Дорогие ученики!

Это учебное пособие разработано всемирно известной корпорацией Майкрософт, мировым лидером в производстве программного обеспечения, в рамках инициативы «Партнерство в образовании». Задача этой инициативы — предоставить школам возможность повышения качества обучения благодаря использованию информационных технологий в учебном процессе.

Информационные технологии обладают достаточным потенциалом, чтобы дать вам возможность приобрести навыки, которые будут необходимы в будущей работе, — навыки эффективной обработки информации и управления ею, навыки общения и совместной (групповой) работы. Для развития этих и других навыков, получивших название «навыки XXI века», и служат разработанные Майкрософт учебные пособия.

Участие Майкрософт в создании этих учебников обеспечивает высокое качество учебных пособий и передачу экспертного знания, накопленного внутри корпорации, непосредственно учителю и ученику. Некоторые учебные курсы Майкрософт серии «Партнерство в образовании» предназначены для подготовки грамотных пользователей персональных компьютеров, другие предназначены для ребят, более глубоко интересующихся информационными технологиями и желающих стать специалистами в этой области.

Учебные курсы Майкрософт серии «Партнерство в образовании» переведены на языки многих стран мира и успешно используются во многих странах.

Вы держите в руках учебное пособие **«Основы компьютерных сетей»**, которое познакомит вас с основами грамотного построения и поддержки компьютерных сетей, с работой сетевых приложений в локальных сетях и в Интернете. Освоив этот курс, вы сможете создавать и поддерживать сетевые соединения, приобретете знания и навыки, востребованные в сегодняшнем высокотехнологичном обществе.

Среди других учебников, разработанных компанией Майкрософт:

- **Учебные проекты с использованием Microsoft Office.** Курс предполагает выполнение различных увлекательных проектов, знакомящих учеников с некоторыми, ранее неизвестными областями деятельности (например, с такими, как основы маркетинга, грамотное составление резюме и поиск работы, оптимальные подходы к совершению покупок и др.).
- **Основы программирования на примере Visual Basic .NET.** Курс поможет вам погрузиться в увлекательный мир объектно-ориентированного программирования и почувствовать себя творцом, способным создавать интересные программы. Этот курс позволит вам лучше понять работу программиста.
- **Персональный компьютер: настройка и техническая поддержка.** Курс дает необходимую теоретическую и практическую подготовку для работы в качестве специалистов службы технической поддержки. Программа курса включает обучение ремонту и настройке компьютеров, базам данных и основам работы служб технической помощи.

Мы желаем вам успехов на пути обретения новых знаний и будем рады, если вам понравится наш курс! О своих впечатлениях об этом учебном курсе вы можете рассказать нам, написав по электронной почте на адрес:

russia@microsoft.com

С самыми наилучшими пожеланиями,
сотрудники российского Представительства Майкрософт
http://www.microsoft.com/rus

Рекомендации по использованию учебного курса

Учебный курс «Основы компьютерных сетей» дает вам возможность познакомиться с основами построения и функционирования локальных и глобальных компьютерных сетей, позволяет научиться планировать, создавать, настраивать и поддерживать работу компьютерных сетей.

В состав курса входят:

- учебное пособие по созданию и поддержке компьютерных сетей;
- методическое пособие для учителей по основам компьютерных сетей, доступное для загрузки с веб-сервера www.microsoft.com\rus\education;
- компакт-диск, прилагаемый к методическому пособию для учителя, в том числе содержащий курс «Системный администратор школьной компьютерной сети», а также дополнительные материалы и полезное программное обеспечение для учителя, обслуживающего школьные компьютерные сети на базе Microsoft Windows XP Professional и Microsoft Windows Server 2003.

В тексте пособия приняты следующие шрифтовые выделения и значки:

- *курсивом* выделены важные понятия и термины;
- **жирным шрифтом** выделены названия диалоговых окон, пунктов меню и управляющих элементов (текстовых полей, кнопок и т. д.) графического интерфейса, а также ключевые термины в определениях;
- выводы и важные замечания отмечены значком  ;
- материалы, содержащие дополнительную интересную информацию, выделены значком  ;
- вопросы и задания в конце каждой главы сопровождаются значком .

Глава 1 Что такое компьютерная сеть

В этой главе вы найдете ответы на следующие вопросы:

- *Что такое сеть?*
- *Какие возможны типы сетей?*
- *Каковы особенности одноранговых сетей и сетей на основе сервера?*
- *Что такое комбинированные сети?*
- *Как компьютеры взаимодействуют друг с другом?*

Попробуем представить себе мир примерно тридцать пять — сорок лет назад. Мир без общедоступных компьютерных сетей. Мир, в котором каждый компьютер должен был иметь собственное хранилище данных и собственный принтер. Мир, в котором не было электронной почты и систем обмена мгновенными сообщениями (например, ICQ). Как ни странно это звучит сейчас, но до появления компьютерных сетей все это было именно так.

Компьютеры — важная часть сегодняшнего мира, а компьютерные сети серьезно облегчают нашу жизнь, ускоряя работу и делая отдых более интересным. Благодаря этой книге вы узнаете, как устроены и работают компьютерные сети, научитесь проектировать и создавать их, освоите работу с наиболее популярными сетевыми приложениями.

Практически сразу после появления ЭВМ возник вопрос о налаживании взаимодействия компьютеров друг с другом, чтобы более эффективно обрабатывать информацию, использовать программные и аппаратные ресурсы. Появились и первые сети, в то время объединявшие только большие ЭВМ в крупных компьютерных центрах. Однако настоящий «сетевой бум» начался после появления персональных компьютеров, быстро ставших доступными широкому кругу пользователей — сначала на работе, а затем и дома. Компьютеры стали объединять

в локальные сети, а локальные сети — соединять друг с другом, подключать к региональным и глобальным сетям. В результате за последние пятнадцать–двадцать лет сотни миллионов компьютеров в мире были объединены в сети, и более миллиарда пользователей получили возможность взаимодействовать друг с другом.

Сегодня можно с уверенностью сказать, что компьютерные сети стали неотъемлемой частью нашей жизни, а область их применения охватывает буквально все сферы человеческой деятельности.

Сеть (Network) — группа компьютеров и/или других устройств, каким-либо способом соединенных для обмена информацией и совместного использования ресурсов.

Представьте, что у вас есть несколько отдельных, не связанных в сеть компьютеров. Чтобы в такой *автономной* среде работать с одними и теми же данными, нужно с одного компьютера скопировать файлы на какой-либо носитель (например, на дискету), после чего перенести эти файлы на другие компьютеры. А для быстрой распечатки документов придется снабдить каждый из компьютеров отдельным принтером. Одновременная же совместная работа нескольких пользователей с одним и тем же документом в такой ситуации просто исключается.

Теперь соединим компьютеры в сеть (рис. 1.1) и настроим общий доступ к требуемым ресурсам. Оказывается, что дискеты больше нам не нужны, да и принтер потребуется только один. И выгодно, и удобно!

Ресурсы — программы, файлы данных, а также принтеры и другие совместно используемые периферийные устройства в сети.

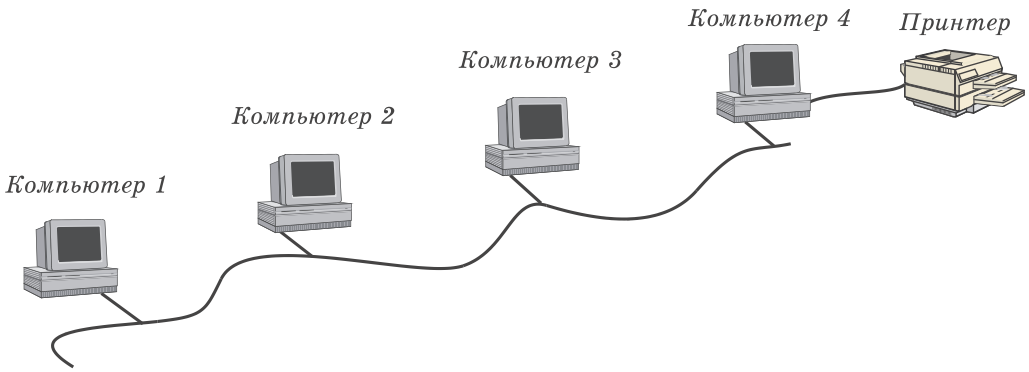


Рис. 1.1. Простейшая сеть: несколько компьютеров и общий принтер

Классификация компьютерных сетей

Возможно множество различных способов классификации компьютерных сетей. Здесь мы рассмотрим только основные из них.

- В зависимости от *расстояния между связываемыми узлами* сети можно разделить на три основных класса: *локальные*, *региональные* и *глобальные* (рис. 1.2).

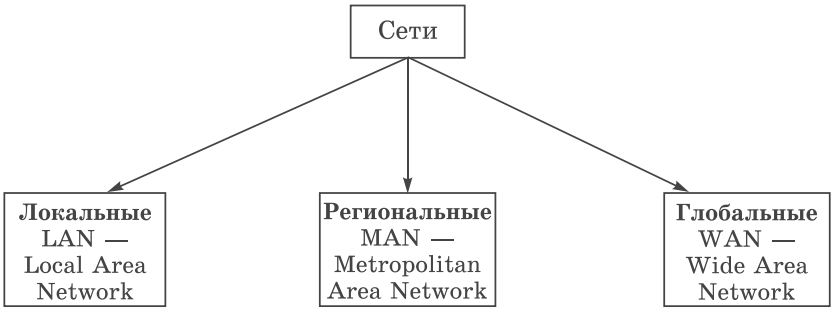


Рис. 1.2. Классификация сетей по расстоянию между узлами

Локальная вычислительная сеть (ЛВС) — небольшая группа компьютеров, связанных друг с другом и расположенных обычно в пределах одного здания или организации.

Региональная сеть — сеть, соединяющая множество локальных сетей в рамках одного района, города или региона.

Глобальная сеть — сеть, объединяющая компьютеры разных городов, регионов и государств.

Объединение глобальных, региональных и локальных вычислительных сетей позволяет создавать многоуровневые иерархии, которые предоставляют мощные средства для обработки огромных массивов данных и доступ к практически неограниченным информационным ресурсам. На рис. 1.3 приведена одна из возможных иерархий вычислительных сетей.

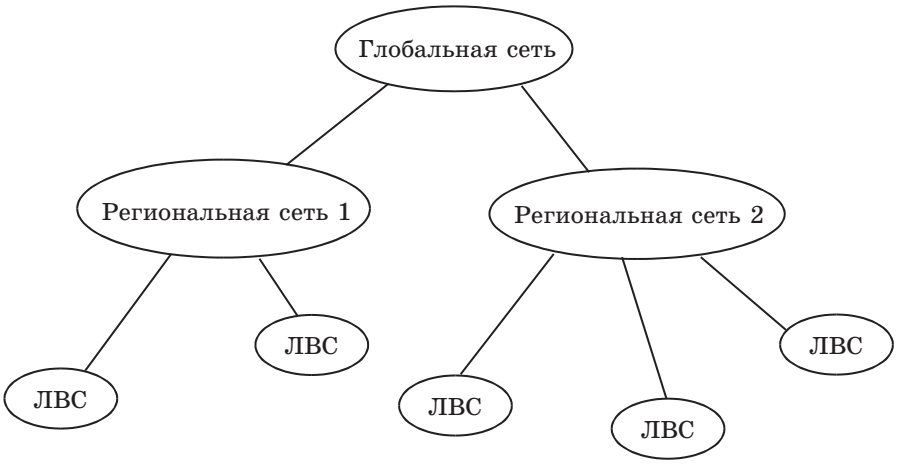


Рис. 1.3. Пример объединения сетей

Локальные вычислительные сети (ЛВС) могут входить в качестве компонентов в состав региональной сети; региональные сети — объединяться в составе глобальной сети; наконец, глобальные сети могут образовывать еще более крупные структуры. Самым большим объединением компьютерных сетей в масштабах планеты Земля на сегодня является «сеть сетей» — *Интернет*.

Интересным примером связи локальных и глобальных сетей является *виртуальная частная сеть* (*Virtual Private Network, VPN*). Так называется сеть организации, получающаяся в результате объединения двух или нескольких территориально разделенных ЛВС с помощью общедоступных каналов глобальных сетей, например, через Интернет (рис. 1.4).

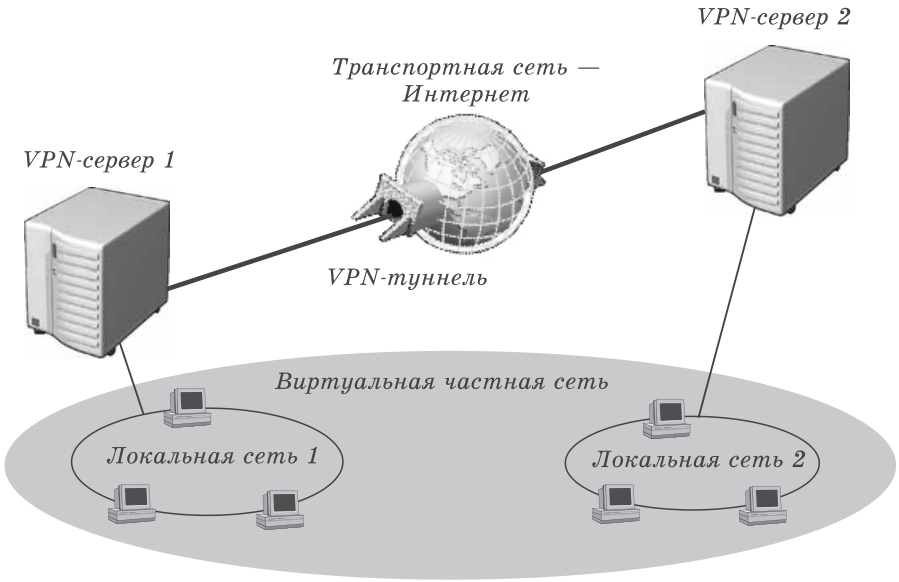


Рис. 1.4. Виртуальная частная сеть — несколько локальных сетей предприятия, объединенных через Интернет

➢ *По типу среды передачи* сети делятся на *проводные* и *беспроводные* (рис. 1.5).

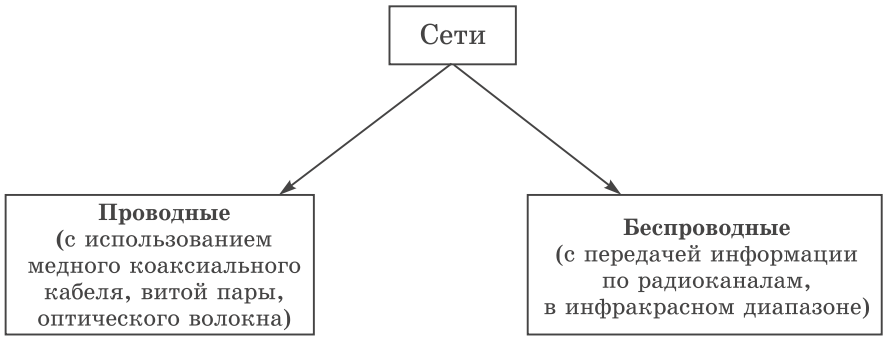


Рис. 1.5. Классификация сетей по типу среды передачи

➢ *По скорости передачи информации* сети можно разделить на *низко-*, *средне-* и *высокоскоростные* (рис. 1.6).

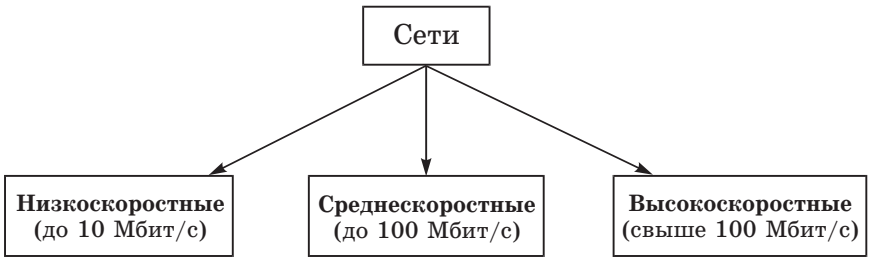


Рис. 1.6. Классификация сетей по скорости передачи информации

➢ С точки зрения *распределения ролей между компьютерами* сети бывают *одноранговые* и *клиент-серверные* (рис. 1.7).

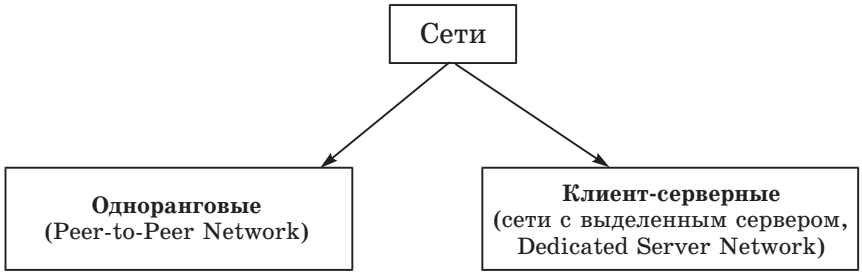


Рис. 1.7. Классификация сетей по распределению ролей между компьютерами

Сервер — специально выделенный высокопроизводительный компьютер, оснащенный соответствующим программным обеспечением, централизованно управляющий работой сети и/или предоставляющий другим компьютерам сети свои ресурсы (файлы данных, накопители, принтер и т. д.).

Клиентский компьютер (**клиент, рабочая станция**) — компьютер рядового пользователя сети, получающий доступ к ресурсам сервера (серверов).

Поскольку понятия одноранговых и клиент-серверных сетей очень важны, рассмотрим их подробнее.

Одноранговые сети

В одноранговой сети (рис. 1.8) все компьютеры равноправны. Каждый из них может выступать как в роли сервера, т. е. предоставлять файлы и аппаратные ресурсы (накопители, принтеры и пр.) другим компьютерам, так и в роли клиента, пользующегося ресурсами других компьютеров. Например, если на вашем компьютере установлен принтер, то с его помощью смогут распечатывать свои документы все остальные пользователи сети, а вы, в свою очередь, сможете работать с Интернетом, подключение к которому осуществляется через соседний компьютер.

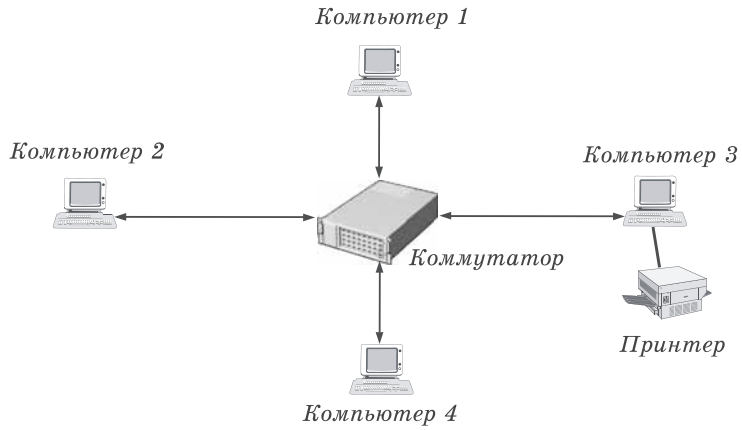


Рис. 1.8. Пример одноранговой сети

Преимущества и недостатки одноранговых сетей

Преимущества	*Недостатки*
☑ легкость в установке и настройке; ☑ независимость отдельных компьютеров и их ресурсов друг от друга; ☑ возможность для пользователя контролировать ресурсы своего собственного компьютера; ☑ сравнительно низкая стоимость развертывания и поддержки; ☑ отсутствие необходимости в дополнительном программном обеспечении (кроме операционной системы); ☑ отсутствие необходимости в постоянном присутствии администратора сети	☒ необходимость помнить столько паролей, сколько имеется разделенных ресурсов (для сетей на основе Windows 95/98), либо имен и паролей для входа (для сетей на основе Windows NT/2000/XP); ☒ необходимость производить резервное копирование отдельно на каждом компьютере, чтобы защитить все совместно используемые данные; ☒ отсутствие возможности централизованного управления сетью и доступом к данным; ☒ как результат — низкая общая защищенность сети и данных

Администратор сети — человек, обладающий всеми полномочиями для управления компьютерами, пользователями и ресурсами в сети.

Администрирование сети — решение целого комплекса задач по управлению работой компьютеров, сетевого оборудования и пользователей, защите данных, обеспечению доступа к ресурсам, установке и модернизации системного и прикладного программного обеспечения.

Число компьютеров в одноранговых сетях обычно не превышает 10, отсюда их другое название — *рабочая группа*. Типичными примерами рабочих групп являются домашние сети или сети небольших офисов.

Сети с выделенным сервером (сети типа «клиент–сервер»)

Как правило, сети создаются в учреждениях или крупных организациях. В таких сетях (рис. 1.9) выделяются один или несколько компьютеров, называемых *серверами*, задача которых состоит в быстрой и эффективной обработке большого числа запросов дру-

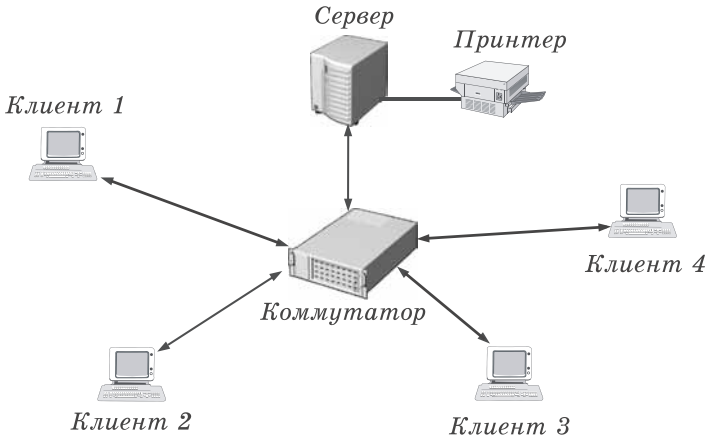


Рис. 1.9. Пример сети с выделенным сервером

гих компьютеров — *клиентов*. При этом *клиентские запросы* бывают самыми разными, начиная с простейшей проверки имени и пароля пользователя при входе в систему и заканчивая сложными поисковыми запросами к базам данных, на обработку которых даже современный многопроцессорный компьютер может потратить несколько часов.

Обычно в роли серверов выступают более мощные и надежные компьютеры, чем пользовательские рабочие станции. Серверы часто оснащают специализированным оборудованием, например емкими хранилищами данных (жесткими дисками и так называемыми «рейд-массивами» на их основе), накопителями на магнитной ленте для резервного копирования, высокоскоростными сетевыми адаптерами и т. д. Такие компьютеры работают постоянно, круглосуточно предоставляя пользователям свои ресурсы и обеспечивая доступ к своим службам.

Службы (services) — работающие на серверах программы, выполняющие какие-либо действия по запросу клиента.

Преимущества и недостатки клиент-серверных сетей

Преимущества	*Недостатки*
☑ использование мощного серверного оборудования обеспечивает быстрый доступ к ресурсам и эффективную обработку запросов клиентов: один сервер может обслуживать тысячи пользователей; ☑ централизация данных и ресурсов позволяет наладить четкое управление информацией и пользовательскими данными; ☑ размещение данных на сервере существенно упрощает процедуры резервного копирования; ☑ повышается общая защищенность сети и сохранность данных	☒ неисправность сервера может сделать всю сеть практически неработоспособной, а ресурсы — недоступными; ☒ сложность развертывания и поддержки требует наличия квалифицированного персонала, что увеличивает общую стоимость сопровождения сети; ☒ стоимость сопровождения сети также увеличивается из-за потребности в выделенном оборудовании и специализированном программном обеспечении; ☒ требуется один (а чаще всего — несколько) постоянно присутствующих на рабочем месте администраторов

Взаимодействие компьютеров в сети

Наконец, кратко рассмотрим, как компьютеры взаимодействуют друг с другом в сети. Чтобы такая работа стала возможной, сначала нужно каким-либо образом соединить между собой всех участников сети — серверы, стационарные рабочие станции пользователей, ноутбуки, карманные компьютеры (КПК), принтеры, сетевые хранилища данных и т. д. Для этих целей применяются *сетевые кабели* различных типов, *телефонные* или *спутниковые каналы*, а в последнее время все более популярными становятся *беспроводные решения* (WLAN, Wi-Fi, WiMAX). При использовании кабелей обычно требуются специальные *коннекторы*, закрепленные на их концах. Затем кабель одним концом вставляется в *сетевой адаптер* — специальную печатную плату («карту расширения»), установленную в компьютер и позволяющую подключить его к сети, а другим — в какое-либо *устройство связи* (концентратор, мост, коммутатор, маршрутизатор, шлюз и т. д.). В большинстве современных компьютеров сетевой адаптер является встроенным (соответствующий разъем имеется непосредственно на материнской плате). Если же используется *беспроводной сетевой адаптер*, то взаимодействие с сетью происходит за счет передачи радиосигналов между адаптером и *точкой доступа*, соединенной с локальной сетью.

Однако соединить компьютеры друг с другом недостаточно — нужно еще и «научить их разговаривать» друг с другом. Для этого требуются *сетевые операционные системы*, поддерживающие один и тот же *набор протоколов*, или языков, с помощью которых компьютеры общаются по сети. И только после этого, запустив *сетевое приложение*, можно будет, например, пообщаться с другом, находящимся на другом конце земного шара.

