удаленного доступа со встроенными модемами, терминальными адаптерами и адаптерами DSL, а также с программным обеспечением для удаленного доступа (как, например, служба Remote Access Service в системе Windows 2000).

Перед тем как выбрать поставщика услуг глобальных сетей, узнайте, какое оборудование предлагает конкретный поставщик для реализации подключения к глобальной сети. В некоторых случаях вы можете приобрести оборудование либо у поставщика, либо в другой компании, продающей сетевые устройства. В других случаях вам остается лишь выбрать вариант оборудования, которое предлагает сам поставщик. Когда вы решаете, какое оборудование нужно покупать, помните о том, что стоит потратить немного больше денег и приобрести самое надежное оборудование, которое обеспечит вам бесперебойную связь.

Резюме

1. При проектировании сети выбирайте те сетевые технологии и устройства, которые позволяют расширять сеть в будущем. Помимо этого, учитывайте имеющиеся в организации требования к безопасности и предусматривайте возможность подключения сети к линиям глобальных коммуникаций. Важно правильно выбрать кабельную систему, поскольку она определяет всю инфраструктуру сети.
2. Качественная кабельная система включает в себя гибкую, многофункциональную горизонтальную разводку, выполненную с учетом требований к структурированной разводке (примером может

служить звездообразная топология с использованием витой пары, соединяющая рабочие станции с коммутаторами).

3.Вертикальная разводка в структурированной сети представляет собой высокоскоростной кабель, проложенный между этажами (например, многомодовый оптоволоконный кабель).

4. Структурированная сеть может быть построена централизованно, т. е. в ней можно выделить опорные точки, позволяющие расширять сеть и управлять ею.

5. Современные методы проектирования предусматривают использование дуплексных коммуникаций, в которых отсутствуют конфликты.

6. В современных сетях используются коммутаторы и маршрутизаторы (для обеспечения гибкости сетевой структуры), а также предусматриваются высокоскоростные решения и избыточность. Многие сети создаются с избыточностью для того, чтобы обеспечить практически бесперебойное обслуживание даже в случае отказа некоторой части сети.

7. В процессе проектирования следует составлять запросы информации и заявки на предложения, которые позволяют организации сформулировать свои потребности, а поставщикам – продемонстрировать свои решения, удовлетворяющие этим потребностям.

8. Сети проектируются так, чтобы трафик к хостам и серверам был изолирован. Это позволяет уменьшить общий трафик в сети и обеспечить безопасность хостов и серверов. Сети для мультимедийных приложений зачастую требуют большей полосы пропускания и установки протокола Internet Group Management Protocol (IGMP).

9. В беспроводных локальных сетях используются две основные топологии: одноранговая и многоячеечная.

10.П Эксплуатация локальной сети – это непрерывный процесс, для упрощения которого можно, в частности, составить план замены устаревающих устройств, чтобы их обновление происходило раньше, чем они начнут усложнять эксплуатацию сети.

11. Для подключения локальных сетей к глобальным используются различные проектировочные решения и правильно выбранное коммуникационное оборудование (коммутаторы, серверы доступа, модемы, мультиплексоры, коммутаторы и беспроводные технологии).

12. Наиболее подходящие решения для создания беспроводных региональных сетей – это технологии, использующие радиоволны и инфракрасное излучение. Для построения беспроводных глобальных сетей применяются геосинхронные и низкоорбитальные (LEO) спутники Земли, причем LEO-спутники будут введены в строй только в 2005 году.

13.При проектировании подключений к глобальной сети нужно учитывать такие факторы, как стоимость, необходимая полоса пропускания и выбор оборудования, совместимого с оборудованием поставщика услуг глобальных сетей.