Подробно обо всем этом вы прочитаете в следующих главах.

Вопросы и задания

1. Что такое компьютерная сеть?
2. Какие типы сетей вы знаете?
3. Какие преимущества дает сеть?
4. Что такое одноранговая сеть? Каковы ее преимущества и недостатки?
5. Что такое сеть «клиент-сервер»? Каковы ее преимущества и недостатки?
6. Что входит в понятие «администрирование сети»?
7. Как компьютеры взаимодействуют друг с другом в сети?

Глава 2

Как компьютеры взаимодействуют в сети

В этой главе вы найдете ответы на следующие вопросы:

- ***Что такое эталонная модель OSI?***
- ***Каковы функции каждого уровня в модели OSI?***
- ***Как определять уровни модели OSI, на которых выполняются конкретные сетевые операции?***
- ***Какие возможны расширения модели OSI со стороны IEEE?***

В предыдущей главе вы узнали, что такое компьютерные сети, познакомились с основными типами сетей и поняли, как компьютеры (точнее, работающие на них программы) общаются друг с другом в сети. Теперь рассмотрим принципы взаимодействия компьютеров в сети более подробно.

Чтобы общаться, люди чаще всего используют устную речь. Однако такое непосредственное общение возможно, только если собеседники находятся рядом друг с другом и только в воздушной среде. Но представьте себе, что надо передать данные вашему товарищу, который живет в другом городе, а тем более — в другой стране. Здесь уже не обойтись без целого ряда определенных действий: нужно написать текст на листе бумаги, подписать его, вложить в конверт, указать на нем адреса отправителя и получателя, наклеить марку и отдать почтальону (или бросить в почтовый ящик). Дальнейшая судьба этого письма зависит уже не от вас, а от почтовой службы. Каким-либо способом — на поезде, корабле, самолете или как-то иначе, но письмо доходит до страны и города, где живет ваш друг, затем доставляется в его почтовое отделение и, наконец, попадает к нему в почтовый ящик. Только тогда ваш адресат получает возможность открыть конверт и прочитать ваше сообщение. Заметим, что если какая-либо из стадий доставки не сработает, например, из-за отсутствия почтальона или различий в

правилах записи адресов в разных странах, то информация до вашего друга так и не дойдет.

Точно так же поступают и компьютеры при общении в сети. Способов непосредственного общения у них нет — разговаривать друг с другом компьютеры пока еще не научились. Поэтому, чтобы общаться, им приходится прибегать к целому ряду последовательно выполняемых процедур, называемых *сетевыми протоколами*. Чтобы протоколы работали надежно и согласованно, каждая операция в них строго регламентируется. А чтобы программы и оборудование разных производителей могли взаимодействовать друг с другом, протоколы должны соответствовать определенным *промышленным стандартам*.

Протокол — набор правил и процедур, регулирующих порядок взаимодействия компьютеров в сети.

За долгие годы существования компьютерных сетей было создано великое множество различных протоколов — как открытых (опубликованных для бесплатного применения), так и закрытых (разработанных коммерческими компаниями и требующих лицензирования для их использования). Однако все эти протоколы принято соотносить с так называемой *эталонной моделью взаимодействия открытых систем* (*Open Systems Interconnection Reference Model*), или просто *моделью OSI*. Ее описание было опубликовано в 1984 г. Международной организацией по стандартизации (International Standards Organization, ISO), поэтому для нее часто используется другое название — *модель ISO/OSI*. Эта модель представляет собой набор спецификаций, описывающих сети с неоднородными устройствами, требования к ним, а также способы их взаимодействия.

Структура модели OSI

Модель OSI имеет вертикальную структуру, в которой все сетевые функции распределены между семью *уровнями* (рис. 2.1). Каждому такому уровню соответствуют строго определенные операции, оборудование и протоколы.

Реальное взаимодействие уровней, т. е. передача информации внутри одного компьютера, возможно *только по вертикали и только с соседними уровнями* (выше- и нижележащими).

Логическое взаимодействие (в соответствии с правилами того или иного протокола) осуществляется *по горизонтали — с аналогичным уровнем другого компьютера* на противоположном конце линии связи. Каждый более высокий уровень пользуется услугами нижележащего уровня, зная, в каком виде и каким способом (т. е. через какой *интерфейс*) нужно передать ему данные.

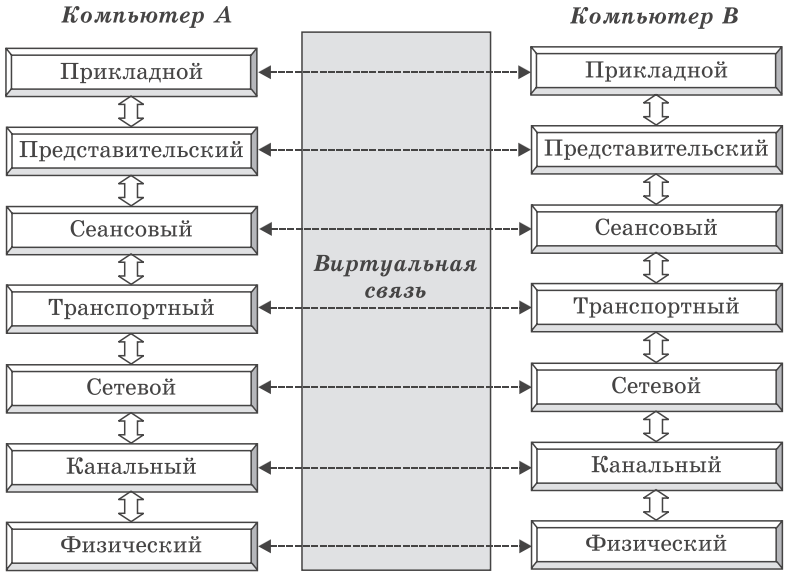


Рис. 2.1. Взаимосвязи между уровнями модели OSI

Задача более низкого уровня — принять данные, добавить свою информацию (например, форматирующую или адресную, которая необходима для правильного взаимодействия с аналогичным уровнем на другом компьютере) и передать данные дальше. Только дойдя до самого нижнего, физического уровня сетевой модели, информация попадает в среду передачи и достигает компьютера-получателя. В нем она проходит сквозь все слои в обратном порядке, пока не достигнет того же уровня, с которого была послана компьютером-отправителем.

Как видим, все это очень похоже на наш пример с работой почты — программы общаются по сети примерно так же, как вы со своим другом по почте. Ваш лист бумаги с текстом передается с верхнего уровня вниз, проходя множество необходимых стадий. При этом он «обрастает» служебной информацией (конверт определенного вида, адрес на конверте, почтовый индекс) и подвергается определенной обработке (почтальон в отделении забирает письмо, на конверт наклеивают марки, ставят штемпели, а после сортировки письмо попадает в контейнер для перевозки почты в другой город). Так ваша информация доходит до самого нижнего уровня — почтового транспорта, которым она перевозится в пункт назначения. Там происходит обратный процесс: открывается контейнер, письмо извлекается, считывается адрес, после чего почтальон доставляет письмо вашему другу. А затем ваш друг получает информацию в первоначальном виде — когда извлекает лист из конверта, проверяет подпись и читает текст.

Таким образом, вы с вашим другом *логически имеете прямую связь*, и детали доставки вас мало заботят. Почтальоны также имеют прямую связь: почтальон в чужом городе получит в точности то, что вы передали своему почтальону — конверт с письмом и адресной информацией. Почтальонов при этом не волнуют проблемы, например, железнодорожников, которые в действительности и осуществляли перевозку почтовой корреспонденции.

Теперь познакомимся поближе с уровнями модели OSI и определим сетевые услуги, которые они предоставляют смежным уровням.

Уровни модели OSI

- **Уровень 0** — не определен в общей схеме (на рис. 2.1), но весьма важен для понимания. Здесь представлены посредники, по которым собственно и происходит передача сигналов: кабели различных типов, радио-, ИК-сигналы и т. д. На этом уровне ничего не описывается, уровень 0 предоставляет физическому уровню 1 только *среду передачи*.

Можно предположить, что контрольная сумма (CRC) как способ контроля правильности передачи данных появилась одновременно с первыми ЭВМ. Но оказывается, что идея «контрольной суммы» была впервые изобретена... церковниками, озабоченными большим количеством расхождений в текстах переписываемых вручную Библий (еще до изобретения книгопечатания): ведь при каждом таком копировании писцы не только повторяли все ошибки своего оригинала, но и добавляли новые. Из этой проблемы был найден следующий выход. На специальном совещании высших духовных чинов был выбран и утвержден некий канонический вариант Библии. В нем были подсчитаны количества слов и букв в каждой главе. Переписчик же, закончив свою работу, должен был подсчитать эти количества в сделанной копии и сравнить с полагающимися для оригинала.

- **Уровень 1 — Физический (Physical).** Здесь осуществляется передача неструктурированного потока битов, полученных от вышележащего канального уровня 2, по физической среде — например, в виде электрических или световых сигналов. Физический уровень отвечает за *поддержание связи* (*link*) и детально описывает электрические, оптические, механические и функциональные интерфейсы со средой передачи: напряжения, частоты, длины волн, типы коннекторов, число и функциональность контактов, схемы кодирования сигналов и т. д.
- **Уровень 2 — Канальный (Data Link).** Обеспечивает *безошибочную передачу данных*, полученных от вышележащего сетевого уровня 3, через физический уровень 1, который сам по себе отсутствия ошибок не гарантирует и может искажать данные. Информация на этом уровне помещается в *кадры* (*frames*), где в начале (*заголовке кадра*) содержатся адреса получателя и отправителя, а также управляющая информация, а в конце — *контрольная сумма*, позволяющая выявить возникающие при передаче ошибки (рис. 2.2).

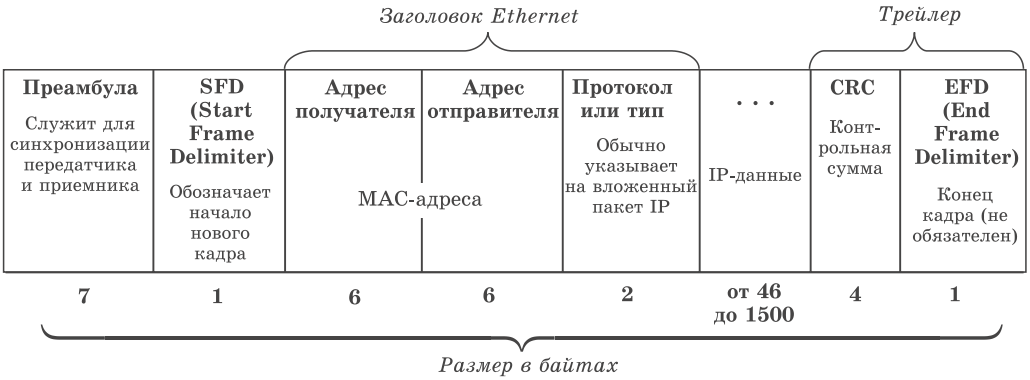


Рис 2.2. Структура кадра

При *получении данных* на канальном уровне определяются начало и конец кадра в потоке битов, сам кадр извлекается из потока и проверяется на наличие ошибок. Поврежденные при передаче кадры, а также кадры, для которых не получено *подтверждение о приеме*, пересылаются заново (*ретранслируются*). Наконец, на канальном уровне обеспечивается управление доступом к среде передачи.

Канальный уровень довольно сложен, поэтому в соответствии со стандартами IEEE (Institute of Electrical and Electronics Engineers), выпущенными в феврале 1980 г. в рамках «Проекта 802» (*Project 802*), его часто разбивают на два подуровня (рис. 2.3): *управления доступом к среде* (*Media Access Control*, *MAC*) и *управления логической связью* (*Logical Link Control*, *LLC*).

Уровень MAC обеспечивает совместный доступ сетевых адаптеров к физическому уровню, определение границ кадров, распознавание *адресов назначения кадров* (эти адреса часто называют *физическими*, или *MAC-адресами*).

Уровень LLC, действующий над уровнем MAC, отвечает за установление канала связи и за безошибочную посылку и прием сообщений с данными.

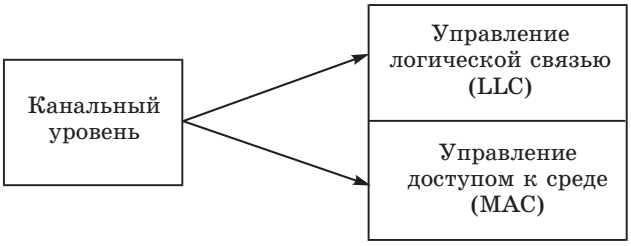


Рис 2.3. Разделение канального уровня на подуровни MAC и LLC

- **Уровень 3 — Сетевой (Network).** Отвечает за *обеспечение связи* между любыми, даже находящимися в разных концах земного шара, точками в сети. Этот уровень осуществляет *проводку сообщений по сети*, которая может состоять из множества отдельных сетей, соединенных множеством линий связи. Такая доставка требует *маршрутизации*, т. е. *определения пути доставки сообщения*, а также решения задач управления потоками данных и обработки ошибок передачи.

- **Уровень 4 — Транспортный (Transport).** Гарантирует *доставку информации* от одного компьютера другому. На этом уровне компьютера-отправителя большие блоки данных разбиваются на более мелкие *пакеты*, которые доставляются компьютеру-получателю *в нужной последовательности*, *без потерь и дублирования*. На транспортном уровне компьютера-получателя пакеты вновь собираются в исходные блоки данных. Таким образом, транспортный уровень *завершает процесс передачи данных*, скрывая от более высоких уровней все детали и проблемы, связанные с доставкой информации *любого объема* между *любыми точками* во всей сети.

- **Уровень 5 — Сеансовый (Session).** Позволяет двум *сетевым приложениям* на разных компьютерах устанавливать, поддерживать и завершать соединение,

называемое *сетевым сеансом*. Этот уровень также отвечает за восстановление аварийно прерванных сеансов связи. Кроме того, на пятом уровне выполняется преобразование удобных для людей имен компьютеров в сетевые адреса (*распознавание имен*), а также реализуются функции *защиты сеанса*.

- **Уровень 6 — Представительский, или Уровень представления данных (Presentation).** Определяет *форматы* передаваемой между компьютерами информации. Здесь решаются такие задачи, как *перекодировка* (перевод информации в вид, понятный для всех участвующих в обмене компьютеров), сжатие и распаковка данных, шифрование и дешифровка, поддержка сетевых файловых систем и т. д.

- **Уровень 7 — Прикладной (Application), или Уровень Приложений.** Обеспечивает интерфейс взаимодействия программ, работающих на компьютерах в сети. Именно с помощью этих программ пользователь получает доступ к таким сетевым услугам, как обмен файлами, передача электронной почты, удаленный терминальный доступ и т. д.

К моменту появления модели OSI уже существовали и показали высокую эффективность другие *наборы* (*стеки*) *протоколов*, например *стек TCP/IP*. Поэтому построенный в полном соответствии с описанной выше моделью *набор протоколов OSI* так и не получил широкого распространения. Большинство современных сетевых архитектур и наборов протоколов соответствуют этой модели лишь до определенной степени. Несмотря на это, сама модель ISO/OSI до сих пор широко используется для описания взаимодействия в сетевых средах.

Вопросы и задания

1. Что понимается под термином «сетевой протокол»?
2. Какие сетевые функции осуществляются в модели OSI?
3. Какой уровень, согласно модели OSI, отвечает за выбор маршрута передачи данных?
4. На каком уровне модели OSI взаимодействуют программы, обеспечивающие передачу сообщений электронной почты?

Глава 3

Сетевые топологии и способы доступа к среде передачи данных

В этой главе вы найдете ответы на следующие вопросы:

- ***Какие существуют сетевые топологии?***
- ***Каковы преимущества и недостатки различных топологий?***
- ***Какой тип сети сейчас наиболее популярен?***
- ***Какие возможны способы (методы) доступа к среде передачи данных?***

При организации компьютерной сети исключительно важным является выбор *топологии*, т. е. *компоновки сетевых устройств и кабельной инфраструктуры*. Нужно выбрать такую топологию, которая обеспечила бы надежную и эффективную работу сети, удобное управление потоками сетевых данных. Желательно также, чтобы сеть по стоимости создания и сопровождения получилась недорогой, но в то же время оставались возможности для ее дальнейшего расширения и, желательно, для перехода к более высокоскоростным технологиям связи.

Это непростая задача! Чтобы ее решить, необходимо знать, какие вообще бывают сетевые топологии. Заметим, что при этом следует различать понятия *физической топологии*, т. е. способа размещения компьютеров, сетевого оборудования и их соединения с помощью кабельной инфраструктуры, и *логической топологии* — структуры взаимодействия компьютеров и характера распространения сигналов по сети.

Базовые сетевые топологии

Существует три базовые топологии, на основе которых строится большинство сетей.

- **«Шина» (Bus).** В этой топологии все компьютеры соединяются друг с другом *одним кабелем* (рис. 3.1). Посланные в такую сеть данные передаются *всем компьютерам*, но обрабатывает их только тот компьютер, аппаратный MAC-адрес сетевого адаптера которого записан в кадре как адрес получателя.

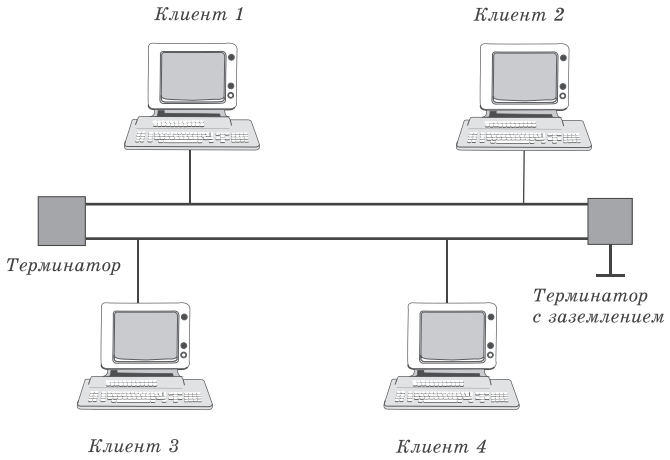


Рис 3.1. Сеть с топологией «шина»

Эта топология исключительно проста в реализации и дешева (требует меньше всего кабеля), однако имеет ряд существенных недостатков.

Недостатки сетей типа «шина»

- Такие сети трудно *расширять* (увеличивать число компьютеров в сети и количество *сегментов* — отдельных отрезков кабеля, их соединяющих).
- Поскольку шина используется совместно, в каждый момент времени передачу может вести *только один из компьютеров*. Если передачу одновременно начинают два или больше компьютеров, возникает искажение сигнала (*столкновение*, или *коллизия*), приводящее

к повреждению всех кадров. Тогда компьютеры вынуждены приостанавливать передачу, а затем по очереди ретранслировать данные. Влияние столкновений тем заметнее, чем выше объем передаваемой по сети информации и чем больше компьютеров подключено к шине. Оба этих фактора, естественно, снижают как максимально возможную, так и общую производительность сети, замедляя ее работу.

- «Шина» является *пассивной топологией* — компьютеры только «слушают» кабель и не могут восстанавливать затухающие при передаче по сети сигналы. Чтобы удлинить сеть, нужно использовать *повторители* (*репитеры*), усиливающие сигнал перед его передачей в следующий сегмент.
- Надежность сети с топологией «шина» невысока. Когда электрический сигнал достигает конца кабеля, он (если не приняты специальные меры) *отражается*, нарушая работу всего сегмента сети. Чтобы предотвратить такое отражение сигналов, на концах кабеля устанавливаются специальные *резисторы* (*терминаторы*), поглощающие сигналы. Если же в любом месте кабеля возникает обрыв — например, при нарушении целостности кабеля или просто при отсоединении коннектора, — то возникают два незатерминированных сегмента, на концах которых сигналы начинают отражаться, и вся сеть перестает работать.

Проблемы, характерные для топологии «шина», привели к тому, что эти сети, столь популярные еще десять лет назад, сейчас уже практически не используются.

- **«Кольцо» (Ring).** В данной топологии каждый из компьютеров соединяется с двумя другими так, чтобы от одного он получал информацию, а второму — передавал ее (рис. 3.2). Последний компьютер подключается к первому, и кольцо *замыкается*.

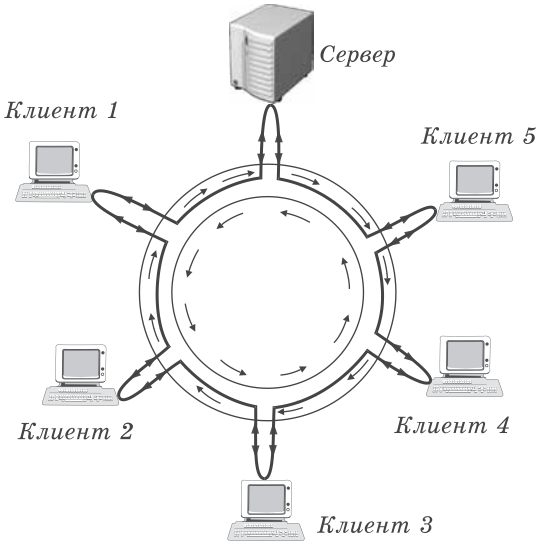


Рис. 3.2. Сеть с топологией «кольцо»

Преимущества и недостатки сетей с топологией «кольцо»

Преимущества	*Недостатки*
☑ поскольку у кабелей в этой сети нет свободных концов, терминаторы здесь не нужны; ☑ каждый из компьютеров выступает в роли *повторителя*, усиливая сигнал, что позволяет строить сети большой протяженности; ☑ из-за отсутствия *столкновений* топология обладает высокой устойчивостью к перегрузкам, обеспечивая эффективную работу	☒ сигнал в «кольце» должен пройти последовательно (и только в одном направлении) через все компьютеры, каждый из которых проверяет, не ему ли адресована информация, поэтому время передачи может быть достаточно большим; ☒ подключение к сети нового компьютера часто требует ее остановки, что нарушает работу всех других компьютеров; ☒ выход из строя хотя бы одного из компьютеров или устройств нарушает работу всей сети;

Преимущества	*Недостатки*
с большими потоками передаваемой по сети информации	☒ обрыв или короткое замыкание в любом из кабелей кольца делает работу всей сети невозможной; ☒ чтобы избежать остановки работы сети при отказе компьютеров или обрыве кабеля, обычно прокладывают два кольца, что существенно удорожает сеть

Здесь, так же как и для сетей с топологией «шина», недостатки несколько перевешивают достоинства, в результате чего популярные ранее кольцевые сети теперь используются гораздо реже.

- **Активная топология «звезда» (Active Star).** Эта топология возникла на заре вычислительной техники, когда к мощному центральному компьютеру подключались все остальные абоненты сети. В такой конфигурации все потоки данных шли исключительно через центральный компьютер; он же полностью отвечал за управление информационным обменом между всеми участниками сети. Конфликты при такой организации взаимодействия в сети были невозможны, однако нагрузка на центральный компьютер была столь велика, что ничем другим, кроме обслуживания сети, этот компьютер, как правило, не занимался. Выход его из строя приводил к отказу всей сети, тогда как отказ периферийного компьютера или обрыв связи с ним на работе остальной сети не сказывался. Сейчас такие сети встречаются довольно редко.

  Гораздо более распространенной сегодня топологией является похожий вариант — **«звезда-шина» (Star Bus)**, или **«пассивная звезда»** (рис. 3.3). Здесь периферийные компьютеры подключаются не к центральному компьютеру, а к пассивному *концентра-*

тору, или *хабу* (*hub*). Последний, в отличие от центрального компьютера, никак не отвечает за управление обменом данными, а выполняет те же функции, что и повторитель, то есть восстанавливает приходящие сигналы и пересылает их всем остальным подключенным к нему компьютерам и устройствам. Именно поэтому данная топология, хотя физически и выглядит как «звезда», логически является топологией «шина» (что и отражено в ее названии).

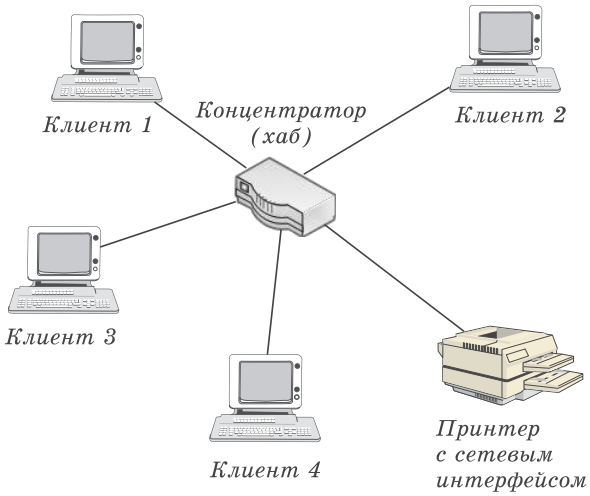


Рис. 3.3. Сеть с топологией «звезда-шина»

Несмотря на больший расход кабеля, характерный для сетей типа «звезда», эта топология имеет существенные преимущества перед остальными, что и обусловило ее широчайшее применение в современных сетях.

Преимущества сетей типа «звезда-шина»

- ☑ *Надежность* — подключение к центральному концентратору и отключение компьютеров от него никак не отражается на работе остальной сети; обрывы кабеля влияют только на еди-

ничные компьютеры; терминаторы не требуются.

- ☑ *Легкость при обслуживании и устранении проблем* — все компьютеры и сетевые устройства подключаются к центральному соединительному устройству, что существенно упрощает обслуживание и ремонт сети.
- ☑ *Защищенность* — концентрация точек подключения в одном месте позволяет легко ограничить доступ к жизненно важным объектам сети.

Отметим, что при использовании вместо концентраторов более «интеллектуальных» сетевых устройств (*мостов*, *коммутаторов* и *маршрутизаторов* — подробнее о них будет рассказано позже) получается «промежуточный» тип топологии между активной и пассивной звездой. В этом случае устройство связи не только ретранслирует поступающие сигналы, но и производит управление их обменом.

Другие возможные сетевые топологии

Реальные компьютерные сети постоянно расширяются и модернизируются. Поэтому почти всегда такая сеть является *гибридной*, т. е. ее топология представляет собой комбинацию нескольких базовых топологий. Легко представить себе гибридные топологии, являющиеся комбинацией «звезды» и «шины», либо «кольца» и «звезды».

Однако особо следует выделить **топологию «дерево» (tree)**, которую можно рассматривать как объединение нескольких «звезд» (рис. 3.4). Именно эта топология сегодня является наиболее популярной при построении локальных сетей.

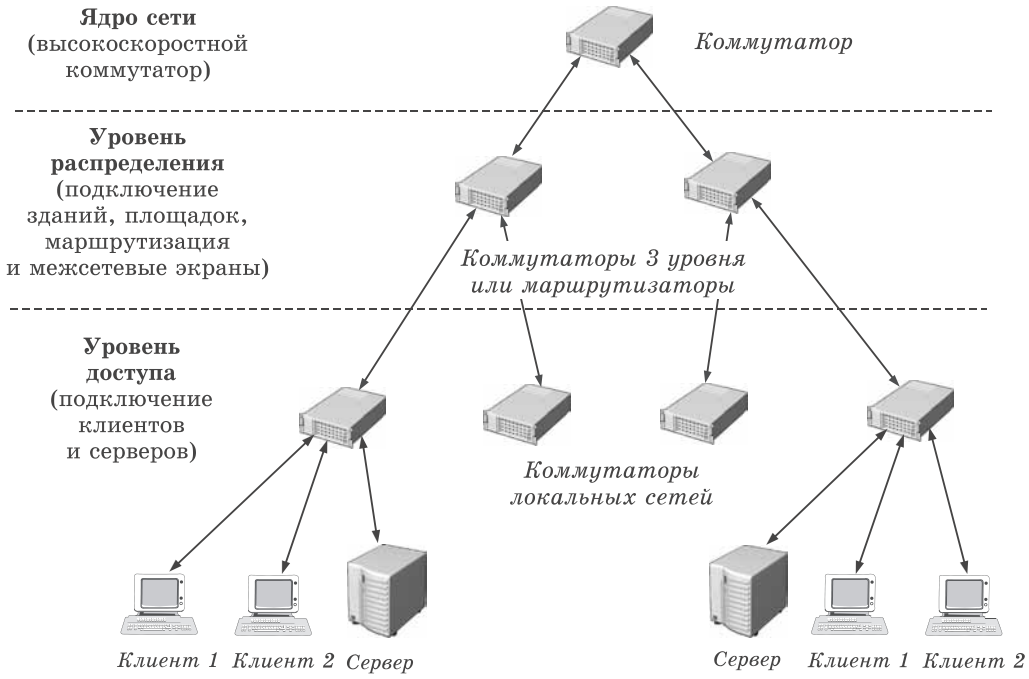


Рис. 3.4. Сеть с топологией «дерево»

Своего рода «предтечей» Интернета была сеть ARPANet, изначально созданная по заказу Министерства обороны США. Целью этого проекта была разработка такой системы связи, которая могла бы функционировать даже в условиях атомной войны. Нынешний же Интернет как свободно доступная всемирная компьютерная сеть стал отчасти неожиданным, «конверсионным» результатом военных разработок.

Наконец, следует упомянуть о **сетчатой**, или **сеточной (mesh) топологии**, в которой все либо многие компьютеры и другие устройства соединены друг с другом напрямую (рис. 3.5). Такая топология исключительно надежна — при обрыве любого канала передача данных не прекращается, поскольку возможно *несколько маршрутов доставки информации*. Сеточные топологии (чаще всего не полные, а частичные) используются там, где требуется обеспечить *максимальную отказоустойчивость* сети, например при объединении нескольких участков сети крупного предприятия или при подключении к Интернету, хотя за это, конечно, приходится платить: существенно увеличивается расход кабеля, усложняется сетевое оборудование и его настройка.

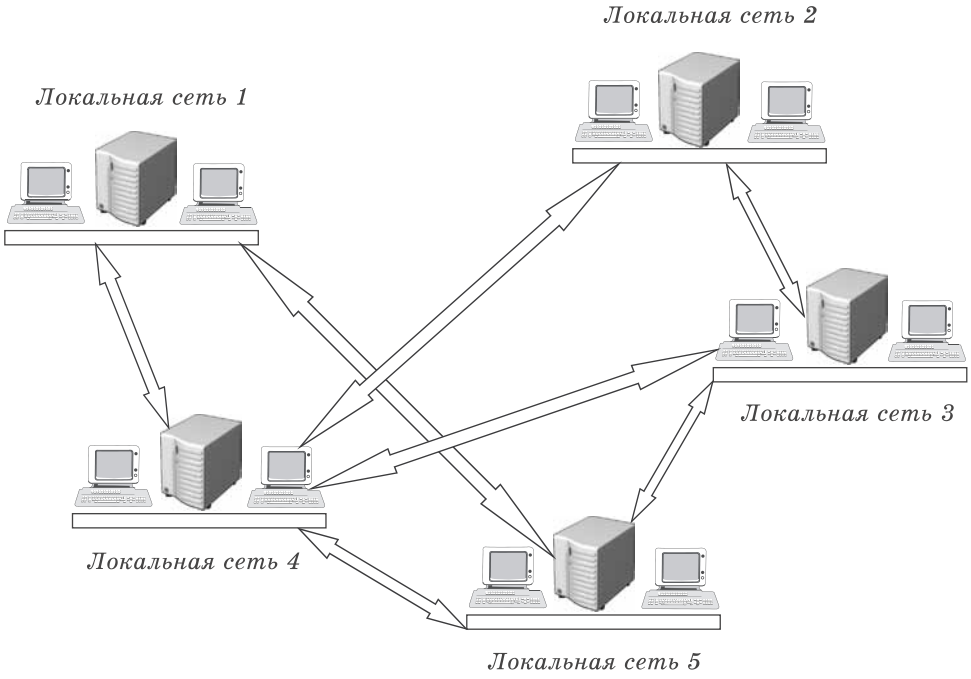


Рис. 3.5. Сеть с сетчатой топологией

Доступ к среде передачи

С сетевой топологией тесно связано понятие *способа доступа к среде передачи*, под которым понимается набор правил, определяющих, как именно компьютеры должны отправлять и принимать данные по сети.

Таких способов возможно несколько. Основными из них являются:

- множественный доступ с контролем несущей и обнаружением столкновений;
- множественный доступ с контролем несущей и предотвращением столкновений;
- передача маркера.

- При **множественном доступе с контролем несущей и обнаружением столкновений** (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) все компьютеры (*множественный доступ*) «слушают» кабель (*контроль несущей*), чтобы определить, передаются по нему данные или нет. Если кабель свободен, любой компьютер может начать передачу; тогда все остальные компьютеры должны ждать, пока кабель не освободится. Если компьютеры начали передачу одновременно и возникло столкновение, все они приостанавливают передачу (*обнаружение столкновений*), каждый — на разные промежутки времени, после чего ретранслируют данные.

  Серьезным недостатком этого способа доступа является то, что при большом количестве компьютеров и высокой нагрузке на сеть число столкновений возрастает, а пропускная способность падает, иногда очень существенно.

  Однако этот метод очень прост в технической реализации, поэтому именно он используется в наиболее популярной сегодня *технологии Ethernet*. А чтобы уменьшить количество столкновений, в современных сетях применяются такие устройства, как мосты, коммутаторы и маршрутизаторы.

- Метод **множественного доступа с контролем несущей и предотвращением столкновений** (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) отличается от предыдущего тем, что перед передачей данных компьютер посылает в сеть специальный небольшой пакет, сообщая остальным компьютерам о своем намерении начать трансляцию. Так другие компьютеры «узнают» о готовящейся передаче, что позволяет избежать столкновений. Конечно, эти уведомления увеличивают общую нагрузку на сеть и снижают ее пропускную способность (из-за чего метод CSMA/CA работает медленнее, чем CSMA/CD), однако они, безусловно, необходимы для работы, например, беспроводных сетей.

- В сетях **с передачей маркера** (Token Passing) от одного компьютера к другому по кольцу постоянно курсирует небольшой блок данных, называемый *маркером*. Если у компьютера, получившего маркер, нет информации для передачи, он просто пересылает его следующему компьютеру. Если же такая информация имеется, компьютер *«захватывает» маркер*, дополняет его данными и отсылает все это следующему компьютеру по кругу. Такой информационный пакет передается от компьютера к компьютеру, пока не достигает станции назначения. Поскольку в момент передачи данных маркер в сети отсутствует, другие компьютеры уже не могут ничего передавать. Поэтому в сетях с передачей маркера невозможны ни столкновения, ни временные задержки, что делает их весьма привлекательными для использования в системах автоматизации работы предприятий.

Выбор компьютерной сети

Рассмотрев наиболее часто используемые сегодня сетевые топологии и методы доступа, обсудим и другие факторы, определяющие выбор нужного типа сети.

При этом следует учитывать:

- уже имеющуюся кабельную систему и оборудование — есть ли в вашем доме, школе, офисе сеть, которую нужно просто расширить, или у вас имеются только отдельные компьютеры;
- физическое месторасположение — важно учитывать, как расположены компьютеры и где вы собираетесь разместить сетевое оборудование. Объединить компьютеры в одной комнате довольно просто, однако если ваши компьютеры располагаются на разных этажах здания или даже в нескольких зданиях, наилучшую конфигурацию сети и ее топологию следует тщательно продумать;

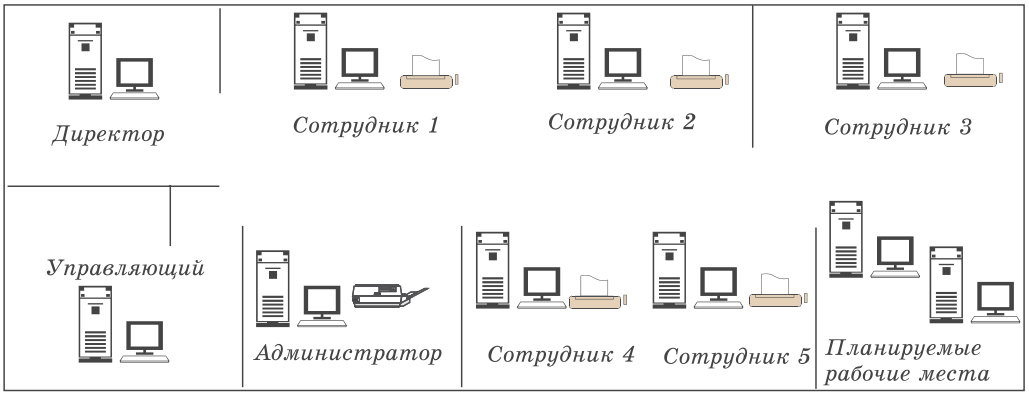
- размеры планируемой сети — если у вас имеется лишь несколько компьютеров, структура сети будет довольно простой; если же компьютеров сотни или тысячи, то, скорее всего, придется остановить свой выбор на сложной гибридной топологии;
- объем и тип информации для совместного использования — эти параметры должны обязательно учитываться при выборе типа сети: если между компьютерами передаются большие файлы — музыкальные, видео- или графические, то вам потребуется высокоскоростная сеть, позволяющая быстро и без задержек передавать такие объемы информации.

Подавляющее большинство современных сетей используют топологию «звезда» или гибридную топологию, представляющую собой объединение нескольких «звезд» (например, топологию типа «дерево»), и метод доступа к среде передачи CSMA/CD (множественный доступ с контролем несущей и обнаружением столкновений).

Вопросы и задания

1. В чем заключается различие между физическими и логическими связями?
2. Какие топологии лежат в основе любой компоновки сети?
3. Каковы преимущества и недостатки конфигурации «звезда»? В каких локальных сетях она применяется?
4. Каковы преимущества и недостатки топологии «кольцо»? В каких локальных сетях она применяется?
5. Каковы преимущества и недостатки конфигурации «шина»? В каких локальных сетях она применяется?

6. Какие гибридные топологии вам известны?
7. Какие факторы необходимо учитывать при планировании сети?
8. Вам поручено установить сеть для небольшой, но развивающейся компании, занимающей половину этажа. В состав компании входят директор, управляющий, администратор и пять сотрудников. Планируется взять на работу еще двух сотрудников. У каждого сотрудника компании есть компьютер. Если необходимо обменяться деловой информацией, приходится делать это устно или с помощью дискет. Лазерный принтер находится у администратора. У каждого сотрудника имеется отдельный матричный принтер.



Какую топологию сети вы предложили бы для этой компании? Оцените суммарную длину кабеля, требуемого для прокладки сети, в каждом из предложенных вариантов и выберите из них наиболее оптимальный.

9. Вам необходимо установить сеть на трех этажах школы. В каждом учебном помещении имеется компьютер и принтер. На первом и втором этаже — 8 помещений. На третьем — 10. Какую топологию сети можно выбрать для этого случая?

Глава 4 Строим сеть: линии связи

В этой главе вы найдете ответы на следующие вопросы:

- ***Какие виды среды передачи сигналов могут использоваться в компьютерных сетях?***
- ***Какие возможны типы и категории кабельных соединений?***
- ***Как выполняются кабельные соединения?***
- ***Какие существуют типы разъемов (коннекторов)?***
- ***Какие возможны типы беспроводных сетей?***

Чтобы компьютеры могли взаимодействовать, необходима какая-либо среда, обеспечивающая возможность передачи сигналов на физическом уровне. Эта *среда передачи* может представлять собой *кабельную инфраструктуру*, т. е. набор проводов различных типов, соединительных *разъемов* (*коннекторов*) и *устройств связи*. Но она может быть и просто атмосферой или даже безвоздушным пространством, — лишь бы имелась возможность каким-то образом *передать сигнал* от одного компьютера к другому.

Кабельные соединения

Наиболее часто в компьютерных сетях применяются кабельные соединения, выступающие в качестве среды передачи электрических или оптических сигналов между компьютерами и другими сетевыми устройствами. При этом используются следующие типы кабеля:

- коаксиальный кабель (coaxial cable);
- витая пара (twisted pair):
  - неэкранированная (unshielded, UTP),
  - экранированная (shielded);
- волоконно-оптический, или оптоволоконный кабель (fiber optic).

➢ Еще десять–пятнадцать лет назад при создании сетей в основном применялся именно *коаксиальный кабель*, состоящий из передающей сигнал медной или алюминиевой жилы, слоя изоляции, экранирующей оплетки из медных проводов или алюминиевой фольги и защитной внешней оболочки (рис. 4.1). Для передачи сигнала в коаксиальном кабеле использовалась центральная жила, тогда как оплетка заземлялась, выступая в роли «электрического нуля».

Рис. 4.1. Коаксиальный кабель

При этом использовались два возможных типа кабеля — «тонкий» и «толстый».

Тонкий коаксиальный кабель — гибкий, диаметром около 0,5 см, позволял передавать данные без затухания на расстояния до 185 м (в реальных сетях — даже до 300 м).

Для подключения кабеля к сетевым устройствам применялись специальные *разъемы типа BNC*.

На концах отрезков кабеля монтировались простые BNC-коннекторы. Сращивание этих отрезков производили с помощью BNC I-коннекторов (или «баррел-коннекторов»), а для соединения с сетевыми адаптерами и устройствами использовались BNC T-коннекторы.

Аббревиатуру «BNC» расшифровывают разными способами: чаще всего — как «Bayonet Neill-Concelman» — от фамилий изобретателей этого разъема, реже — как «Bayonet Navy Connector», «British Naval Connector» или «Bayonet Nut Connector».

Чтобы отраженный сигнал поглощался на концах кабеля, там устанавливали BNC-терминаторы, один из которых обязательно заземлялся (рис. 4.2).

Рис. 4.2. BNC-коннекторы различных типов

Толстый коаксиальный кабель — относительно жесткий, диаметром чуть больше 1 см. В нем медная жила была толще, чем у тонкого коаксиального кабеля и, следовательно, ее электрическое сопротивление было меньшим. Поэтому толстый коаксиальный кабель позволял передавать сигнал на расстояния до 500 м.

«Зуб вампира» обеспечивал быстрый способ подключения трансивера к коаксиальному кабелю: он должен был проколоть оплетку кабеля и изоляцию, обеспечивая контакт трансивера с центральной жилой. Два других, меньших «зуба» обеспечивали контакт с оплеткой кабеля.

Для подключения к толстому коаксиальному кабелю применялись специальные устройства — *трансиверы* (от «transmitter-receiver» — «приемопередатчик») с довольно оригинальным названием «сетевой вампир». В качестве разъемов использовались AUI- или DIX-коннекторы (рис. 4.3).

Широкое распространение сетей, построенных на основе коаксиального кабеля, было вызвано двумя обстоятельствами: дешевизной (особенно для сетей на тонком коаксиальном кабеле) — расходы на

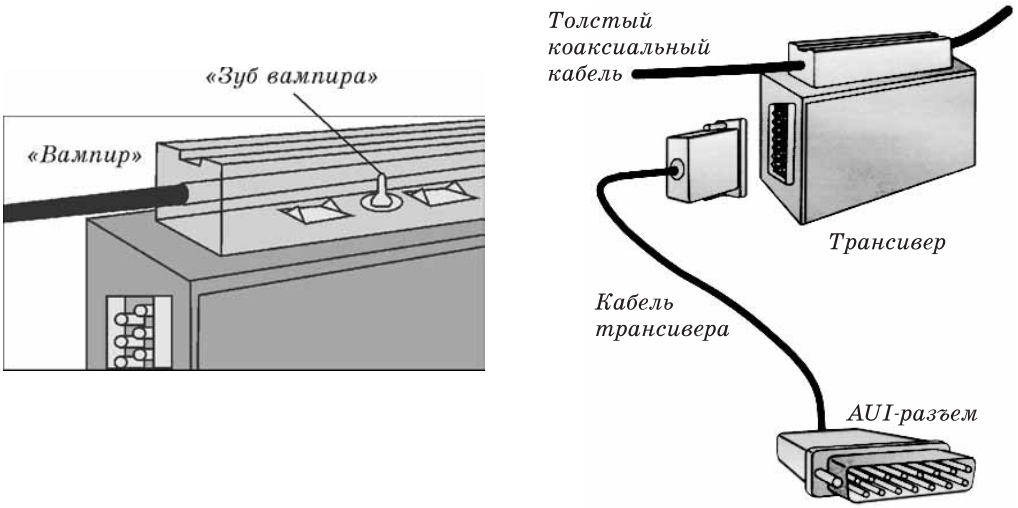


Рис. 4.3. Подключение через трансивер «сетевой вампир»

кабель и коннекторы были минимальными, а больше для небольших сетей ничего и не требовалось, и простотой — достаточно было проложить магистральный кабель, установить на его концах терминаторы и подключить к нему все компьютеры, — и сеть готова (рис. 4.4).

Тем не менее сейчас коаксиальный кабель в большинстве сетей заменен витой парой или оптическими кабелями.

- *Витая пара* — два скрученных друг с другом изолированных медных провода. Подавляющее большинство кабелей на основе витой пары состоит из четырех пар, перевитых с разным шагом для уменьшения электрических наводок со стороны соседних пар и внешних источников и покрытых пластиковой оболочкой (рис. 4.5). В *экранированной витой паре*, кроме того, используется одна или несколько оплеток из алюминиевой или медной фольги, существенно повышающих помехозащищенность кабеля.

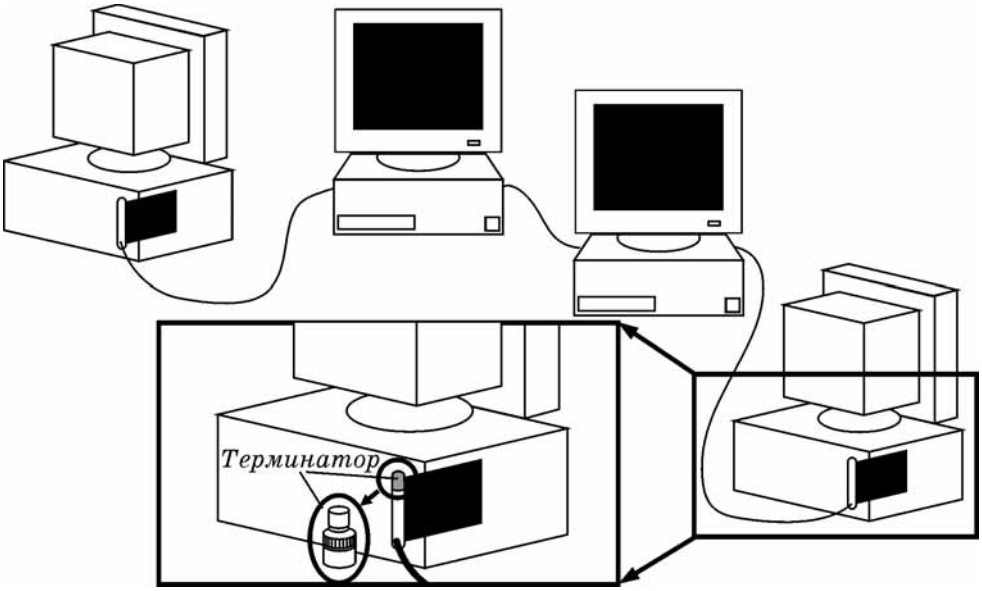


Рис. 4.4. Пример сети на тонком коаксиальном кабеле

Такие кабели выпускаются в соответствии со стандартом EIA/TIA 568 («Американский стандарт проводки в коммерческих зданиях») и подразделяются на *категории*. Кабели разной категории различаются, в первую очередь, шагом скрутки витых пар. Чем меньше шаг, тем выше категория и тем больших скоростей передачи данных можно достичь при его использовании (табл. 4.1).

Рис. 4.5. Витая пара

Таблица 4.1

Категории кабеля «витая пара»

Категория	Характеристика
1	Телефонный кабель для передачи голоса или данных с помощью аналоговых модемов
2	Старый 2-парный тип кабеля. Поддерживает передачу данных со скоростью до 4 Мбит/с. Использовался в сетях Token Ring и ARCNet (о сетевых технологиях — чуть ниже). Сегодня иногда применяется в телефонных сетях
3	2-парный кабель. Использовался в сетях Token Ring и 10BASE-T. Поддерживает передачу данных со скоростью только до 10 Мбит/с. Применяется в телефонных сетях
4	4-парный кабель. Использовался в сетях Token Ring, 10BASE-T, 10BASE-T4 для скоростей до 16 Мбит/с. Сегодня практически не используется
5	Именно этот 4-парный кабель обычно подразумевается под названием «витая пара». Способен передавать данные со скоростью до 100 Мбит/с при использовании двух пар (Fast Ethernet) и до 1000 Мбит/с — при использовании всех четырех пар (Gigabit Ethernet). Наиболее распространен в современных локальных сетях, хотя при прокладке новых сетей чаще применяется кабель *категории 5e*, лучше пропускающий высокочастотные сигналы. Выпускается также в экранированном варианте
6	4-парный кабель (экранированный или неэкранированный). Способен передавать данные со скоростью до 10000 Мбит/с (10 Gigabit Ethernet) на частотах до 200 МГц. В кабелях *категории 6e* предельная частота передачи увеличена до 500 МГц. Более половины современных сетей строится с использованием кабеля этой категории
7	4-парный кабель, спецификация для которого еще окончательно не утверждена. Скорость передачи данных — до 10000 Мбит/с, частота пропускания — до 600–700 МГц. Все отдельные пары и сам кабель для этой категории экранированы

Благодаря своей дешевизне, легкости в установке и универсальности (может использоваться в большинстве сетевых технологий), неэкранированная витая пара сейчас является самым распространенным типом кабеля, используемым при построении локальных сетей. Экранированная витая пара, несмотря на большую помехозащищенность, не получила широкого распространения из-за сложностей в установке — требуется заботиться о заземлении, да и кабель по сравнению с неэкранированной витой парой более жесткий.

Витая пара подключается к компьютерам и другим устройствам с помощью *восьмиконтактного разъема RJ-45* (Registered Jack 45). Этот коннектор (рис. 4.6) похож на применяемый в телефонных линиях коннектор RJ-11, только немного больше него. В табл. 4.2 приведено описание способов заделки кабеля «витая пара» в коннектор RJ-45 в соответствии со стандартами EIA/TIA 568A и 568B; эта операция выполняется с помощью специального обжимного инструмента. (Если расположить разъем контактами вверх и от себя, то нумеровать их надо слева направо, от 1 до 8.)

Рис. 4.6. Разъем RJ-45

Таблица 4.2

Разводка проводников в коннекторах RJ-45

Контакт	Цвет оплетки провода	
	568A	568B
1	бело-зеленый	бело-оранжевый
2	зеленый	оранжевый
3	бело-оранжевый	бело-зеленый
4	голубой	голубой
5	бело-голубой	бело-голубой
6	оранжевый	зеленый
7	бело-коричневый	бело-коричневый
8	коричневый	коричневый

Заметим, что кабели, применяемые для подключения компьютеров к концентраторам и коммутаторам, обжимаются с двух сторон одинаково, то есть по одному и тому же стандарту. При этом получается так называемый *прямой кабель*. Однако для непосредственного соединения сетевых адаптеров компьютеров либо для связи между концентраторами и коммутаторами используется *перекрестный кабель* (*«кросс-кабель»*). С одной стороны такого кабеля витые пары при их заделке в разъем меняют местами: зеленый провод — на место оранжевого, а голубой — на место коричневого, и наоборот.

- *Оптоволоконный кабель* (рис. 4.7) отличается от других видов сетевой проводки тем, что передает световые, а не электрические импульсы. Он очень похож на коаксиальный, но вместо медной или алюминиевой жилы используется стекловолокно.

  При этом могут применяться два вида оптоволоконных кабелей: *многомодовый* (multi-mode) или *одномодовый* (single-mode).

  В относительно дешевом многомодовом кабеле центральное стекловолокно имеет диаметр 50 или 62,5 мкм, а оболочка — 125 мкм. Для передачи сигналов по многомодовому кабелю применяют недорогие *светодиодные трансиверы* с длиной волны 850 нм.

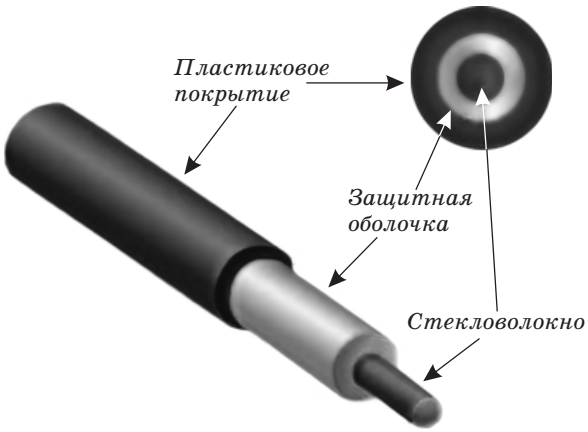


Рис. 4.7. Оптоволоконный кабель

В высококачественном (но дорогом) одномодовом кабеле волокно тоньше — диаметром 9–10 мкм, а затухание светового сигнала в нем существенно меньше. Кроме того, для передачи сигналов по одномодовому кабелю используются *лазерные трансиверы* с длиной волны 1300 нм. В результате максимальное расстояние передачи светового сигнала при применении одномодовых кабелей и трансиверов гораздо больше, чем для многомодовых.

Для подключения оптоволоконного кабеля используются специальные коннекторы (рис. 4.8). *Коннекторы FC* и *ST* сегодня считаются устаревшими, поэтому в новом оборудовании чаще всего применяются разъемы для *коннекторов SC*. Монтаж

FC-коннектор *ST-коннектор* *SC-коннектор*

Рис. 4.8. Оптоволоконные коннекторы различных типов

коннекторов (заделка оптоволоконного кабеля в коннектор) довольно сложен и требует специального оборудования. Правда, в последнее время появились наборы, позволяющие заделывать такие коннекторы и в домашних условиях. Однако их использование требует точности и терпения, поскольку производится путем вклейки оптического волокна в наконечник с последующей сушкой и тонкой шлифовкой.

По сравнению с электрическими кабелями оптоволокно обеспечивает непревзойденные параметры помехозащищенности и защиты передаваемого сигнала от перехвата. Кроме того, при его использовании данные удается передавать на существенно большие расстояния, да и теоретически возможные скорости передачи в оптоволокне намного выше. Недостатки оптоволокна — большая стоимость кабеля, сложность заделки коннекторов (при которой требуется сварка стекловолокна) и необходимость применения дополнительных трансиверов, преобразующих световые сигналы в электрические и обратно. Все это заметно повышает общую стоимость развертывания сети, поэтому до сих пор оптоволокно в локальных сетях применяется реже, чем витая пара.

После выбора подходящего типа кабеля, которым вы собираетесь соединить компьютеры и сетевые устройства, и определения места коммутации и распределения можно приступать к *прокладке кабеля*. При прокладывании кабеля в здании проводку обычно заделывают в стены либо размещают в специальных пространствах под фальшполом или за навесным потолком, а затем выводят в *настенные сетевые розетки*.

Если проложить кабели в указанных местах невозможно, используются настенные (реже — напольные) *кабель-каналы* (*коробы*). **Короб** — это полая пластиковая сборно-разборная труба, обычно прямоугольной формы, в которой прокладываются сетевые кабели, чаще всего вместе с электрическими (рис. 4.9).

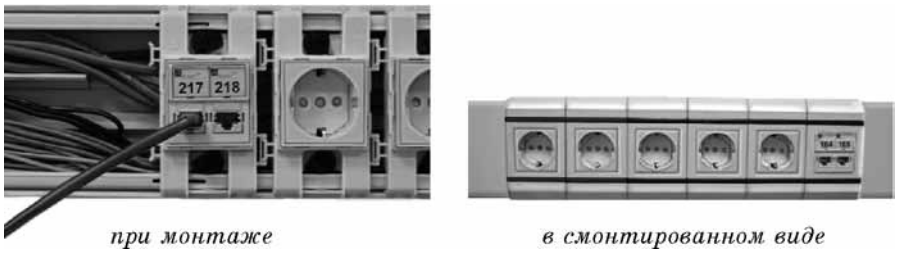


Рис. 4.9. Пластиковый короб для прокладки кабелей (с установленными сетевыми и электрическими розетками)

Беспроводные сети

Основные проблемы, характерные для всех проводных сетей, — их низкая *мобильность*, довольно большие капиталовложения в кабельную инфраструктуру и относительно малая дальность передачи сигнала. К беспроводным сетям это относится в меньшей степени, поэтому они все чаще входят в нашу жизнь. Хотя понятие «кабель» в беспроводных сетях отсутствует, среда передачи в них, безусловно, существует.

Для беспроводной передачи данных используют несколько способов.

- *Технологии радиосвязи* пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Они используются как в локальных сетях, так и для сетевых соединений на больших расстояниях. Поскольку радиосигналы легко перехватить, требуется обязательная защита данных кодированием и/или шифрованием.
- Передача данных *в микроволновом диапазоне* использует более высокие частоты и применяется как на коротких расстояниях (объединение локальных сетей в разных зданиях), так и в глобальных коммуникациях — с помощью спутников и наземных спутниковых антенн. Главное ограничение такой

связи: и передатчик, и приемник должны быть в зоне прямой видимости друг друга.

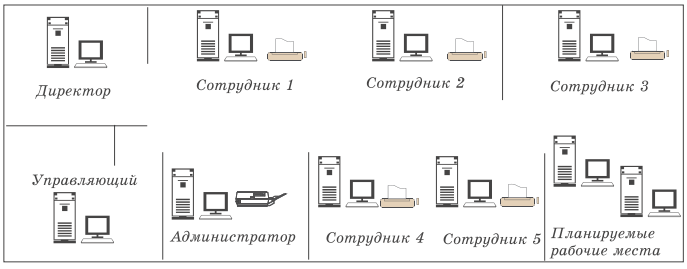
- Технологии, использующие *инфракрасное (ИК) излучение*, часто применяются для двусторонней или широковещательной передачи на близких расстояниях. Инфракрасная передача обычно используется в складских и офисных помещениях, чаще всего для взаимодействия с портативными (мобильными) устройствами. Хотя скорости инфракрасных сетей и удобство их использования очень привлекательны, возникают трудности при передаче сигналов на расстояние более 30 метров. К тому же ИК-сигналы легко блокируются любыми предметами, а также подвержены помехам со стороны сильных источников света и тепла, которые есть практически в любом помещении.
- Для беспроводных сетей также применяют *световое излучение в видимом диапазоне* (например, с помощью лазеров), хотя этот способ передачи используется редко. Тем не менее этот способ соединения может быть удобен для связи между высотными зданиями.

Кабели «витая пара» категории *5e* (или более высокой) сегодня являются наиболее универсальным, надежным и расширяемым решением для подключения к локальной сети стационарных рабочих станций и серверов. Оптоволокно чаще всего применяется для передачи сигналов на большие расстояния, например при соединении локальных сетей, расположенных в разных зданиях или даже районах. Использование радиосигналов обеспечивает подключение к сети мобильных устройств (ноутбуков, планшетных компьютеров или КПК).

Результатом работы по построению сети на данном этапе должна стать проложенная кабельная инфраструктура и, если это необходимо, установленные *беспроводные точки доступа к сети*.

Вопросы и задания

1. Кабель типа «витая пара» выпускается как в неэкранированном, так и в экранированном вариантах. Существует ли экранированный коаксиальный кабель?
2. К какой категории относится кабель из неэкранированной витой пары, способный передавать данные со скоростью до 10 Мбит/с?
3. Передача электрического сигнала требует наличия двух проводников. Какие именно проводники используются в коаксиальном кабеле? Зачем в кабеле «витая пара» используется несколько пар проводников (2 или 4)?
4. Какой разъем используется для подключения кабеля «витая пара» к компьютерам?
5. Основная задача коннекторов для металлических кабелей — обеспечить надежный электрический контакт при соединении отрезков кабеля или устройств сети. Какова основная задача коннекторов для оптоволоконного кабеля?
6. Что может создать помехи работе беспроводной сети, если в ней используется радиосвязь? Что может создать помехи работе беспроводной сети, основанной на использовании инфракрасного излучения?
7. Для ранее разработанной сети развивающейся компании (см. вопросы и задания к предыдущей главе) составьте проект прокладки кабеля «витая пара» категории 5 в кабельных каналах согласно выбранной вами топологии.



Глава 5 Строим сеть: выбор сетевой архитектуры

В этой главе вы найдете ответы на следующие вопросы:

- ***Какие существуют сетевые архитектуры?***
- ***Какими параметрами характеризуются сетевые архитектуры?***
- ***Какая сетевая архитектура наиболее распространена?***
- ***Как выбрать архитектуру для локальной или домашней сети?***

В предыдущей главе мы познакомились с основными типами кабельных соединений и выбрали для нашей сети оптимальный тип кабеля. Однако это только начало. Теперь нужно определиться с *сетевой архитектурой* — набором стандартов, топологий и протоколов низкого уровня, необходимых для создания работоспособной сети. Далее мы рассмотрим основные сетевые архитектуры, их преимущества и недостатки и выберем из них наилучшую: высокоскоростную, надежно функционирующую и расширяемую.

За многие годы развития сетевых технологий было разработано довольно много различных архитектур. Некоторые из них уже вышли из употребления, тогда как другие, такие как *Ethernet*, не только активно используются по сей день, но и постоянно совершенствуются.

Начнем изучение сетевых архитектур с тех их типов, которые сейчас применяются довольно редко.

Token Ring

Эта технология была разработана компанией IBM в 70-х гг., а затем стандартизована IEEE в «Проекте 802» как спецификация 802.5. Она имеет следующие характеристики:

- физическая топология — «звезда»;
- логическая топология — «кольцо»;

- метод доступа — передача маркера;
- скорость передачи данных — 4 или 16 Мбит/с;
- максимальный размер кадра — до 16 Кбайт;
- среда передачи — витая пара (используется 2 пары);
- максимальная длина сегмента:
  - UTP — 150 м (для 4 Мбит/с) или 60 м (для 16 Мбит/с),
  - STP — 300 м (для 4 Мбит/с) или 100 м (для 16 Мбит/с);
- максимальная длина сегмента с репитерами:
  - UTP — 365 м,
  - STP — 730 м;
- максимальное количество компьютеров на сегмент — 72 или 260 (в зависимости от типа кабеля).

Для объединения компьютеров в сетях Token Ring используются *концентраторы MSAU* (Multi-Station Access Unit), неэкранированная или экранированная витая пара (возможно и применение оптоволокна); в качестве разъемов используются специализированные соединители фирмы IBM либо стандартные коннекторы RJ-45.

К преимуществам архитектуры Token Ring можно отнести высокую дальность передачи (при использовании повторителей MSAU можно передавать данные на расстояние до 730 м), а также то, что в подобной сети легко рассчитать максимальную задержку при передаче информации между любыми двумя устройствами — ведь в качестве метода доступа к среде используется передача маркера. Последнее обстоятельство особенно важно в автоматизированных системах управления, требующих обработки процессов в реальном времени.

Недостатки архитектуры Token Ring — довольно высокая стоимость, низкая совместимость оборудо-

вания (например, в 16-мегабитных сетях Token Ring нельзя использовать 4-мегабитные устройства), а также довольно малая (по современным меркам) скорость передачи данных.

ARCNet

Сетевая среда ARCNet (Attached Resource Computing Network) была разработана корпорацией Datapoint в 1977 г. Стандартом она так и не стала, но в целом соответствует спецификации IEEE 802.4. Эта простая, гибкая и недорогая архитектура для небольших сетей (до 256 компьютеров) характеризуется следующими параметрами:

- физическая топология — «шина» или «звезда»;
- логическая топология — «шина»;
- метод доступа — передача маркера;
- скорость передачи данных — 2,5 или 20 (в ARCNet Plus) Мбит/с;
- максимальный размер кадра — 516 байт (в ARCNet Plus — около 4 Кбайт);
- среда передачи — витая пара или коаксиальный кабель;
- максимальная длина сегмента:
  - для витой пары — 244 м (для любой топологии),
  - для коаксиального кабеля — 305 или 610 м (для топологии «шина» или «звезда», соответственно).

Для соединения компьютеров здесь используются концентраторы. Основной тип кабеля — коаксиальный типа RG-62; поддерживается также витая пара и оптоволокно. Для коаксиального кабеля использу-

ются BNC-коннекторы, для витой пары — коннекторы RJ-45.

Единственным на сегодня преимуществом ARCNet можно считать большую дальность передачи при невысокой стоимости оборудования. Однако это преимущество никак не компенсирует множество проблем: сейчас весьма затруднительно найти сетевые адаптеры ARCNet, да и драйверы к ним в современных операционных системах отсутствуют.

AppleTalk

AppleTalk — «фирменная» сетевая среда, предложенная компанией Apple в 1983 г. и встроенная в компьютеры Macintosh (последняя версия — AppleTalk Phase 2). Она включает в себя целый набор протоколов, соответствующих модели OSI. На уровне сетевой архитектуры используется *протокол LocalTalk*, имеющий следующие характеристики:

- топология — «шина» или «дерево»;
- метод доступа — CSMA/CA;
- скорость передачи данных — 230,4 Кбит/с;
- среда передачи — экранированная витая пара;
- максимальная длина сети — 300 м;
- максимальное число компьютеров — 32.

Очень низкая пропускная способность встроенной архитектуры LocalTalk привела к тому, что многие производители стали предлагать адаптеры расширения, позволявшие AppleTalk работать с сетевыми средами большей пропускной способности — EtherTalk, TokenTalk и FDDITalk. В локальных сетях, построенных на базе IBM-совместимых компьютеров, сетевая среда AppleTalk практически не встречается.

100VG-AnyLAN

Архитектура 100VG-AnyLAN была разработана в 90-х гг. компаниями AT&T и Hewlett-Packard для объединения сетей Ethernet и Token Ring (отсюда слово «Any» в названии) и последующей миграции к единой скоростной сети. В 1995 г. эта архитектура получила статус стандарта IEEE 802.12. Она имеет следующие параметры:

- топология — «звезда»;
- метод доступа — по приоритету запроса;
- скорость передачи данных — 100 Мбит/с;
- среда передачи — витая пара категории 3, 4 или 5 (используются все 4 пары);
- максимальная длина сегмента (для оборудования HP) — 225 м.

В соответствии со спецификацией, концентратор 100VG-AnyLAN можно настроить на поддержку как кадров Ethernet, так и кадров Token Ring. Интересной особенностью сетей 100VG-AnyLAN является используемый в них *метод доступа по приоритету запроса* (*Demand Priority*), при котором концентраторы управляют доступом к кабелю, опрашивая каждый узел в сети и выявляя *запросы на передачу*. При одновременных запросах предпочтение отдается узлу, имеющему больший приоритет. Это позволяет без задержек передавать в сети 100VG-AnyLAN мультимедийные данные (аудио- и видеофайлы).

Из-за сложности и, как следствие, довольно высокой стоимости оборудования архитектура 100VG-AnyLAN так и не получила широкого распространения, проиграв гораздо более дешевой, надежной и совместимой архитектуре Fast Ethernet. В настоящее время она практически не применяется.

Архитектуры для домашних сетей: Home PNA

В 1996 г. целый ряд компаний объединились для создания стандарта, позволяющего строить домашние сети на основе обычной телефонной проводки. Результатом их работы стало появление в 1998 г. архитектуры Home PNA 1.0 (Home Phoneline Networking Alliance), а затем — архитектур Home PNA 2.0 и Home PNA 3.0. Их краткие характеристики приведены в табл 5.1.

Таблица 5.1

Сравнение стандартов Home PNA

Версия Home PNA	Топология	Скорость передачи данных, Мбит/с	Дальность передачи по телефонному проводу, м	Максимальное число компьютеров в сегменте
1.0	«звезда» или «шина»	1	150	25
2.0	«шина»	10	350	32
3.0	«звезда» или «шина»	128	300	50

Во всех указанных стандартах используется самый популярный на сегодня метод доступа к среде — CSMA/CD; в качестве среды передачи, естественно, рекомендуется использование телефонного кабеля; в качестве разъемов используются телефонные коннекторы RJ-11. Однако устройства Home PNA могут работать и с витой парой, и с коаксиальным кабелем, причем дальность передачи при этом существенно возрастает. Стоит также отметить, что использование топологии «звезда» и коммутаторов в Home PNA версий 1.0 и 3.0 позволяет объединять сегменты, тогда общее количество устройств в объединенной сети Home PNA может быть гораздо большим, чем показано в табл. 5.1.

Несмотря на кажущуюся заманчивой перспективу использования телефонных линий для создания домашних сетей, следует учесть, что телефонная проводка в нашей стране во многом не отвечает стандартам развитых стран как по качеству, так и по охвату (по наличию уже установленных розеток во всех комнатах). Кроме того, цены на адаптеры и устройства для сетей Home PNA довольно высоки. Поэтому шансов встретить в России домашние сети, построенные на основе этой технологии, пока немного. Тем не менее архитектуру Home PNA (особенно ее последнюю версию) вполне можно рассматривать в качестве альтернативы как для беспроводных сетей (в офисных зданиях и жилых домах), так и для модемных соединений (при подключении к Интернету).

Домашние сети на базе электропроводки

Еще более специфичными являются попытки использования в качестве среды передачи обычной электропроводки. Эта технология появилась совсем недавно и получила название Home PLC (Power Line Communication), или просто «HomePlug» (рис. 5.1).

Попытки ряда крупных компаний, объединившихся под эгидой некоммерческой организации HomePlug Powerline Alliance, продвигать этот стандарт в качестве способа создания домашних сетей, в том числе с подключением к Интернету, пока особым успехом не увенчались. Однако сетевое оборудование HomePlug уже имеется в продаже. Большинство из таких устройств на практике являются *конвертерами* (преобразователями), обеспечивающими подключение к сети HomePlug адаптеров таких популярных сетевых технологий, как Ethernet или Wi-Fi (о них будет рассказано далее). Существуют и совсем «экзотические» устройства, например позволяющие

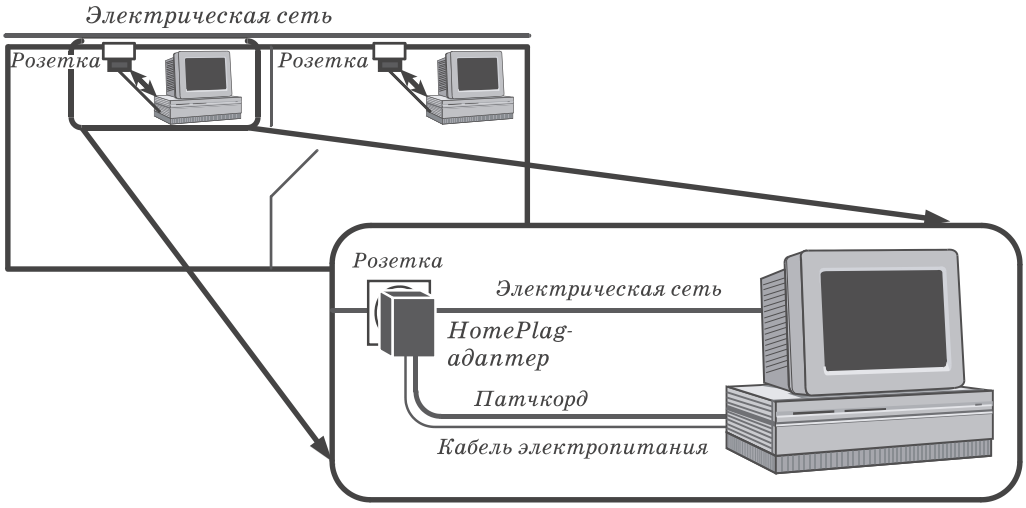


Рис. 5.1

передавать по электропроводке аудиоинформацию между компьютером и музыкальным центром.

Параметры сетей HomePlug:

- топология — «шина»;
- метод доступа — CSMA/CD;
- скорость передачи данных — до 85 Мбит/с;
- среда передачи — электрическая проводка;
- дальность связи — до 200 м;
- рекомендуемое число устройств в сети — не более 15.

Недостатки сетей Home PLC — незащищенность от перехвата, требующая обязательного применения технологий шифрования, и большая чувствительность к электрическим помехам, которые довольно резко снижают скорость передачи на больших расстояниях. К тому же устройства HomePlug пока еще достаточно дороги. Тем не менее стандарт Home PLC представляется весьма перспективным для использования в зданиях, где сетевая и телефонная проводка отсутствует, а также для обеспечения связи с управляемыми домашними бытовыми приборами.

Теперь перейдем к изучению наиболее популярных технологий, используемых в современных локальных сетях.

Ethernet

Архитектура Ethernet фактически объединяет целый набор стандартов, имеющих как общие черты, так и отличия. Первоначально она была создана фирмой Xerox в середине 70-х гг. и тогда представляла собой систему передачи со скоростью 2,93 Мбит/с. После доработки с участием компаний Intel и DEC архитектура Ethernet послужила основой принятого в 1985 г. стандарта IEEE 802.3, определившего для нее следующие параметры:

- топология — «шина»;
- метод доступа — CSMA/CD;
- скорость передачи — 10 Мбит/с;
- среда передачи — коаксиальный кабель;
- применение терминаторов — обязательно;
- максимальная длина сегмента сети — до 500 м;
- максимальная длина сети — до 2,5 км;
- максимальное количество компьютеров в сегменте — 100;
- максимальное количество компьютеров в сети — 1024.

В исходной версии Ethernet предусматривалось применение коаксиального кабеля двух видов — «толстого» и «тонкого» (стандарты 10Base-5 и 10Base-2, соответственно). Однако в начале 90-х гг. также появились спецификации для построения сетей Ethernet с использованием витой пары (10Base-T) и оптоволокна (10Base-FL). Позже, в 1995 г., был опубликован стандарт архитектуры Fast Ethernet (IEEE 802.3u), обеспечивающей передачу на скоростях до

100 Мбит/с, в 1998 г. — стандарт Gigabit Ethernet (IEEE 802.3z и 802.3ab), а в 2002 г. — стандарт 10 Gigabit Ethernet (IEEE 802.3ae).

Сравнение различных стандартов Ethernet приведено в табл. 5.2.

Заметим, что в современных версиях Ethernet использование физической топологии «шина» уже не предусмотрено, да и найти сейчас сети, построенные на коаксиальном кабеле, весьма затруднительно.

Таблица 5.2

Характеристики различных стандартов Ethernet

Реализация	Скорость передачи данных, Мбит/с	Топология	Среда передачи	Максимальная длина кабеля, м
		Ethernet		
10Base-5	10	«шина»	толстый коаксиальный кабель	500
10Base-2	10	«шина»	тонкий коаксиальный кабель	185; реально — до 300
10Base-T	10	«звезда»	витая пара	100
10Base-FL	10	«звезда»	оптоволокно	500 (станция-концентратор); 2000 (между концентраторами)
		Fast Ethernet		
100Base-TX	100	«звезда»	витая пара категории 5 (используется две пары)	100
100Base-T4	100	«звезда»	витая пара категории 3, 4 или 5 (используется четыре пары)	100
100Base-FX	100	«звезда»	многомодовое или одномодовое оптоволокно	2000 (многомодовый); 15000 (одномодовый); реально — до 40 км

Реализация	Скорость передачи данных, Мбит/с	Топология	Среда передачи	Максимальная длина кабеля, м
		Gigabit Ethernet		
1000Base-T	1000	«звезда»	витая пара категории 5 или выше	100
1000Base-CX	1000	«звезда»	специальный кабель типа STP	25
1000Base-SX	1000	«звезда»	оптоволокно	220–550 (многомодовый), в зависимости от типа
1000Base-LX	1000	«звезда»	оптоволокно	550 (многомодовый); 5000 (одномодовый); реально — до 80 км
		10 Gigabit Ethernet		
10GBase-*x* (*x* — набор стандартов)	10000	«звезда»	оптоволокно	300–40000 (в зависимости от типа кабеля и длины волны лазера)

Основной недостаток сетей Ethernet связан с использованием в них метода доступа к среде CSMA/CD (напомним: это сокращение расшифровывается как «множественный доступ с контролем несущей и обнаружением столкновений»). При увеличении количества компьютеров растет число столкновений, что снижает пропускную способность сети и увеличивает время доставки кадров. Поэтому рекомендуемой нагрузкой для сетей Ethernet считается уровень в 30–40 % от общей полосы пропускания. Сразу заметим, что в современных сетях этот

недостаток довольно легко устраняется путем замены концентраторов *мостами* и *коммутаторами*, умеющими «изолировать» передачу данных между двумя компьютерами в сети от других (об этих устройствах будет рассказ в следующей главе).

А вот преимуществ у архитектуры Ethernet довольно много. Прежде всего, сама эта технология довольно проста в реализации. Соответственно, Ethernet-устройства (сетевые адаптеры, концентраторы, коммутаторы и т. д.) оказываются значительно дешевле аналогичных устройств других сетевых архитектур. В Ethernet можно использовать практические любые виды кабеля, а применение оптоволокна позволяет объединять участки сетей, расположенные далеко друг от друга. Наконец, совместимость различных вариантов Ethernet очень высока, что позволяет не только наращивать мощности сети с использованием существующей кабельной инфраструктуры, но и легко расширять сеть, подключая к ней новые, более скоростные сегменты. Поэтому сегодня архитектура Ethernet не только стала господствующей в локальных сетях, но и вытесняет другие технологии в региональных и глобальных сетях.

Беспроводные сети

Перейдем теперь к беспроводным сетевым решениям, из которых в локальных сетях сейчас наиболее часто применяются технологии Wi-Fi и Bluetooth.

Wi-Fi (сокращение от «Wireless Fidelity», «беспроводная точность») — популярная в мире и быстро развивающаяся в России технология, обеспечивающая беспроводное подключение мобильных пользователей к локальной сети и Интернету (рис. 5.2).

Под именем «Wi-Fi» на самом деле скрывается несколько стандартов, разработанных для беспро-

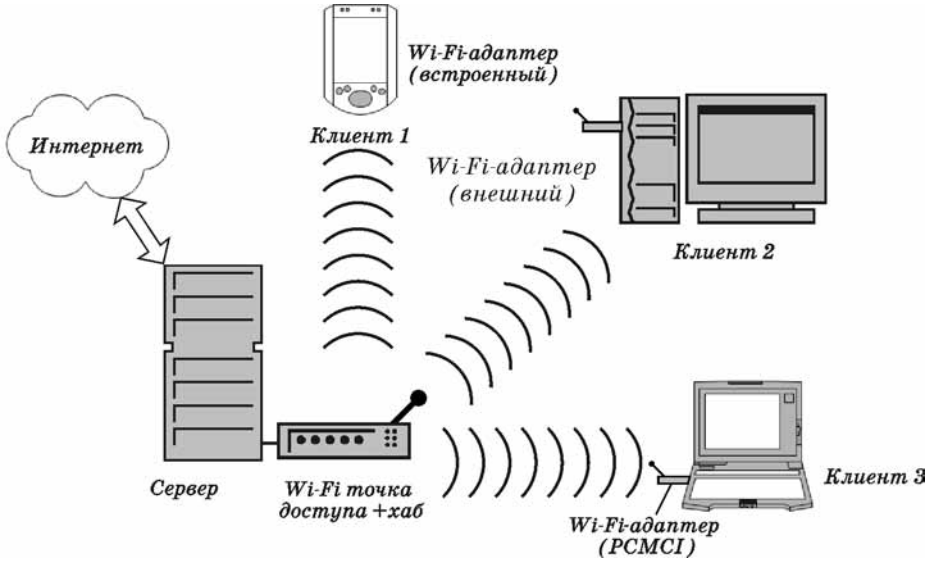


Рис. 5.2

водных сетей на основе выпущенной еще в 1997 г. спецификации IEEE 802.11 (табл. 5.3).

Важно отметить, что в стандарте 802.11 предусматривается использование только *полудуплексных приемопередатчиков*, которые не могут одновременно передавать и принимать информацию. Из-за этого в беспроводных сетях 802.11 станция в принципе не может обнаружить столкновение во время передачи (поскольку в это время не имеет возможности принимать данные). Поэтому в качестве метода доступа к среде во всех стандартах используется метод CSMA/CA (с предотвращением коллизий), позволяющий избегать столкновений. Это приводит к дополнительным сложностям при взаимодействии и, как следствие, к существенно меньшим скоростям передачи данных, чем, например, в технологии Ethernet.

Основным же недостатком сетей Wi-Fi на сегодня является довольно малая дальность передачи данных,

Таблица 5.3

Наиболее важные стандарты IEEE 802.11*x*

Стандарт	Среда передачи	Скорости передачи, Мбит/с	Примечание
802.11	радиосигнал с частотой около 2,4 ГГц или ИК-сигнал	1 или 2	Базовый стандарт, определяющий взаимодействие на физическом и канальном уровнях модели OSI
802.11a	радиосигнал с частотой около 5 ГГц	до 54	Несовместим на физическом уровне со стандартами 802.11b и g; в России не используется
802.11b	радиосигнал с частотой 2,4–2,483 ГГц	до 11	Имеет относительно низкую скорость и защищенность (защита шифрованием по технологии WEP — Wireless Equivalent Privacy). Обеспечивает несколько большую, по сравнению с другими стандартами, дальность передачи данных
802.11g	радиосигнал с частотой 2,4–2,483 ГГц	до 54	Обеспечивает обратную совместимость со стандартом 802.11b, но характеризуется большей скоростью и защищенностью (кроме WEP, поддерживается стандарт защиты WPA — Wi-Fi Protected Access)

не превышающая для большинства устройств 150 м (максимум 300 м) на открытом пространстве или всего нескольких десятков метров — в помещении.

Решением указанной проблемы может стать архитектура **WiMAX** (Worldwide Interoperability for Microwave Access), разрабатываемая в рамках рабочей группы IEEE 802.16. Реализация этой технологии, также использующей радиосигналы в качестве среды передачи, позволит предоставить пользователям скоростной беспроводной доступ на расстояниях до нескольких десятков километров (рис. 5.3).

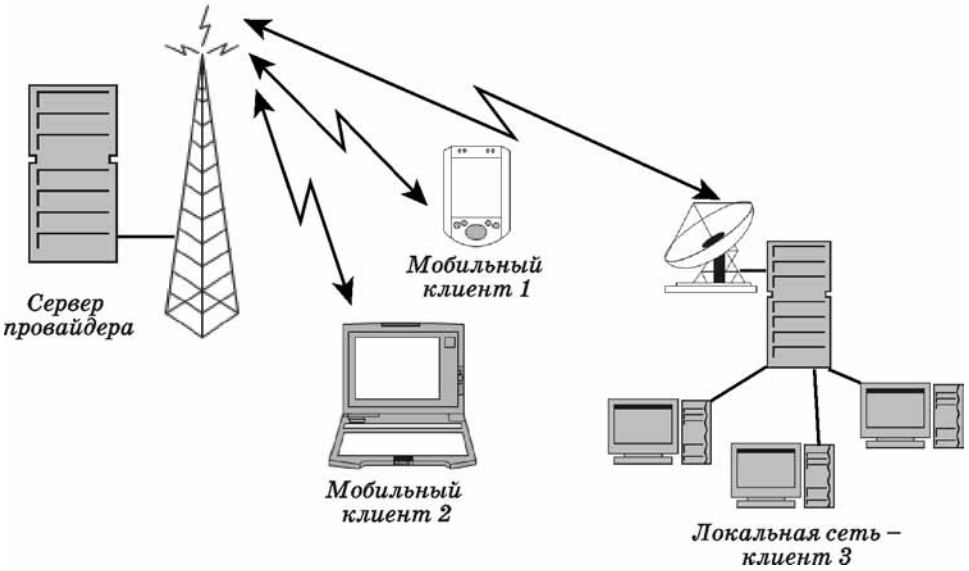


Рис. 5.3

Wireless USB — альтернатива Bluetooth

Технология Wireless USB основана на использовании нового стандарта ультраширокополосной беспроводной связи — UWB и обеспечивает сверхвысокоскоростную (до 480 Мбит/с, а в перспективе — и до 1 Гбит/с) передачу данных на короткие расстояния (до 10 м). Она позволяет реализовать беспроводное подключение периферийных устройств, аналогичное USB 2.0.

Первый серийный образец адаптера Wireless USB был представлен на Форуме Intel для разработчиков (IDF-2005). В продаже такие адаптеры, должны появиться в начале 2006 г.

Наконец, стоит упомянуть еще об одной из популярных сегодня беспроводных архитектур — о **технологии Bluetooth** (стандарт IEEE 802.15.1), а также о совсем новой **технологии ZigBee**.

Как и в Wi-Fi, в Bluetooth используется радиосигнал с частотой 2,4 ГГц, однако эти стандарты между собой несовместимы. Bluetooth характеризуется довольно низким энергопотреблением, что позволяет с успехом применять эту технологию в переносных устройствах — ноутбуках, КПК и мобильных телефонах (рис. 5.4). К тому же Bluetooth практически не требует настройки — этот стандарт позволяет устройствам устанавливать взаимодействие при минимальном участии пользователя. С другой стороны, у Bluetooth весьма низкие показатели по дальности передачи и пропускной способности — не более 10 метров и 400–700 Кбит/с, — что резко ограничивает возможности использования этой технологии в локальных сетях.

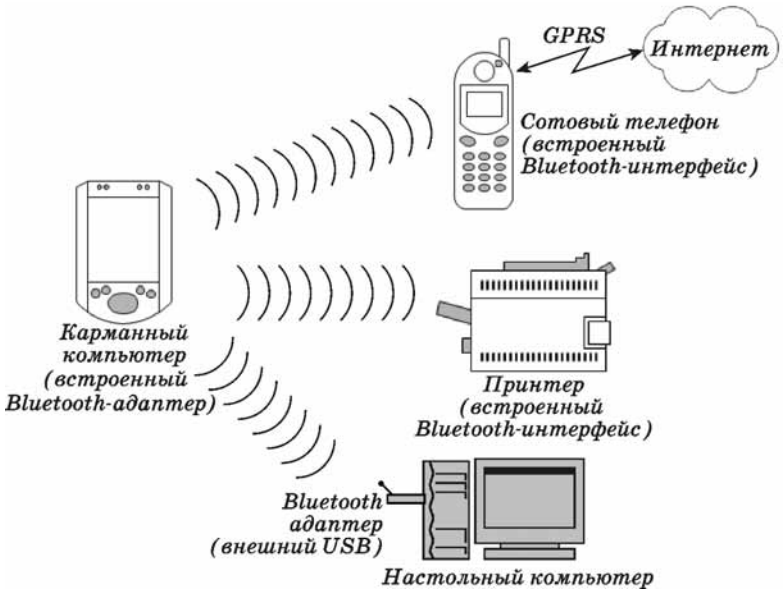


Рис. 5.4

У технологии ZigBee, появившейся недавно благодаря усилиям нескольких крупных коммуникационных компаний (стандарт 802.15.4), показатели еще «скромнее» — ее спецификация предусматривает защищенную передачу данных в радиусе 10–75 метров и с максимальной скоростью до 250 Кбит/с. Казалось бы, зачем она нужна, если скорости передачи в ней еще ниже, чем для Bluetooth. Однако «изюминкой» устройств ZigBee является их сверхнизкое энергопотребление и способность переходить в «спящий режим», когда передача данных не требуется. Поэтому основной сферой использования ZigBee-устройств станут не локальные сети, а системы мониторинга и контроля аппаратуры, в том числе сетевого оборудования.

Основной технологией, используемой сегодня в проводных сетях, является Ethernet. Важно лишь определить конкретный стандарт или набор стандартов, которые используются в сети, и закупить нужное оборудование. При этом рекомендации достаточно просты: старайтесь выбрать наиболее скоростное и надежное оборудование, удовлетворяющее вас по цене. Желательно, чтобы это оборудование было максимально функциональным и управляемым, однако эти критерии более значимы для сетевых администраторов крупных корпоративных сетей.

Для подключения беспроводных клиентов следует остановиться на технологии Wi-Fi, причем выбирать нужно устройства, поддерживающие последний стандарт 802.11g, — только в нем обеспечивается достаточная скорость передачи данных и, самое главное, их надежная защита.

Вопросы для повторения

1. Какие вы знаете сетевые архитектуры? Каковы их преимущества и недостатки?
2. Почему архитектура Ethernet сегодня получила наибольшее распространение?
3. Какие вы знаете разновидности архитектуры Ethernet? Чем они различаются?
4. Какие вы знаете беспроводные сетевые технологии?
5. Какие сетевые технологии, на ваш взгляд, лучше всего использовать:
   - при создании локальной сети в крупном офисе?
   - при развертывании домашней сети в городской квартире (с телефоном)?
   - при развертывании домашней сети в сельском доме (не телефонизированном)?
   - при объединении в сеть мобильных компьютеров (КПК) на территории торгового центра или склада?
   - при организации систем сбора данных в полевых условиях на территории поселка в сельской местности?

Глава 6

Строим сеть: выбор устройств связи

В этой главе вы найдете ответы на следующие вопросы:

- ***Что такое сетевой адаптер, какие функции он выполняет?***
- ***Какие устройства отвечают за связь компьютеров с сетью?***
- ***В чем сходство и различие таких устройств связи, как концентраторы, мосты, коммутаторы и шлюзы?***
- ***Как правильно выбрать устройство связи?***

Проанализировав рассмотренные в предыдущей главе сетевые архитектуры, мы решили использовать в нашей сети технологии Ethernet (на базе «витой пары») и Wi-Fi. Будем считать, что кабельная инфраструктура у нас уже готова — в нужных местах проложены кабели, смонтированы розетки и панели для подключения сетевых устройств. Теперь нужно выбрать устройства, которые позволят объединить компьютеры, серверы, ноутбуки и КПК в единую сеть.

Устанавливаем сетевой адаптер

Начнем с компьютеров. Чтобы взаимодействовать с сетью, компьютеру требуется какой-либо *сетевой адаптер* (проводной или беспроводной). Обычно с этим проблем не бывает — подавляющее большинство современных компьютеров имеют встроенные сетевые адаптеры Ethernet и Wi-Fi, интегрированные в материнскую плату (иногда — даже несколько). Не беда, если в вашем компьютере не окажется нужного сетевого адаптера, — его легко приобрести в любом компьютерном магазине и установить в слот расширения компьютера или в порт USB.

Кроме того, следует установить *драйвер сетевого адаптера* — специальное программное обеспечение, позволяющее операционной системе (ОС) работать с этим устройством. Как правило, современная ОС

(например, Windows XP) сама распознает устройство и устанавливает для него требуемый драйвер. Если же этого не произошло (или с автоматически установленным драйвером сеть не работает), то надо установить драйвер вручную с дискеты, входящей в комплект поставки адаптера.

Сетевой адаптер и драйвер работают *на физическом уровне* и *подуровне управления доступом к среде* (*MAC*) модели OSI, обеспечивая взаимодействие физического и сетевого уровней.

Соответственно, адаптер должен иметь нужный разъем для подключения коннектора (обычно RJ-45), а также уникальный физический (или «MAC») адрес, используемый *для однозначной идентификации компьютера в данном сегменте сети*. Обычно этот адрес назначается производителем адаптера при изготовлении, однако некоторые модели адаптеров допускают смену MAC-адреса вручную, например через настройки BIOS адаптера или с помощью специальной программы.

Если на компьютере с операционной системой Windows 2000 или XP установлен протокол TCP/IP, то MAC-адреса установленных в этом компьютере адаптеров можно легко определить с помощью целого ряда утилит: `IPCONFIG`, `NBTSTAT`, `ROUTE PRINT`, `NETSTAT`, `NET CONFIG`. Достаточно в командной строке подать команду

```
IPCONFIG /ALL
```

и в выданном на экран тексте обратить внимание на параметр «Физический адрес».

В операционной системе Windows XP это сделать еще проще — достаточно дважды щелкнуть мышью на значке подключения в окне **Сетевые подключения**, в открывшемся окне состояния адаптера выбрать вкладку **Поддержка** и на ней нажать кнопку **Подробности**.

Выбираем устройство связи

Ранее мы уже упоминали различные типы устройств, используемых для связи компьютеров в сетях. Теперь рассмотрим их подробнее, поскольку от правильного выбора устройства связи зависят не только качество и скорость работы сети, но и возможности ее дальнейшего расширения.

Чтобы объединить сетью только *два* компьютера (например, в домашней сети), устройства связи вообще не нужны — достаточно наличия в них совместимых сетевых адаптеров. При использовании Ethernet нам потребуется *перекрестный кабель* (как его изготовить, было сказано в главе 4), который достаточно вставить в разъемы RJ-45 сетевых адаптеров. При использовании же Wi-Fi следует переключить беспроводные адаптеры в специальный режим *Ad-Hoc*, обеспечивающий прямое взаимодействие компьютеров друг с другом. Заметим, что таким способом можно соединить и несколько компьютеров с беспроводными адаптерами, однако скорость передачи данных будет уменьшаться с увеличением числа компьютеров в такой сети.

Концентраторы (повторители)

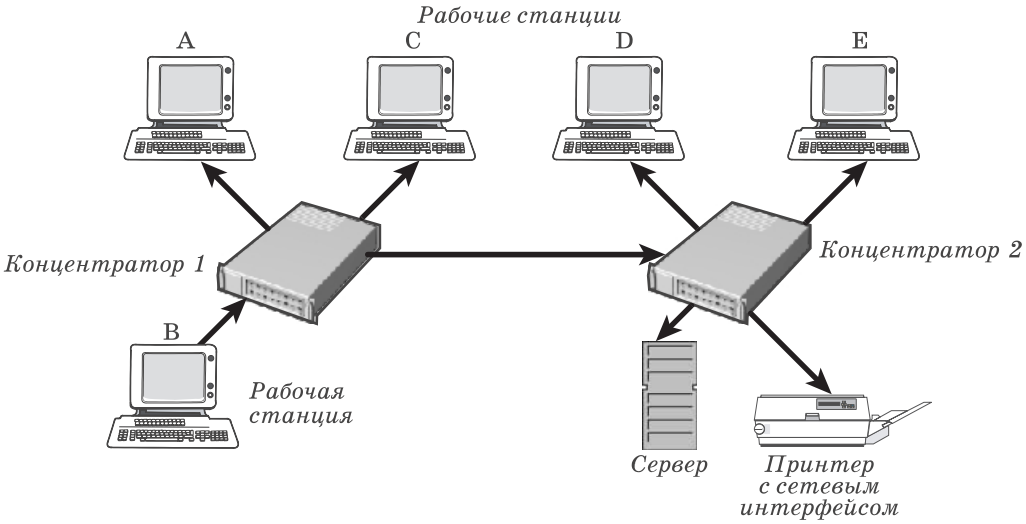
Простейшим устройством, обеспечивающим связь компьютеров друг с другом, является *концентратор*, или «*хаб*» (*hub*). В сетях, использующих коаксиальный кабель, концентраторы принято называть *повторителями*, или *репитерами* (*repeater*).

Обычно концентратор имеет от 4 до 32 гнезд (*портов*) для подсоединения коннекторов различных типов. В большинстве случаев это будут, конечно, гнезда для коннекторов RJ-45, однако существуют и *гибридные концентраторы* с портами RJ-45 и BNC, позволяющие объединять сегменты Ethernet стандартов 10Base-T и 10Base-2. К портам можно

подключать не только компьютеры, но и другие концентраторы, формируя таким образом *цепочки* (*каскады*) *концентраторов* или еще более сложные топологии типа «дерево».

В стандартах 10Base-5 и 10Base-2 на такое *каскадирование* концентраторов действовали довольно жесткие ограничения, описываемые «правилом 5-4-3»: в сети не могло быть больше 5 сегментов, соединенных 4 репитерами, и только в 3 сегментах допускалось подключение компьютеров. В сетях стандарта 10Base-T допускалось максимум 5 сегментов. В стандарте 100Base-T все было еще сложнее — концентраторы класса I, поддерживающие одновременную работу с устройствами 100Base-T4, 100Base-TX и 100Base-FX, каскадировать было вообще нельзя, а концентраторы класса II можно было объединять только в пару. В этом и состояла первая проблема сетей на основе концентраторов — построить крупную сеть с помощью только концентраторов было просто невозможно.

Концентраторы работают на физическом уровне модели OSI и являются достаточно примитивными *активными устройствами* (требующими подключения к электрической сети). Их основная задача — *принять, усилить и ретранслировать электрический сигнал*, полученный от одного компьютера, во все остальные активные порты (рис. 6.1). Никакой другой обработке сигнал в концентраторе не подвергается, его буферизация не производится, а коллизии не обрабатываются (хотя на многих моделях концентраторов есть индикатор уровня столкновений).



Пакет, отправленный компьютером B компьютеру A, будет передан всем рабочим станциям, серверу, принтеру и другим сетевым устройствам.

Рис. 6.1. Пример передачи данных с помощью концентраторов

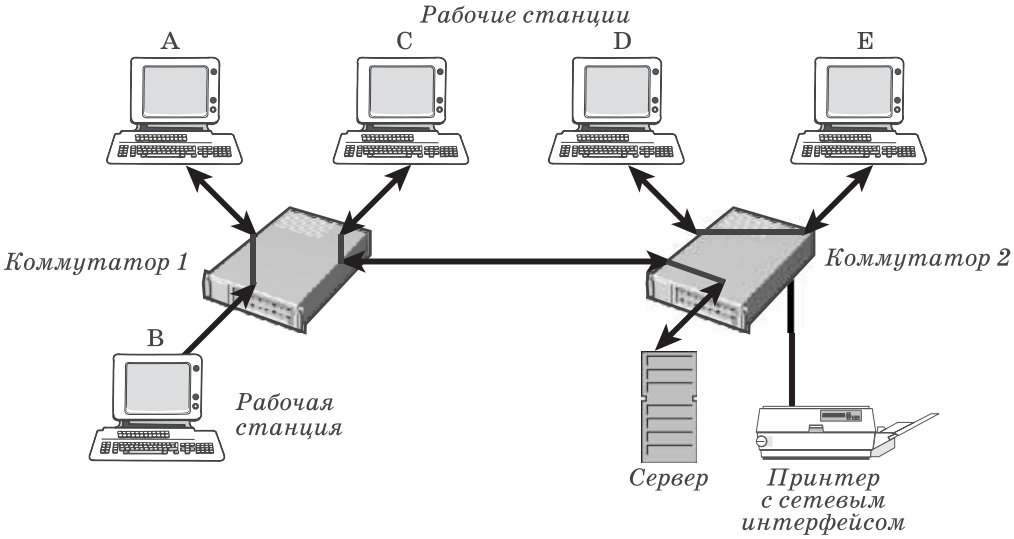
Отсюда вытекает вторая основная проблема, с которой рано или поздно сталкиваются все администраторы сетей, применяющие только концентраторы, — очень большое количество столкновений, возрастающее с увеличением числа сегментов и компьютеров в сети (вспомним, что в сети Ethernet используется метод доступа CSMA/CD). Есть даже термин, описывающий такое поведение сети: говорят, что концентраторы *формируют «область столкновений»* (Collision Domain). Поэтому сегодня концентраторы в сетях практически не используются — их вытеснили сначала *мосты*, а затем *коммутаторы*.

Мосты и коммутаторы

Мосты (*bridge*), а затем и *коммутаторы* (*switch*) были призваны помочь в объединении сетей и устранении проблемы возникновения большого числа

коллизий. Существенным отличием этих устройств от концентраторов является то, что они умеют определять MAC-адреса источника и приемника сигналов, а также поддерживать *таблицу соответствия своих портов и используемых в сети MAC-адресов*. Такую таблицу мост (или коммутатор) формирует сразу после включения по следующему принципу — как только порт получает ответ от устройства с определенным физическим адресом, в таблице появляется строчка соответствия: «MAC-адрес ↔ порт».

Таким образом, эти устройства работают *не только на физическом уровне модели OSI, но и на канальном*, — точнее, *на подуровне управления доступом к среде (MAC)*. Получив кадр и определив адрес назначения, мост или коммутатор транслируют кадр только в тот порт, с которым этот MAC-адрес сопоставлен



Обмен данными между компьютерами A и B ***никак не влияет*** *на взаимодействие компьютера C с сервером, а компьютера D и E — друг с другом.*

Рис. 6.2. Передача кадров с помощью коммутаторов

в таблице соответствий. Кадры, передаваемые между компьютерами одного сегмента, коммутатор получает, но никуда не транслирует (рис. 6.2).

Единственными сигналами, передаваемыми во все порты, являются кадры, предназначенные для адресов, пока не имеющих записей в таблице соответствий, и специальные *широковещательные сообщения*, предназначенные всем компьютерам локальной сети. Чтобы обозначить эту особенность работы мостов и коммутаторов, говорят, что они *формируют «область широковещания»* (*Broadcast Domain*).

Различие между мостами и коммутаторами заключается в том, что мост в каждый момент времени может передавать только один кадр, обслуживая передачу от одного компьютера к другому (поэтому первые модели мостов были двухпортовыми). Коммутатор же умеет выстраивать большое число виртуальных каналов связи между портами (т. е. коммутировать порты друг с другом, отсюда и название устройства), производя *параллельную обработку* кадров, поступающих с разных портов. Естественно, производительность сетей, построенных на базе коммутаторов, существенно выше.

Подчеркнем, что подавляющее большинство современных сетей строится именно на коммутаторах, тогда как встретить концентратор или мост сегодня довольно трудно.

Маршрутизаторы

Маршрутизаторы работают на еще более высоком уровне модели OSI — *сетевом*. В их задачу входит анализ адресов, используемых в протоколе этого уровня (например, IP-адресов), и определение наилучшего *маршрута доставки пакета данных* по назначению (подробнее о маршрутизации будет рассказано в следующих главах). Конечно, маршрутизаторы работают и на более низких уровнях модели OSI — как концентраторы они восстанавливают уро-

вень и форму предаваемого сигнала, как мосты и коммутаторы — позволяют избежать столкновений. Однако, в отличие от вышеперечисленных устройств, маршрутизаторы *изменяют передаваемые кадры Ethernet* — точнее, «разбирают» их до сетевого уровня, а затем формируют заново по определенным правилам. Кстати, без определенной настройки маршрутизаторы не передают в другие порты даже широковещательные пакеты, и, таким образом, служат в сетях *границами областей столкновений и широковещаний*.

Кроме того, совместно с программами более высокого уровня модели OSI, маршрутизаторы умеют выполнять целый ряд весьма сложных действий, например обнаруживать проблемы в сети и сообщать о них, вести статистику полученных и переданных данных, фильтровать пакеты, проводить авторизацию пользователей при выходе в Интернет и т. д.

Мощные маршрутизаторы являются довольно сложными и дорогими программно-аппаратными комплексами, поэтому в современных сетях они все чаще заменяются *коммутаторами 3-го уровня* — устройствами, занимающими промежуточную ступень между коммутаторами и маршрутизаторами. От обычных коммутаторов они отличаются тем, что могут выполнять простейшие функции маршрутизации, оставаясь при этом производительными и не очень дорогими.

Кроме того, следует упомянуть и о такой функции современных коммутаторов, как возможность строить *виртуальные локальные сети* (*Virtual LAN*), когда в один *логический* сегмент сети объединяются компьютеры, *физически* подключенные к разным коммутаторам (рис. 6.3). Критерии для такого объединения могут быть различными, начиная с MAC- или IP-адресов и заканчивая именами компьютеров.

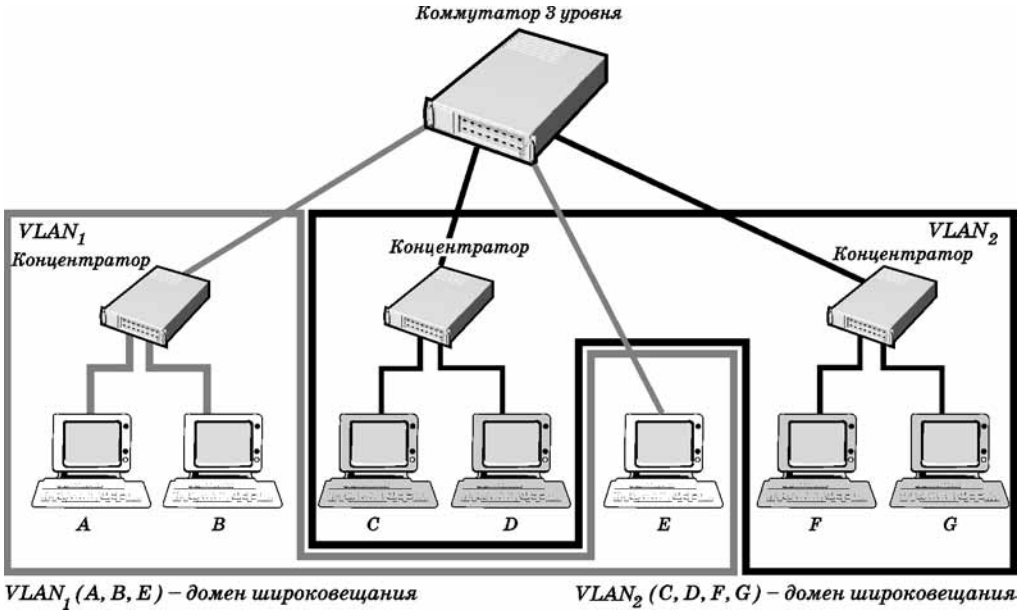


Рис. 6.3. Пример формирования локальной виртуальной сети

Шлюзы

Вообще говоря, под шлюзом обычно понимается любое устройство или программа, позволяющие *объединять разнородные системы* (например, существуют почтовые шлюзы, используемые для связи разных систем электронной почты). Но если речь идет о взаимодействии в сетях, то здесь под шлюзом подразумевается устройство, *соединяющее разные сетевые архитектуры* (пример: шлюз из Ethernet в Token Ring). Важно здесь то, что шлюз должен не только иметь физические порты для подключения разнородных систем, но и «понимать» разнородные протоколы, выступая для них в роли «переводчика».

Типичным примером шлюзов являются широко используемые в современных домашних сетях интегрированные устройства, в которых объединены ADSL-модем для подключения к Интернету, беспро-

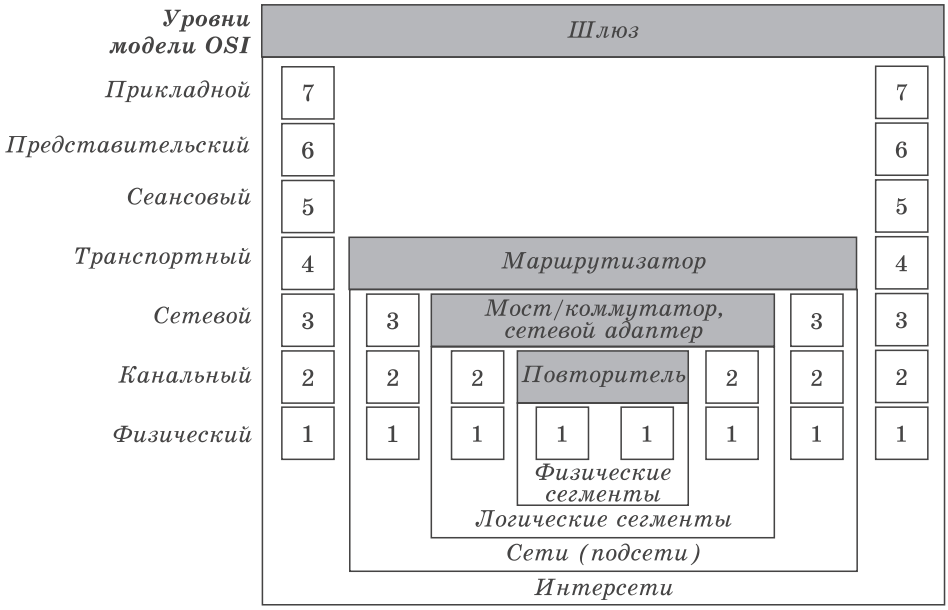


Рис. 6.4. Соответствие функций коммуникационного оборудования модели OSI

водная точка доступа, работающая по стандарту IEEE 802.11b (или g), и коммутатор Fast Ethernet с поддержкой стандарта IEEE 802.3u.

Сформулируем несколько рекомендаций, которыми можно руководствоваться при выборе устройств связи.

Наиболее распространенными устройствами связи в сетях сегодня являются коммутаторы Fast и Gigabit Ethernet, а подключение беспроводных устройств к локальной сети осуществляется с помощью *шлюзов*, объединяющих функции *коммутатора* и *точки беспроводного доступа*, работающей по стандарту 802.11g.

Для домашних и небольших офисных сетей вполне подойдут недорогие 8- и 16-портовые коммутаторы Fast Ethernet, желательно с функцией управления портами. Если передача больших объе-

мов данных не планируется, можно остановиться на беспроводных точках доступа, хотя это мобильное решение обойдется дороже и будет менее скоростным.

В крупных сетях основу должны составлять мощные и надежные коммутаторы Gigabit или 10Gigabit Ethernet, к которым подключаются коммутаторы подразделений (зданий), а к ним, в свою очередь, — коммутаторы этажей (офисов). Размещение точек доступа в крупных сетях следует тщательно планировать, чтобы пользователь при перемещении по территории предприятия последовательно переключался с одной точки доступа на другую, сохраняя связь с локальной сетью.

Применение *маршрутизаторов* требуется там, где нужно четко контролировать потоки IP-пакетов в сложной маршрутизируемой сети, а также обеспечивать резервные маршруты доставки пакетов, — например, при взаимодействии с удаленным офисом или Интернетом.

При выборе *сетевого адаптера* для компьютера следует обратить внимание на возможность поддержки стандартов Ethernet или Wi-Fi. Лучше всего выбрать несколько более дорогой, но современный сетевой адаптер, например Gigabit Ethernet или Wi-Fi стандарта 802.3g. Поскольку эти стандарты *обратно совместимы* с предыдущими, такие адаптеры вполне смогут работать со старыми концентраторами 10Base-T и точками доступа 802.11b, пока не будут заменены указанные устройства связи.

Вопросы и задания

1. Какое устройство обеспечивает интерфейс между компьютером и сетевым кабелем?
2. Что понимается под названием «устройство связи»?
3. В чем сходство и различие между концентраторами и повторителями?

4. Что такое каскадирование? Какие преимущества оно обеспечивает?
5. В чем сходство и различие между мостами и коммутаторами? Чем они отличаются от концентраторов?
6. Что такое маршрутизатор? Может ли он заменить собой концентратор, мост или коммутатор?
7. Для чего предназначены шлюзы?
8. Что такое «точка беспроводного доступа»? Для чего она предназначена?
9. На каких уровнях модели OSI работает каждый из изученных вами типов устройств связи?
10. Спроектируйте (в виде примерной структурной схемы) сеть крупной фирмы, состоящей из трех подразделений:
    - офис администрации (отдельный этаж здания в центре Москвы, 10 рабочих мест; см. вопросы и задания к главам 3 и 4);
    - склад (отдельное здание за пределами МКАД), оснащен 5 стационарными рабочими станциями;
    - торговый центр (рынок стройматериалов большой площади плюс автостоянки для покупателей), персонал которого при работе с клиентами использует КПК, свободно перемещаясь по территории торгового центра и стоянок на расстояния до 1,5–2 км.

    При этом в пределах офиса и склада подсети должны иметь звездообразную структуру, для офиса администрации необходимо обеспечить возможность выхода в Интернет по каналу ADSL, а связь между подразделениями фирмы осуществляется при помощи оптоволоконного кабеля. Считать определяющими параметры скорости и надежности работы сети, пренебрегая ее стоимостью.

Глава 7

Налаживаем взаимодействие между компьютерами: выбор стека протоколов

В этой главе вы найдете ответы на следующие вопросы:

- ***Что такое стек протоколов?***
- ***Какие существуют стеки протоколов?***
- ***Какой стек протоколов наиболее распространен?***
- ***Какие протоколы различных уровней используются в TCP/IP?***

В прошлых главах мы узнали, как компьютеры объединяются в сети, выбрали сетевую топологию и архитектуру, соединили компьютеры с помощью коммутаторов (или других устройств связи) и настроили драйверы сетевых адаптеров. Однако чтобы компьютеры могли работать в сети, всего этого недостаточно. Теперь нужно научить сетевые приложения «разговаривать» друг с другом — обмениваться данными с помощью протоколов на уровнях, более высоких, чем канальный. Поскольку этих уровней несколько, нам потребуется не один, а несколько протоколов, объединенных в набор, или, как говорят, в *стек*.

В этой главе мы изучим некоторые наиболее часто применяемые в сетях *стеки протоколов*, в том числе самый распространенный на сегодня набор протоколов — *стек TCP/IP*.

Как и в случае с сетевыми архитектурами, начнем изучение с протоколов, которые сейчас применяются достаточно редко.

Аббревиатура NetBEUI расшифровывается как «NetBIOS Extended User Interface» — «улучшенная версия протокола NetBIOS».

NetBEUI

Небольшой по объемам требуемого программного обеспечения протокол, реализующий поддержку *сетевого*, *транспортного* и *сеансового уровней* модели OSI. Наиболее прост в настройке (фактически ее не требует), работает эффективно и быстро в небольших и средних по размерам сетях (до 200 компьютеров). Серьезными, по современным меркам, недостатками протокола NetBEUI являются ограничения при работе в сетях с большим количеством компьютеров и, самое главное, отсутствие поддержки маршрутизации — возможности сетевой адресации и функции пересылки пакетов между сетями в нем просто не реализованы. Соответственно, его нельзя использовать в крупных сетях, объединенных маршрутизаторами, и при работе с Интернетом. Протокол NetBEUI поставлялся в составе всех операционных систем Windows вплоть до Windows 2000, однако в последних версиях его поддержка прекращена.

IPS/SPX и NWLink

Стек протоколов IPX/SPX был разработан фирмой Novell в начале 80-х гг. для своей сетевой операционной системы NetWare. Основа стека — это протоколы IPX (Internetwork Packet eXchange) и SPX (Sequenced Packet eXchange), реализующие функции *сетевого* и *транспортного уровней* модели OSI соответственно. Как и NetBEUI, протокол IPX/SPX является небольшим (его программную поддержку легко уместить на обычной дискете 1,44 Мб вместе с DOS) и быстрым, что было особенно важно в эпоху первого поколения IBM-совместимых компьютеров с малым объемом оперативной памяти (640 Кбайт). Кроме того, в стеке IPX/SPX поддерживается маршрутизация. Оба этих фактора, наряду с надежностью серверов на базе опера-

ционной системы Novell Netware тех лет, способствовали широкому распространению стека IPX/SPX в локальных сетях в 80-е и 90-е гг. К недостаткам этого стека протоколов следует отнести интенсивное использование широковещательных сообщений, серьезно нагружающих сеть, особенно при работе по медленным глобальным каналам. Это обстоятельство, а также то, что стек IPX/SPX принадлежит фирме Novell и для его реализации другим производителям сетевых операционных систем приходилось покупать лицензию, привели в итоге к вытеснению IPX/SPX общедоступным стеком TCP/IP. Важную роль здесь сыграло и то, что все больше организаций в 90-е гг. стало подключаться к Интернету, в котором использовался именно стек TCP/IP, а поддерживать в сети два стека протоколов — лишняя «головная боль» для сетевых администраторов.

NWLink — реализация стека IPX/SPX компанией Microsoft, поставляемая во всех версиях Windows.

TCP/IP

История развития стека TCP/IP (как и история Интернета) началась еще в конце 60-х гг. прошлого, XX века с проекта ARPANet — сети Агентства перспективных исследовательских проектов (Advanced Research Project Agency Network) Министерства обороны США. Поскольку для военных во времена «холодной войны» была особенно важна возможность передачи данных даже в условиях атомных бомбардировок, ARPANet задумывалась как высоконадежная сеть, объединяющая военные, государственные и научные учреждения. Получившаяся в результате сеть и разработанный несколько позже (в 70-х гг.) стек протоколов TCP/IP оказались настолько удачными, что даже после прекращения финансирования проекта ARPANet Министерством обороны продолжали жить и успешно развиваться, создав основы современного Интернета.

Основные преимущества стека TCP/IP перед другими (например, перед стеком IPX/SPX) — более удобная система *сетевой адресации*, возможность *фрагментации пакетов* и очень небольшое количество широковещательных сообщений. Эти преимущества оказались решающими не только при построении глобальных сетей, объединяющих сети с разнородными архитектурами, но и при создании крупных корпоративных сетей. В результате сегодня стек TCP/IP практически вытеснил все остальные — он используется и в небольших домашних сетях, и в глобальной сети Интернет.

Поскольку стек TCP/IP является *общедоступным*, его стандарты (а также просто информационные материалы) публикуются в Интернете в виде специальных документов под названием «RFC» («Request for Comments», «запрос комментариев») с последовательно возрастающим номером. К примеру, спецификация протокола IP опубликована в RFC 791, а протокола HTTP версии 1.1 — в RFC 2616. Первый документ RFC был представлен еще в апреле 1969 г., а сейчас текущие номера RFC перевалили за 4 тысячи.

Стек TCP/IP, в отличие от семиуровневой модели OSI, принято описывать в рамках четырех уровней (рис. 7.1).

- *На физическом уровне* TCP/IP поддерживает работу с основными технологиями локальных сетей — Ethernet, Token Ring, Wi-Fi, Bluetooth и т. д.
- *На сетевом уровне* располагаются несколько протоколов:
  - *протокол ARP* (*Address Resolution Protocol*) является звеном, связывающим сетевой уровень с физическим. Он отвечает за преобразование сетевых IP-адресов в аппаратные MAC-адреса;

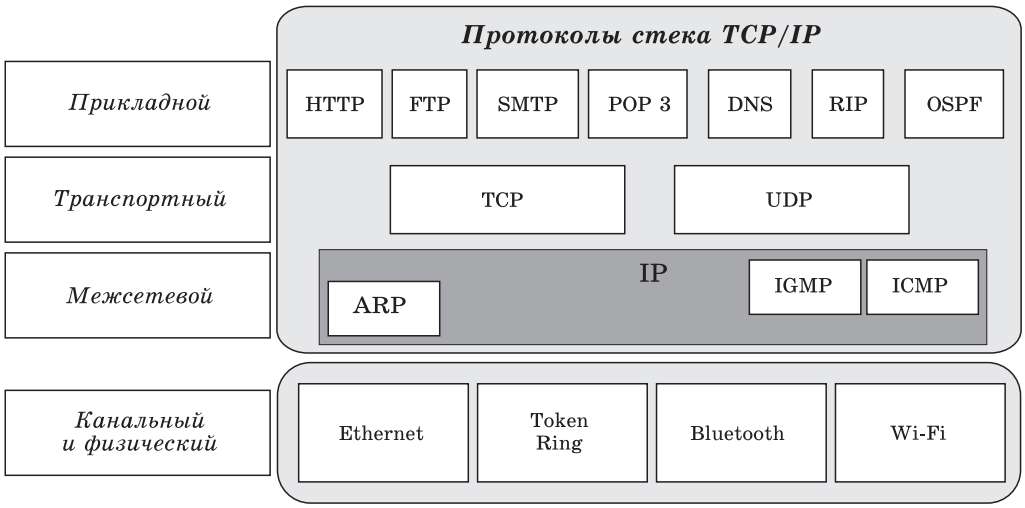


Рис. 7.1. Основные протоколы стека TCP/IP

Проверить, IP-адреса каких компьютеров вашей сети были в последнее время преобразованы в соответствующие им MAC-адреса, можно с помощью команды `ARP –A`.

- *протокол RARP* (*Reverse Address Resolution Protocol*) — осуществляет обратное преобразование MAC-адресов в IP-адреса (в операционных системах Windows поддержка протокола RARP не предусмотрена);
- *протокол ICMP* (*Internet Control Message Protocol*) — используется для передачи сообщений об ошибках, диагностики доступности сетевого узла и маршрута доставки пакетов (именно его используют такие популярные утилиты, как `PING` и `TRACERT`);
- *протокол IGMP* (*Internet Group Management Protocol*) — используется для управления группами компьютеров, например, при передаче в сетях потокового видео и звука, когда для снижения нагрузки на сеть пакет посылается по специальному адресу сразу нескольким компьютерам (*многоадресная рассылка*);

- *протокол IP* (*Internet Protocol*) — один из самых важных в стеке TCP/IP. Как следует из его названия («IP» переводится как «межсетевой протокол»), он отвечает за доставку *IP-дейтаграмм* (так правильно называются пакеты на уровне протокола IP), обеспечивая передачу пакета из одной сети в другую. О том, как это происходит, будет подробно рассказано далее.

➢ *На транспортном уровне* работают два протокола:

- *протокол TCP* (*Transmission Control Protocol*, *протокол управления передачей*) — основной протокол транспортного уровня. Обеспечивает *установку соединения* между отправителем и получателем, *разбиение* крупного *блока информации* (например, файла) *на небольшие TCP-пакеты* и их *гарантированную доставку* получателю (в нужном порядке и без ошибок). Соответственно, протокол TCP используется в тех приложениях, где важно обеспечить целостность при передаче данных;
- *протокол UDP* (*User Datagram Protocol*), в отличие от TCP, не устанавливает соединения перед передачей информации и не обеспечивает надежной доставки данных, работая при этом быстрее, чем TCP. Его используют там, где обеспечение доставки информации не особенно важно по сравнению со скоростью передачи (контроль за целостностью данных в этом случае возлагается на использующее протокол UDP приложение).

Чтобы лучше представить себе работу протоколов TCP и UDP, вернемся к нашей аналогии с почтой. Пусть вам надо переслать в издательство целый роман, а в письмо разрешается вкладывать не больше нескольких страниц текста. Чтобы в такой

ситуации ничего не потерять при пересылке и не перепутать при приеме рукописи в печать, вначале хорошо бы договориться с издательством о системах обозначения именно для вашего романа (есть ведь и другие авторы!) и о нумерации сообщений. Для этого нужно послать письмо, извещающее издательство о вашем намерении переслать роман, в котором указать исходящий номер вашего следующего сообщения. Издательство подтвердит получение вашего сообщения и в ответном письме сообщит вам свои исходящие и входящие номера, а вы подтвердите получение этих номеров. Таким образом, обе стороны согласуют номера сообщений, которые они позже будут ожидать друг от друга, что и означает установку связи. Дальше вам остается только разделить роман на небольшие части и посылать каждую в отдельном письме, а издательству — подтверждать получение этих частей. Ошибки работы почты (если какое-то сообщение не дойдет до издательства из-за потери или повреждения письма либо придет вне очереди) легко определить по входящим и исходящим номерам, чтобы принять соответствующие меры — заново переслать утерянную часть или собрать страницы романа в нужном порядке.

Примерно так же работает и протокол TCP:

- устанавливает соединение между компьютерами по определенным портам;
- на компьютере-отправителе разбивает информацию на пакеты, нумерует их и с помощью протокола IP передает получателю;
- на компьютере-получателе проверяет, все ли пакеты получены, а если пакет пропущен или поврежден, запрашивает у отправителя повторную пересылку;

- после получения всех пакетов закрывает соединение, собирает пакеты в нужном порядке и передает полученные данные приложению более высокого уровня.

Протокол же UDP в этой аналогии можно сравнить с рассылкой рекламных сообщений. Никакого установления связи и подтверждения получения корреспонденции здесь нет — письма с рекламной информацией просто бросают в ваш почтовый ящик. При этом ни отправителя, ни получателя надежность доставки информации или ее целостность, вообще говоря, не особенно беспокоят.

Очевидно, почтовые отправления в обоих этих примерах являются аналогами IP-пакетов, а почтальоны выполняют функции протокола IP.

Порт в TCP или UDP — это логический канал с определенным номером (от 0 до 65536), обеспечивающий текущее взаимодействие между отправителем и получателем. Порты позволяют компьютеру с одним IP-адресом параллельно обмениваться данными с множеством других компьютеров. Некоторые номера портов (так называемые «хорошо известные», или «well-known», порты с номерами от 0 до 1024) привязаны к определенным службам и приложениям, что позволяет клиентам легко обращаться к нужным им сетевым сервисам.

Наконец, самым богатым по набору протоколов является *прикладной уровень* стека TCP/IP. Ниже в табл. 7.1 приведены самые популярные протоколы, а также зарезервированные для них порты. Заметим, что, хотя для протоколов обычно резервируются одинаковые номера портов и для TCP, и для UDP, в таблице приведены порты для наиболее часто применяемого протокола транспортного уровня (TCP или UDP).

Таблица 7.1

Протоколы прикладного уровня стека TCP/IP

Протокол	Назначение	Номер порта
NTP (Network Time Protocol)	Протокол сетевого времени, используется для синхронизации системных часов компьютеров в сетях	123 (UDP)
DNS (Domain Name System, или Service)	Служба доменных имен, используется для преобразования (разрешения) понятных людям имен компьютеров (например, имен типа www.microsoft.com) в IP-адреса	53 (TCP и UDP)
NetBIOS name service и WINS (Windows Internet Naming Service)	Служба имен NetBIOS и служба межсетевых имен Windows, используются для преобразования NetBIOS-имен компьютеров (например, имен типа SERVER) в IP-адреса	137 и 138 (UDP)
NetBIOS session service	Служба сеансов NetBIOS, используется для установления сеансов между компьютерами	139 (TCP)
LDAP (Lightweight Directory Access Protocol)	Простой протокол доступа к каталогу, используется для работы с различными сетевыми каталогами (например, со службой Active Directory в доменах на основе Windows Server 2003)	389 (TCP)
RPC (Remote Procedure Call)	Вызов удаленной процедуры, используется для работы со многими сетевыми службами в сетях Майкрософт	135 (TCP)
Telnet	Протокол для обеспечения терминального доступа к удаленным компьютерам	23 (TCP)
FTP (File Transfer Protocol)	Протокол передачи файлов, один из «старейших» протоколов Интернета; используется для эффективной и надежной передачи файлов между клиентом и сервером FTP	20 и 21 (TCP)
TFTP (Trivial File Transfer Protocol)	Упрощенный вариант FTP, не имеет таких функций, как проверка пользователя при входе, просмотр каталогов и файлов сервера; используется только для записи и чтения файлов	69 (UDP)

Протокол	Назначение	Номер порта
Gopher	Протокол Gopher («суслик»), используется для доступа к текстовым информационным ресурсам на удаленном сервере	70 (TCP)
HTTP (HyperText Transfer Protocol)	Протокол передачи гипертекста, самый популярный сегодня протокол, используемый во Всемирной паутине (World Wide Web); описывает, каким способом нужно представлять данные (текстовые, аудио-, видео- и т. д.) на веб-серверах, как к ним обращаться с помощью веб-браузера (например, программы Internet Explorer) и как передавать эти данные	80 (TCP)
NNTP (Network News Transfer Protocol)	Протокол передачи сетевых новостей, используется для обмена сообщениями в системах телеконференций	119 (TCP)
SMTP (Simple Mail Transfer Protocol)	Простой протокол передачи почты, используется почтовыми серверами для обмена электронными сообщениями (на этапе отправки почтового сообщения его автором)	25 (TCP)
POP3 (Post Office Protocol)	«Протокол почтового отделения», довольно простой протокол, используемый почтовым клиентом (например, программой Outlook Express) для подключения к своему почтовому ящику на сервере и считывания сообщений (на этапе доставки почтового сообщения адресату)	110 (TCP)
IMAP4 (Internet Message Access Protocol)	Протокол доступа к электронным сообщениям — более функциональный, чем POP3, клиентский протокол для доступа к почтовому серверу	143 (TCP)
SSL (Secure Sockets Layer)	Протокол, обеспечивающий согласование алгоритмов и обмен ключами шифрования. Используется для защиты данных при их пересылке по сетям	25 (SMTP) 995 (POP3S) 993 (IMAPS) 443 (HTTPS) (TCP)

Несмотря на существование большого количества наборов протоколов, основным сегодня является общедоступный стек TCP/IP. Он используется практически повсеместно, начиная с небольших домашних сетей и заканчивая крупнейшей сетью — Интернетом.

Чтобы посмотреть, какие порты на вашем компьютере используются или ожидают подключения, достаточно выполнить команду `NETSTAT –AN`.

На физическом уровне стек TCP/IP поддерживает работу со всеми основными сетевыми технологиями локальных и глобальных сетей, на сетевом — обеспечивает логичную систему адресации и эффективной межсетевой маршрутизации, на транспортном уровне — протоколы как гарантированной, так и быстрой доставки данных, а на уровне приложений — целую гамму разнообразных протоколов.

Поэтому мы рекомендуем использовать в сети именно стек TCP/IP.

Вопросы для повторения

1. Что такое набор (стек) протоколов? В чем смысл термина «стек»?
2. Какие наборы протоколов вы знаете? Чем они различаются?
3. Какой стек протоколов сегодня наиболее популярен? Почему?
4. Какие уровни модели OSI поддерживаются в стеке протоколов TCP/IP?
5. В чем сходство и различие между протоколами TCP и UDP? Когда какой из этих протоколов рекомендуется использовать?
6. Перечислите известные вам протоколы прикладного уровня в стеке TCP/IP. Для чего предназначен каждый из них?
7. Что такое «порт» в TCP/IP? Для чего нужны порты?
8. Какой из транспортных протоколов стека TCP/IP вы бы использовали:
   - для пересылки по сети Интернет архивных файлов?
   - для реализации IP-телефонии (передачи голосовых сообщений в реальном времени) между пользователями двух мобильных компьютеров (КПК), соединенных по беспроводному каналу Wi-Fi?

Глава 8

Налаживаем взаимодействие между компьютерами: настройка IP-адресации и маршрутизации

В этой главе вы найдете ответы на следующие вопросы:

- ***Что такое IP-адрес, маска подсети, основной шлюз?***
- ***Как работает IP-маршрутизация?***
- ***Как «читать» таблицу маршрутизации?***
- ***Как маршрутизаторы обмениваются таблицами маршрутизации?***
- ***Как назначать IP-адреса компьютерам в сети?***
- ***Как проверить работоспособность протокола IP?***

Итак, мы выбрали набор протоколов TCP/IP и установили его (инсталлировали соответствующее программное обеспечение). Заметим, что в современных операционных системах этот протокол устанавливается по умолчанию; более того, удалить его, например, из Windows XP или Windows Server 2003 обычным способом невозможно (кнопка **Удалить** в свойствах сетевых подключений неактивна).

К сожалению, одной только установки протокола TCP/IP будет недостаточно. Стек не заработает, пока в нашей сети не будет правильным образом настроена *IP-адресация* и *маршрутизация*. (Опять сравним работу сети с работой почты: как сможет почтальон доставить письмо адресату, если дороги и транспорт хотя и работают, но на домах нет номеров, а почтовые отделения не знают, как пересылать письма из одного города в другой?)

Поэтому сейчас мы должны узнать, что такое *IP-адрес* и *маска подсети*, выяснить, как оба этих параметра используются для определения *локальных* или *удаленных IP-сетей*, и на конкретных примерах ознакомиться с тем, как компьютеры и маршрутизаторы *доставляют IP-пакеты* из одной сети в другую.

IP v6

Многие активно развивающиеся в техническом отношении страны (Китай, Япония, Корея и др.) начинают испытывать дефицит IP-адресов, идентифицирующих не только компьютеры, но и другие устройства с функциями доступа в Интернет. Принятый сейчас 32-битовый стандарт обеспечивает количество IP-адресов, равное почти 4,3 млрд., но их большая часть закреплена за США (около 70%), Канадой и европейскими странами, а вот, например, КНР получила их всего 22 млн.

Новая, 128-разрядная версия протокола IP v.6 позволит увеличить количество IP-адресов до огромной величины — $3{,}4 \times 10^{38}$.

Протокол IP v6 — в Windows XP

Для использования протокола IPv6 в Windows XP имеется необходимое программное обеспечение, которое, однако, по умолчанию не активизировано. Чтобы задействовать новый протокол, достаточно в командной строке (меню **Пуск**, **Выполнить**) ввести и запустить на исполнение команду `ipv6 install`.

Получить необходимые справки по работе с протоколом IPv6 можно (после его инсталляции) командой `ipv6 /?`.

Основы IP-адресации

Первым обязательным параметром в свойствах протокола TCP/IP любого компьютера является его IP-адрес.

IP-адрес — это уникальная 32-разрядная последовательность двоичных цифр, с помощью которой компьютер *однозначно идентифицируется* в IP-сети. (Напомним, что на канальном уровне в роли таких же уникальных адресов компьютеров выступают MAC-адреса сетевых адаптеров, невозможность совпадения которых контролируется изготовителями на стадии производства.)

В этой главе будет обсуждаться наиболее распространенная версия 4 протокола IP, или *IPv4*. Однако уже создана следующая версия протокола — *IP версии 6* (*IPv6*), в которой IP-адрес представляется в виде 128-битной последовательности двоичных цифр. Эта версия протокола IP пока еще не получила широкого распространения, хотя и поддерживается многими современными маршрутизаторами и операционными системами (например, Windows XP или Windows Server 2003).

Для удобства работы с IP-адресами 32-разрядную последовательность обычно разделяют на 4 части по 8 битов (на *октеты*), каждый октет переводят в десятичное число и при записи разделяют эти числа точками. В таком виде (это представление называется «десятичные числа с точками», или, по-английски, «*dotted-decimal notation*») IP-адреса занимают гораздо меньше места и намного легче запоминаются (табл. 8.1).

Таблица 8.1

Различные представления IP-адреса

IP-адрес в 32-разрядном виде	11000000 10101000 0000101 11001000			
IP-адрес, разбитый на октеты	11000000	10101000	00000101	11001000
Октеты в десятичном представлении	192	168	5	200
IP-адрес в виде десятичных чисел, разделенных точками	192.168.5.200			

Чтобы быстро осуществлять подобное преобразование в уме (что сетевым администраторам требуется нередко, а калькулятор не всегда под рукой), полезно запомнить следующую таблицу. В ней приведены десятичные значения степеней числа 2 с показателем, равным порядковому номеру бита в октете (напомним — нумерация битов производится справа налево и начинается с нуля):

Порядковый номер бита в октете	7	6	5	4	3	2	1	0
2 в степени, соответствующей номеру бита	128	64	32	16	8	4	2	1

Запомнив такую таблицу, несложно в уме преобразовывать октеты в десятичные числа и обратно.

Десятичное число легко вычисляется как *сумма цифр, соответствующих ненулевым битам в октете*, например:

$$\mathbf{10101101} \rightarrow \mathbf{128 \cdot 1} + 64 \cdot 0 + \mathbf{32 \cdot 1} + 16 \cdot 0 + \mathbf{8 \cdot 1} + \\ + \mathbf{4 \cdot 1} + 2 \cdot 0 + \mathbf{1 \cdot 1} = 173.$$

Несколько сложнее перевести десятичное представление в двоичное, но при некоторой тренировке это также не представляет проблем. Например:

$$201 \rightarrow \mathbf{128 \cdot 1} + \mathbf{64 \cdot 1} + 32 \cdot 0 + 16 \cdot 0 + \mathbf{8 \cdot 1} + 4 \cdot 0 + \\ + 2 \cdot 0 + \mathbf{1 \cdot 1} = \mathbf{11001001}.$$

Однако одного только IP-адреса компьютеру для работы в сети TCP/IP недостаточно. Вторым обязательным параметром, без которого протокол TCP/IP работать не будет, является *маска подсети*.

Маска подсети — это 32-разрядное число, состоящее из идущих вначале единиц, а затем — нулей, например (в десятичном представлении) `255.255.255.0` или `255.255.240.0`.

Маска подсети играет исключительно важную роль в IP-адресации и маршрутизации. Чтобы понять значение этого параметра, вспомним, что сеть ARPANet строилась как набор соединенных друг с другом гетерогенных сетей. Для правильного взаимодействия в такой сложной сети каждый участник должен уметь определять, какие IP-адреса принадлежат его *локальной* сети, а какие — *удаленным* сетям.

Здесь и используется маска подсети, с помощью которой производится *разделение любого IP-адреса* на две части: *идентификатор сети* (*Net ID*) и *идентификатор узла* (*Host ID*). Такое разделение делается очень просто: там, где в маске подсети стоят единицы, находится идентификатор сети, а где стоят нули — идентификатор узла.

Например, в IP-адресе `192.168.5.200` при использовании маски подсети `255.255.255.0` идентификатором сети будет число `192.168.5.0`, а идентификатором узла — число `200`. Стоит нам поменять маску подсети, скажем, на число `255.255.0.0`, как и идентификатор узла, и идентификатор сети изменятся на `192.168.0.0` и `5.200`, соответственно, и от этого, как мы дальше увидим, иначе будет вести себя компьютер при посылке IP-пакетов.

Правила назначения IP-адресов сетей и узлов

Теперь, когда мы знаем, что такое IP-адрес, маска подсети, идентификаторы сети и узла, полезно запомнить **правила, которые следует применять при назначении этих параметров:**

1) идентификатор сети не может содержать только двоичные нули или только единицы. Например, адрес `0.0.0.0` не может являться идентификатором сети;
2) идентификатор узла также не может содержать только двоичные нули или только единицы — такие адреса зарезервированы для специальных целей:
   - все нули в идентификаторе узла означают, что этот адрес является *адресом сети*. Например, `192.168.5.0` является правильным адресом сети при использовании маски `255.255.255.0` и его нельзя использовать для адресации компьютеров,
   - все единицы в идентификаторе узла означают, что этот адрес является *адресом широковещания* для данной сети. Например, `192.168.5.255` является адресом широковещания в сети `192.168.5.0` при использовании маски `255.255.255.0` и его нельзя использовать для адресации компьютеров;
3) идентификатор узла в пределах одной и той же подсети должен быть уникальным;
4) диапазон адресов от `127.0.0.1` до `127.255.255.254` нельзя использовать в качестве IP-адресов компьютеров. Вся сеть `127.0.0.0` по маске `255.0.0.0` зарезервирована под так называемый *«адрес заглушки»* (*loopback*), используемый в IP для обращения компьютера к самому себе.

Это легко проверить: достаточно на любом компьютере с установленным протоколом TCP/IP выполнить команду

```
PING 127.12.34.56
```

и, если протокол TCP/IP работает, вы увидите, как ваш компьютер будет отвечать на собственные запросы.

Классовая и бесклассовая IP-адресация

Первоначальная система IP-адресации в Интернете выглядела следующим образом. Все пространство возможных IP-адресов (а это более четырех миллиардов, точнее 4 294 967 296 адресов) было разбито на пять *классов*, причем принадлежность IP-адреса к определенному классу определялась по нескольким битам первого октета (табл. 8.2). Заметим, что для адресации сетей и узлов использовались только классы A, B и C. Кроме того, для этих сетей были определены *фиксированные маски подсети по умолчанию*, равные, соответственно, `255.0.0.0`, `255.255.0.0` и `255.255.255.0`, которые не только жестко определяли диапазон возможных IP-адресов узлов в таких сетях, но и механизм маршрутизации.

Таблица 8.2

Классы адресов в первоначальной схеме IP-адресации

Класс	Первые биты в октете	Возможные значения первого октета	Возможное число сетей	Возможное число узлов в сети
A	0	1–126	126	16777214
B	10	128–191	16384	65534
C	110	192–223	2097152	254
D	1110	224–239	Используется для многоадресной рассылки (multicast)	
E	1111	240–254	Зарезервирован как экспериментальный	

Чтобы рассчитать максимально возможное количество узлов в любой IP-сети, достаточно знать, сколько битов содержится в идентификаторе узла, или, иначе, сколько нулей имеется в маске подсети. Это число используется в качестве показателя степени двойки, а затем из результата вычитается два зарезервированных адреса (сети и широковещания). Аналогичным способом легко вычислить и возможное количество сетей классов A, B или C, если учесть, что первые биты в октете уже зарезервированы, а в классе A нельзя использовать IP-адреса `0.0.0.0` и `127.0.0.0` для адресации сети.

Распределением IP-адресов в мире занимается частная некоммерческая корпорация под названием ICANN (Internet Corporation for Assigned Names and Numbers), а точнее, работающая под ее патронажем организация IANA (Internet Assigned Numbers Authority).

Для получения нужного диапазона IP-адресов организациям предлагалось заполнить регистрационную форму, в которой следовало указать текущее число компьютеров и планируемый рост компьютерного парка в течение двух лет.

Первоначально данная схема хорошо работала, поскольку количество сетей было небольшим. Однако с развитием Интернета такой подход к распределению IP-адресов стал вызывать проблемы, особенно острые для сетей класса B. Действительно, организациям, в которых число компьютеров не превышало нескольких сотен (скажем, 500), приходилось регистрировать для себя целую сеть класса B. Поэтому количество доступных сетей класса B стало на глазах «таять», но при этом громадные диапазоны IP-адресов (в нашем примере — более 65000) пропадали зря.

Чтобы решить проблему, была разработана *бесклассовая схема IP-адресации* (*Classless InterDomain Routing*, *CIDR*), в которой не только отсутствует привязка IP-адреса к классу сети и маске подсети по умолчанию, но и допускается применение так называемых *масок подсети с переменной длиной* (*Variable Length Subnet Mask*, *VLSM*). Например, если при выделении сети для вышеуказанной организации с 500 компьютерами вместо фиксированной маски `255.255.0.0` использовать маску `255.255.254.0`,

то получившегося диапазона из 512 возможных IP-адресов будет вполне достаточно. Оставшиеся 65 тысяч адресов можно зарезервировать на будущее или раздать другим желающим подключиться к Интернету.

Этот подход позволил гораздо более эффективно выделять организациям нужные им диапазоны IP-адресов, и проблема с нехваткой IP-сетей и адресов стала менее острой.

IP-адреса для локальных сетей

Все используемые в Интернете адреса, как мы уже говорили, должны регистрироваться в IANA, что гарантирует их уникальность в масштабе всей планеты. Такие адреса называют *реальными*, или *публичными* (*public*) *IP-адресами*.

Для локальных сетей, не подключенных к Интернету, регистрация IP-адресов, естественно, не требуется, так что, в принципе, здесь можно использовать любые возможные адреса. Однако, чтобы не допускать возможных конфликтов при последующем подключении такой сети к Интернету, RFC 1918 рекомендует применять в локальных сетях только следующие диапазоны так называемых *частных* (*private*) *IP-адресов* (в Интернете эти адреса не существуют и использовать их там нет возможности):

- `10.0.0.0` — `10.255.255.255`;
- `172.16.0.0` — `172.31.255.255`;
- `192.168.0.0` — `192.168.255.255`.

Основы IP-маршрутизации

Как уже говорилось, чтобы правильно взаимодействовать с другими компьютерами и сетями, каждый компьютер определяет, какие IP-адреса принадлежат его локальной сети, а какие — удаленным

сетям. Если выясняется, что IP-адрес компьютера назначения принадлежит локальной сети, пакет посылается непосредственно компьютеру назначения, если же это адрес удаленной сети, то пакет посылается по адресу основного шлюза.

Рассмотрим этот процесс подробнее. Возьмем компьютер со следующими параметрами протокола IP:

- IP-адрес — `192.168.5.200`;
- маска подсети — `255.255.255.0`;
- основной шлюз — `192.168.5.1`.

При запуске протокола IP на компьютере выполняется *операция логического «И» между его собственными IP-адресом и маской подсети*, в результате которой все биты IP-адреса, соответствующие нулевым битам маски подсети, также становятся нулевыми:

- IP-адрес в 32-разрядном виде — `11000000 10101000 00000101 11001000`;
- маска подсети — `11111111 11111111 11111111 00000000`;
- идентификатор сети — `11000000 10101000 00000101 00000000`.

Эта простая операция позволяет компьютеру определить *идентификатор собственной сети* (в нашем примере — `192.168.5.0`).

Теперь предположим, что компьютеру надо отправить IP-пакет по адресу `192.168.5.15`. Чтобы решить, как это нужно сделать, компьютер выполняет *операцию логического «И» с IP-адресом компьютера назначения и собственной маской подсети*. Легко понять, что полученный в результате *идентификатор сети назначения* будет совпадать с идентификатором собственной сети компьютера-отправителя. Так наш компьютер определит, что компьютер назначения находится в одной с ним сети, и выполнит следующие операции:

- с помощью протокола ARP будет определен физический MAC-адрес, соответствующий IP-адресу компьютера назначения;
- с помощью протоколов канального и физического уровня по этому MAC-адресу будет послана нужная информация.

Теперь посмотрим, что изменится, если пакет надо отправить по адресу `192.168.10.20`. Компьютер выполнит аналогичную процедуру определения идентификатора сети назначения. В результате будет получен адрес `192.168.10.0`, не совпадающий с идентификатором сети компьютера-отправителя. Так будет установлено, что компьютер назначения находится в удаленной сети, и алгоритм действий компьютера-отправителя изменится:

- будет определен MAC-адрес не компьютера назначения, а маршрутизатора;
- с помощью протоколов канального и физического уровня по этому MAC-адресу на маршрутизатор будет послана нужная информация.

Несмотря на то, что IP-пакет в этом случае не доставляется непосредственно по назначению, протокол IP на компьютере-отправителе считает свою задачу выполненной (вспомните, что и мы при отправке письма всего лишь бросаем его в почтовый ящик). Дальнейшая судьба IP-пакета зависит от правильной настройки маршрутизаторов, объединяющих сети `192.168.5.0` и `192.168.10.0`.

Кстати, в данном примере легко продемонстрировать, насколько важна правильная настройка маски подсети в параметрах IP-адресации. Пусть мы по ошибке указали для компьютера `192.168.5.200` маску подсети, равную `255.255.0.0`. В этом случае при попытке послать пакет по адресу `192.168.10.20` наш компьютер посчитает, что компьютер назначения находится в его собственной сети (ведь идентификаторы сетей при такой маске совпадают!), и будет пытаться отправить пакет самостоятельно.

В итоге этот пакет не попадет в маршрутизатор и не будет доставлен по назначению.

Чтобы понять, как работают маршрутизаторы, давайте сначала проанализируем *таблицу маршрутов*, которую выстраивает при загрузке протокола IP обычный компьютер, например, с операционной системой Windows XP (рис. 8.1).

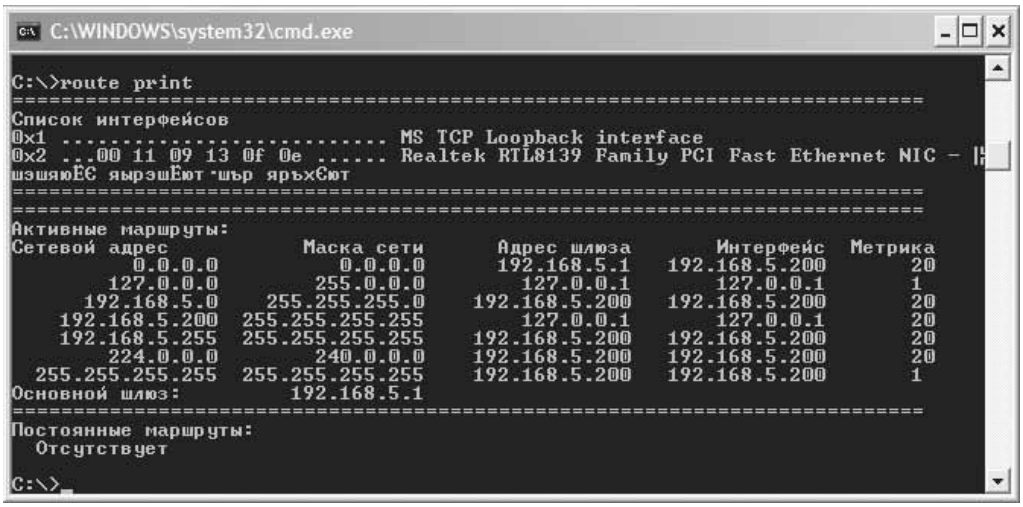


Рис. 8.1. Таблица маршрутов в ОС Windows XP

Как нетрудно видеть, в таблице определено несколько маршрутов с разными параметрами. Читать каждую такую запись в таблице маршрутизации нужно следующим образом:

> *Чтобы доставить пакет в сеть с адресом из поля* ***Сетевой адрес*** *и маской из поля* ***Маска сети****, нужно с интерфейса с IP-адресом из поля* ***Интерфейс*** *послать пакет по IP-адресу из поля* ***Адрес шлюза****, а «стоимость» такой доставки будет равна числу из поля* ***Метрика****.*

Отметим, что параметры **Сетевой адрес** и **Маска сети** вместе задают диапазон всех разрешенных в данной сети IP-адресов. Например, 127.0.0.0 и 255.0.0.0, как мы уже говорили, означают любой IP-адрес от 127.0.0.1 до 127.255.255.254. Вспомним также, что IP-адрес 127.0.0.1 называется «адресом заглушки» — посланные по этому адресу пакеты должны обрабатываться самим компьютером. Кроме того, маска 255.255.255.255 означает сеть из одного IP-адреса, а комбинация 0.0.0.0 — любой неопределенный адрес или маску подсети.

Тогда первая строка в таблице маршрутизации означает в точности то, что делает компьютер при необходимости послать пакет в удаленную, т. е. неизвестную ему из таблицы маршрутизации, сеть — со своего интерфейса пакет посылается на IP-адрес маршрутизатора.

Вторая строка таблицы заставляет компьютер посылать самому себе (и отвечать на них) все пакеты, отправленные по любому IP-адресу из диапазона 127.0.0.1 — 127.255.255.254.

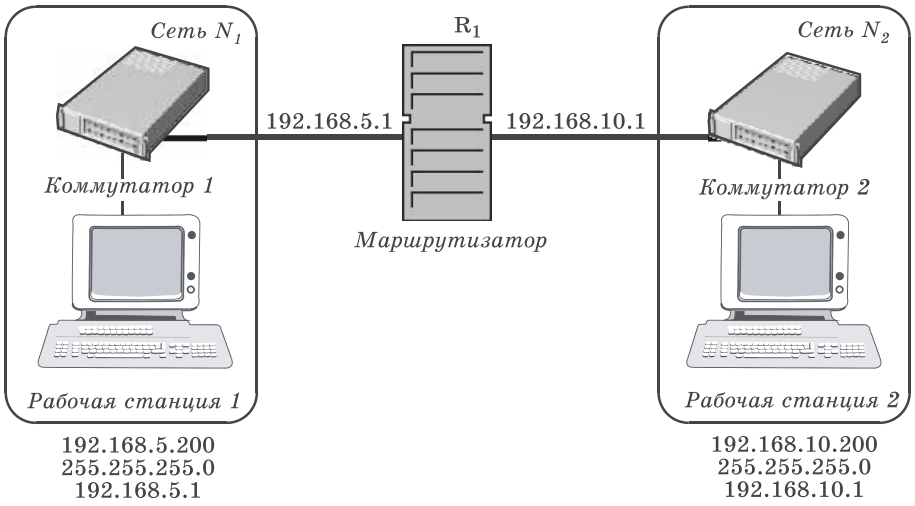
В третьей строке определено, как посылать пакеты компьютерам локальной сети (по адресам из диапазона 192.168.5.1 — 192.168.5.254). Здесь четко видно, что делать это должен сам компьютер — адресом шлюза является его собственный IP-адрес 192.168.5.200.

Аналогично (пятая, шестая и седьмая строки таблицы) нужно поступать и в случае, когда пакеты направляются по адресу рассылки подсети (192.168.5.255), по адресам многоадресной рассылки (224.0.0.0) или по адресу локальной широковещательной рассылки (255.255.255.255).

Четвертая же строка означает, что пакеты, посланные по IP-адресу 192.168.5.200 (обратите внимание на маску!), должны обрабатываться самим компьютером.

Несколько сложнее будет выглядеть таблица маршрутизации компьютера с двумя сетевыми адаптерами, который мы будем использовать в качестве маршрутизатора для объединения двух сегментов небольшой сети (рис. 8.2).

а)



б)

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.5.0    255.255.255.0      192.168.5.1     192.168.5.1      20
        192.168.5.1  255.255.255.255      127.0.0.1       127.0.0.1      20
    192.168.5.255  255.255.255.255      192.168.5.1     192.168.5.1      20
     192.168.10.0    255.255.255.0    192.168.10.1    192.168.10.1      20
     192.168.10.1  255.255.255.255      127.0.0.1       127.0.0.1      20
   192.168.10.255  255.255.255.255    192.168.10.1    192.168.10.1      20
        224.0.0.0        240.0.0.0      192.168.5.1     192.168.5.1      20
        224.0.0.0        240.0.0.0    192.168.10.1    192.168.10.1      20
  255.255.255.255  255.255.255.255      192.168.5.1     192.168.5.1       1
  255.255.255.255  255.255.255.255    192.168.10.1    192.168.10.1       1
```

Рис. 8.2. Объединение сети с помощью маршрутизатора (*а*) и таблица маршрутизации компьютера R_1 (*б*)

В этой таблице появилось несколько дополнительных строк, обозначающих маршруты в обе сети — `192.168.5.0` и `192.168.10.0`. Заметим, что все такие маршруты будут выстроены компьютером автоматически.

Чтобы после этого наладить *обмен IP-пакетами между сетями*, нужно выполнить следующие действия:

- включить маршрутизацию на компьютере R_1 — это можно сделать, например, настроив службу маршрутизации и удаленного доступа, входящую в состав операционной системы Windows Server 2003;
- на всех компьютерах в сети N_1 параметр **Основной шлюз** нужно установить равным IP-адресу интерфейса маршрутизатора, подключенного к этой сети, т. е. равным `192.168.5.1`, а на компьютерах в сети N_2 — равным `192.168.10.1`.

Таким образом, маршрутизатор — это программно-аппаратное устройство с несколькими сетевыми интерфейсами, на котором работает *служба маршрутизации*.

Усложним нашу сеть, добавив в нее второй маршрутизатор и сеть N_3 с адресом `192.168.15.0` (рис. 8.3).

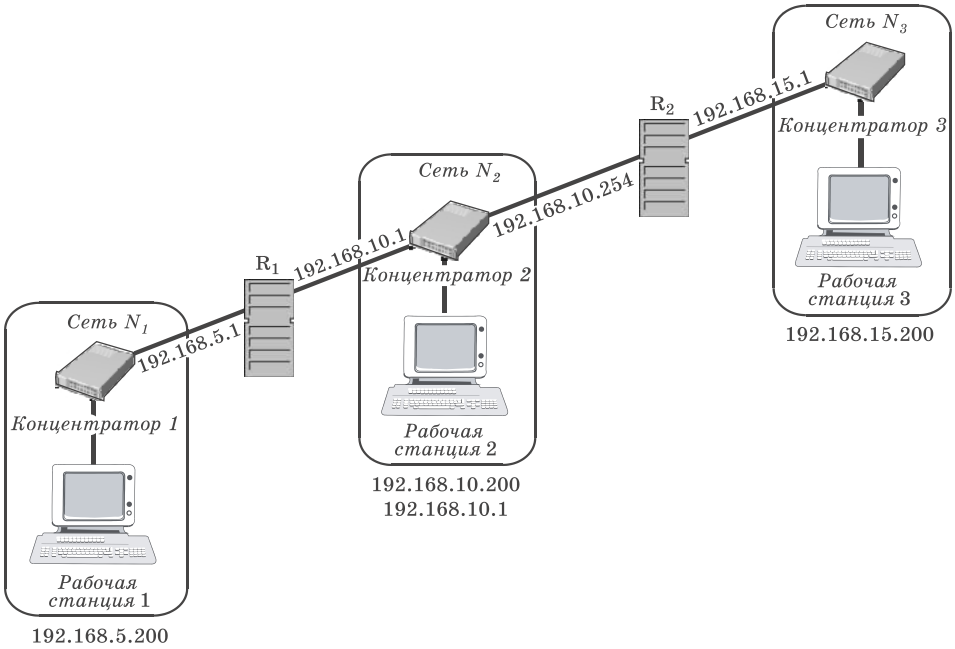


Рис. 8.3. Сеть с двумя маршрутизаторами

В такой сети настройка маршрутизации усложняется. Проблема в том, что, хотя маршрутизатор R_1 «знает», как посылать пакеты в сети N_1 и N_2, маршрута в сеть N_3 у него нет. В свою очередь, у маршрутизатора R_2 отсутствует маршрут в сеть N_1. Значит, обмен IP-пакетами между сетями N_1 и N_3 будет невозможен.

Решить эту проблему в такой небольшой сети довольно просто — надо добавить нужные записи в таблицы маршрутизаторов R_1 и R_2. Для этого на маршрутизаторе R_1 достаточно выполнить команду, предписывающую направлять все пакеты, предназначенные для сети `192.168.15.0`, по адресу `192.168.10.254` (т. е. второму маршрутизатору, который уже сможет доставить эти пакеты по назначению; ключ `P` здесь используется, чтобы сделать этот маршрут постоянным):

```
ROUTE –P ADD 192.168.15.0
      MASK 255.255.255.0 192.168.10.254
```

В качестве IP-адреса маршрутизатора принято выбирать либо первый, либо последний из возможных в данной IP-сети адресов.

Аналогичная команда на маршрутизаторе R_2 должна выглядеть так:

```
ROUTE –P ADD 192.168.5.0
        MASK 255.255.255.0 192.168.10.1
```

После этого взаимодействие в нашей сети будет налажено.

В крупных сетях, содержащих большое количество соединенных друг с другом подсетей, вручную прописывать маршруты доставки пакетов на всех маршрутизаторах довольно утомительно. К тому же такие маршруты являются *статическими*, значит, при каждом изменении конфигурации сети нужно будет проделывать большую работу по перестройке системы IP-маршрутизации.

Чтобы избежать этого, достаточно настроить маршрутизаторы так, чтобы они *обменивались друг*

с другом информацией о маршрутах. Для этого в локальных сетях используют такие протоколы, как *RIP* (*Routing Information Protocol*) и *OSPF* (*Open Shortest Path First*). Протокол RIP проще в настройке, чем OSPF, однако для обмена информацией в нем применяются широковещательные сообщения, заметно нагружающие сеть. Поэтому RIP обычно используют в относительно небольших сетях. Протокол OSPF работает эффективнее, но сложнее настраивается, поэтому его использование рекомендуется для крупных корпоративных сетей.

Назначение IP-адресов и проверка работоспособности TCP/IP

Мы уже видели, насколько важной для взаимодействия компьютеров в сети TCP/IP является правильная настройка протокола IP. Поэтому важно обсудить, какими способами можно настраивать параметры IP на компьютерах и как быстро проверить работоспособность всей системы IP-адресации и маршрутизации.

Самый простой способ настройки параметров протокола IP — назначить их вручную. Достоинством такого метода является то, что сетевые администраторы полностью контролируют все IP-адреса компьютеров в сети, что может быть важно с точки зрения защиты данных или взаимодействия с Интернетом. Однако у этого способа много недостатков. Во-первых, легко ошибиться и ввести неправильные параметры маски или шлюза или, что еще хуже, назначить повторяющийся в сети IP-адрес. Во-вторых, при изменениях параметров IP-адресации в сети (например, при смене IP-адреса маршрутизатора) придется перенастраивать все компьютеры. Но самое неприятное, что при таком способе настройки практически невозможно работать в крупных кор-

поративных сетях с мобильными устройствами типа ноутбуков или КПК, которые часто перемещаются из одного сегмента сети в другой.

Поэтому в организациях чаще применяют специальные серверы, поддерживающие *протокол динамической конфигурации узлов* (*Dynamic Host Configuration Protocol*, *DHCP*), задача которых состоит в обслуживании запросов клиентов на получение IP-адреса и другой информации, необходимой для правильной работы в сети. Именно поэтому компьютеры с операционными системами Windows по умолчанию настроены на автоматическое получение IP-адреса.

Если сервер DHCP недоступен (отсутствует или не работает), то начиная с версии Windows 98 компьютеры самостоятельно назначают себе IP-адрес. При этом используется *механизм автоматической личной IP-адресации* (*Automatic Private IP Addressing*, *APIPA*), для которого корпорацией Microsoft в IANA был зарегистрирован диапазон адресов `169.254.0.0` — `169.254.255.255`.

Наконец, обсудим, какие шаги нужно предпринять *для проверки параметров и работоспособности протокола IP*.

1. **Выполните команду `IPCONFIG /ALL`.**

   Если в выданной на экран информации не содержится никаких параметров, значит, у вас нет активных интерфейсов.

   Если в выданной информации есть диагностическое сообщение «Сеть отключена», значит, у вас проблемы с физическим уровнем — проверьте подключение коннектора в разъеме сетевого адаптера и/или работоспособность коммутатора.

   Если ваши параметры IP-адреса и маски подсети равны `0.0.0.0`, значит, вы используете статический IP-адрес, конфликтующий с другим узлом в сети.

Если ваш IP-адрес находится в диапазоне `169.254.x.x`, значит, DHCP-сервер недоступен и работать вы сможете только с теми компьютерами в сети, которые также самостоятельно назначили себе адрес.

В нормальной ситуации при получении IP-адреса от DHCP-сервера или правильной ручной настройке вы должны увидеть в выданной на экран информации такие параметры, как IP-адрес компьютера, маска подсети, основной шлюз, DNS-сервер и DHCP-сервер (а также, возможно, другие параметры).

2. **Выполните команду `PING 127.0.0.1`.**

   Если ответ не получен, это свидетельствует о неправильной настройке стека протоколов TCP/IP; придется переустановить соответствующую программную поддержку.

   Если ответ получен, значит, стек протоколов TCP/IP работает правильно.

3. **Выполните команду `PING` *`w.x.y.z`*, где *`w.x.y.z`* — IP-адрес соседнего компьютера.**

   Так проверяется работоспособность локальной сети.

4. **Выполните команду `PING` *`w.x.y.z`*, где *`w.x.y.z`* — IP-адрес основного шлюза.**

   Так проверяется доступность и работоспособность маршрутизатора.

5. **Выполните команду `PING` *`w.x.y.z`*, где *`w.x.y.z`* — IP-адрес любого удаленного компьютера.**

   Так проверяется работоспособность всей системы маршрутизации вашей корпоративной сети или соединения с Интернетом.

Во многих современных сетях пакеты протокола ICMP, с помощью которых утилита `PING` тестирует взаимодействие, запрещаются по требованию служб безопасности. ОС Windows XP SP2 с включенным

межсетевым экраном также блокирует ICMP-пакеты. Поэтому, если утилита PING не показывает ответов, не спешите искать причину «сбоя» на своем компьютере, а сначала выясните у сетевого администратора (или в настройках своей ОС Windows XP), разрешено ли в вашей сети использование ICMP.

В заключение приведем набор кратких правил, которые помогут вам не ошибиться при настройке IP-адресации и маршрутизации в сетях TCP/IP:

1) чтобы взаимодействовать в сети TCP/IP, все компьютеры должны иметь IP-адреса;
2) компьютеры, находящиеся в одном физическом сегменте сети (соединенные концентраторами или коммутаторами), должны принадлежать одной IP-сети, но иметь уникальные IP-адреса;
3) для определения идентификаторов локальной сети или удаленных сетей используется маска подсети;
4) чтобы взаимодействовать с удаленными сетями, компьютерам требуется адрес основного шлюза, который должен совпадать с адресом маршрутизатора, соединяющего вашу сеть с другими;
5) маршрутизаторы — это компьютеры с несколькими сетевыми интерфейсами, умеющие передавать IP-пакеты из одной сети в другую в соответствии со своими таблицами маршрутизации;
6) маршрутизатор всегда имеет маршруты во все сети, подключенные к нему непосредственно; маршруты в другие сети нужно настраивать;
7) таблицы маршрутизации можно настраивать вручную либо применять динамические протоколы обмена информацией о маршрутизации.

Вопросы и задания

1. Какие параметры и настройки обязательны для обеспечения работы стека протоколов TCP/IP?
2. Что такое IP-адрес? Какова его структура? Какие возможны способы представления IP-адресов?
3. Чем отличаются версии 4 и 6 протокола IP? Какие преимущества обеспечит версия 6 протокола IP? Почему возникла необходимость в переходе на версию 6 протокола IP?
4. Что такое маска подсети? Для чего она нужна?
5. В чем заключается смысл разделения IP-адреса на идентификаторы сети и узла? Для чего это требуется?
6. Какие IP-адреса и маски являются допустимыми, а какие — нет? Почему?
7. В чем различие между классовой и бесклассовой IP-адресациями? Каковы их преимущества и недостатки?
8. Что такое классы IP-адресов? По каким правилам они определяются?
9. Как назначить IP-адреса в локальной сети (без выхода в Интернет)?
10. Каковы основные принципы маршрутизации пакетов в локальных и удаленных сетях?
11. Что такое таблица маршрутов (таблица маршрутизации)? Объясните смысл каждой из ее колонок.
12. Как «прописать» в таблице маршрутизации отсутствующий в ней новый маршрут?
13. Что такое динамическая конфигурация узлов? Для чего она нужна?
14. В чем заключается технология автоматической личной IP-адресации?
15. Каков типовой алгоритм проверки работоспособности протокола IP?

Глава 9

Налаживаем работу в сети: сетевые службы, клиенты, серверы, ресурсы. Защита при работе в сети

В этой главе вы найдете ответы на следующие вопросы:

- ***Для чего нужна сетевая операционная система?***
- ***Какие функции выполняют клиентские и серверные сетевые операционные системы?***
- ***Какие службы обеспечивают взаимодействие клиентских операционных систем в сетях Microsoft?***
- ***Какие существуют типы серверов?***
- ***Как строится система безопасности в современных сетевых ОС?***
- ***Какие меры защиты рекомендуется соблюдать при работе в сети?***

Итак, наша сеть заработала. Компьютеры объединены с помощью коммутаторов, точек доступа и, возможно, маршрутизаторов, везде установлен протокол TCP/IP и корректно настроены параметры IP.

Теперь нужно научиться работать в сети. Для этого нам потребуются *сетевые операционные системы* (ОС), с помощью которых пользователи смогут обмениваться информацией друг с другом, совместно работать с данными, использовать общие ресурсы и т. д.

Сетевые ОС можно разделить на *клиентские*, такие как Windows 2000 Professional, Windows XP Home Edition или Windows XP Professional, и *серверные*, например Windows Server 2003.

Основная функция клиентской сетевой ОС — предоставить пользователю удобный интерфейс для работы с сетевыми приложениями и службами, обеспечив при этом максимальную защиту компьютера и безопасность при доступе к данным и ресурсам. Серверы же выполняют сервисные функции, предоставляя свои данные и ресурсы для совместного использования, а также обслуживая различные клиентские запросы.

Какие же сервисы используются операционными системами для работы в сети? Начнем с клиентских операционных систем. Если посмотреть список

компонентов, используемых сетевыми подключениями ОС Windows 2000 Professional, то, кроме протокола TCP/IP, обеспечивающего межсетевые и транспортные функции, можно увидеть еще два сервиса: *Служба доступа к файлам и принтерам сетей Microsoft* и *Клиент для сетей Microsoft*. Эти две службы неразрывно связаны друг с другом: первая используется для предоставления каталогов и принтеров в общий доступ, вторая — для подключения к ним по сети.

В операционной системе Windows XP дополнительно предоставляется *Планировщик пакетов QoS* (Quality of Service) — служба, позволяющая *резервировать* некоторую часть общей полосы пропускания сетевого подключения, а затем *выделять* ее для таких приложений, где задержки недопустимы (например, при передаче по сети видеоизображения и речи при видеоконференцсвязи).

Таким образом, даже в клиентской ОС по умолчанию предусмотрена серверная служба доступа к файлам и принтерам. Эта служба позволяет в домашних или небольших офисных сетях обходиться без использования серверов (напомним: такие сети называются *одноранговыми*, или *рабочими группами*). Количество компьютеров в них обычно не превышает 10 (кстати, именно такое количество подключений является максимальным для клиентских ОС Windows). Компьютеры в одноранговых сетях обычно подключаются к одному концентратору или коммутатору, маршрутизаторы не используются. Чтобы обнаружить соседей, компьютеры применяют широковещательные сообщения, и никакие системы преобразования имен в IP-адреса при этом не требуются.

В крупных сетях без серверов уже не обойтись. Более того, чтобы удовлетворить постоянно возрастающим потребностям корпоративных пользователей, приходится постоянно повышать количество и

функциональность серверов, расширять их аппаратные возможности. Многие серверы приходится делать *специализированными* — предназначенными для поддержки конкретных служб или приложений. Другие, не очень сложные сервисы, наоборот, можно *объединять* (*консолидировать*) в рамках одного мощного аппаратного сервера.

Рассмотрим основные типы серверов.

- **Серверы, обеспечивающие работу в сети TCP/IP, или серверы сетевой инфраструктуры.** К ним относятся DHCP-, DNS- и WINS-серверы; обычно настройку работы в крупной сети начинают именно с них:

  - *DHCP-серверы* уже упоминались в прошлой главе. Они нужны, чтобы по запросу *DHCP-клиента* (компьютера, у которого в настройках протокола TCP/IP включен режим автоматического получения IP-адреса) выдать ему такие параметры, как уникальный IP-адрес и маска подсети. Кроме них, клиент может получать от DHCP-сервера ряд дополнительных параметров, важных для взаимодействия с другими сетями и удобной работы в сети: адрес основного шлюза, адреса DNS- и WINS-серверов, название домена, в который входит этот компьютер, и некоторые другие;

Под сервером в разных случаях может пониматься как собственно компьютер, так и установленное на нем специализированное программное обеспечение, либо весь этот программно-аппаратный комплекс в целом.

  - *DNS-серверы* выполняют очень важную функцию *преобразования (разрешения) имен узлов* (*host names*) *в соответствующие им IP-адреса*. Напомним: DNS (Domain Name System) расшифровывается как «система (служба) доменных имен». Служба DNS была реализована в Интернете в 1981 г., а с 2000 г. (с выходом ОС семейства Windows 2000) она стала основной службой преобразования имен в сетях Microsoft;

- *WINS-серверы* регистрируют в сети NetBIOS-имена компьютеров и их IP-адреса, а затем по запросу *WINS-клиентов* преобразуют эти имена в IP-адреса. Название WINS (Windows Internet Name Service) правильно переводится как «служба межсетевых имен Windows»; эта служба была разработана, чтобы обеспечить поддержку работы *NetBIOS- приложений* в маршрутизируемых сетях на базе протокола TCP/IP. Сейчас она по-прежнему используется, чтобы в сети корректно работали такие устаревшие ОС, как Windows 9*x* или Windows NT.

Напомним, что компьютеры для взаимодействия друг с другом используют IP-адреса. Человеку же с числовыми IP-адресами работать неудобно, поэтому при работе в сетях обычно используются словесные имена компьютеров. (Впрочем, в подавляющем большинстве приложений можно и непосредственно применять IP-адреса; иногда это удобный способ проверки работоспособности приложения, особенно если системы разрешения имен в данной сети не работают.)

Имена компьютеров при этом возможны двух типов:

- *имена узлов* — состоят из комбинаций букв, цифр и знака дефиса, разделенных точками. Это могут быть имена компьютеров как в Интернете (пример: `www.microsoft.com`), так и в локальной сети (`server1.domain.local`);
- *NetBIOS-имена* — «собственные» имена компьютеров, содержащие не более 15 любых символов, кроме точек (например, `SERVER1`).

➢ **Серверы файлов (файл-серверы)** нужны для хранения больших объемов данных и предоставления к ним доступа пользователей. Один файловый сервер может поддерживать одновременную работу сотен и

даже тысяч пользователей. Чтобы обеспечить сохранность информации, файл-серверы, как правило, оснащены отказоустойчивыми наборами (массивами) жестких дисков и системами резервного копирования на магнитную ленту или другой носитель.

- **Серверы печати (принт-серверы)** предназначены для обеспечения доступа пользователей к одному или нескольким общим принтерам. Они принимают по сети задания на печать, поступающие от пользовательских приложений, и управляют *очередями заданий на печать*, обычно обслуживая несколько печатающих устройств.

  Похожие функции выполняют и **факс-серверы**, обслуживающие клиентские задания на отправку факсов, но они, кроме того, отвечают за получение факсов и их доставку пользователям.

Файл-серверы и серверы печати — это одни из наиболее часто встречающихся типов серверов.

- **Серверы приложений** выполняют задачи обслуживания запросов пользователей на выборку или обработку какой-либо информации; их часто объединяют с **серверами баз данных**. Важно, что с серверами приложений и баз данных одновременно может работать большое число пользователей, причем выполнение клиентских запросов на специализированном многопроцессорном сервере производится намного быстрее, чем на компьютерах пользователей.

- **Серверы удаленного доступа** и **серверы VPN** (Virtual Private Network — «виртуальная частная сеть») обеспечивают удаленное подключение к локальной сети по модему или через Интернет. Это дает пользователям возможность работать с ресурсами локальной сети предприятия, офиса или учебного заведения из дома или из любого места, где есть подключение к Интернету, например из Интернет-кафе.

- **Терминальные серверы** предоставляют возможность работы с другими серверами через специальные программы — *терминальные клиенты*. С помощью этих программ администраторы, находясь вдалеке от локальной сети, оказываются как будто за консолью сервера и могут полностью управлять им, а пользователи могут удаленно работать с установленными на сервере приложениями.
- **Брандмауэры (межсетевые экраны)** используются при подключении к Интернету для защиты внутренней сети от проникновения или атаки злоумышленников на корпоративные серверы. **Прокси-серверы (серверы-посредники)** выполняют функции контроля доступа пользователей в Интернет и кэширования часто запрашиваемых веб-страниц (что позволяет снизить расходы на пользование Интернетом). Поскольку оба этих сервера предназначены для установки на компьютер, связывающий локальную сеть с Интернетом, их часто объединяют в единую программно-аппаратную систему.
- **Серверы электронной почты (почтовые серверы, mail-серверы)** обслуживают почтовые ящики пользователей в данной организации, обеспечивая подключения к ним *почтовых клиентов*, а также обрабатывают все входящие и исходящие сообщения. Их также можно использовать для ведения адресных книг, общих папок и систем электронного документооборота.
- **Веб- и FTP-серверы** предоставляют для внешних (а часто — и для внутренних) пользователей доступ к веб- и FTP-ресурсам, размещенным в данной сети.
- **Контроллеры домена** обеспечивают в сетях Microsoft работу служб *Активного каталога* (Active Directory) и поддерживают базу данных всех зарегистрированных в *домене* пользователей, компьютеров, групп и ресурсов. Наличие такой базы данных

позволяет администраторам централизованно управлять всеми сетевыми объектами и ресурсами. Пользователи же получают возможность входить в сеть с любого принадлежащего домену компьютера, а затем «прозрачно» (без ввода имени и пароля) подключаться к другим компьютерам и работать с их ресурсами.

Этот список далеко не полон, существуют и другие типы серверов. Однако перечисленные выше их разновидности можно найти практически в любой корпоративной сети.

Основы безопасности при работе в сетях

В те времена, когда компьютеры не были объединены в сети или подключены к Интернету, о безопасности данных можно было особенно не заботиться. Достаточно было обеспечить *физическую защиту* компьютера и контролировать доступ посторонних пользователей к устройствам записи (например, к дисководам).

После объединения компьютеров в сети все изменилось — без серьезной защиты теперь уже не обойтись, иначе и операционная система, и хранящиеся на компьютере или передаваемые по сети данные могут стать легкой добычей злоумышленников, причем так, что работающие на этом компьютере пользователи ничего не заметят. Поэтому далее мы изучим основные принципы, используемые при построении современных сетевых ОС, обсудим главные угрозы, представляющие опасность для компьютеров, пользователей и их данных, а также укажем простейшие правила обеспечения безопасности, которые обязательно следует соблюдать при работе в сети.

Принципы построения защищенных ОС:

- все современные ОС являются *многопользовательскими* — они рассчитаны на работу в системе (в том числе одновременную) нескольких пользователей;
- чтобы отличить одного пользователя от другого, применяются *учетные записи* (accounts) с уникальными *именами* и *паролями*;
- учетные записи различаются *уровнем полномочий* (*привилегий*, *прав*) — набором действий, которые обладатель данной учетной записи может выполнять в системе. Обычно учетные записи разделяют на *административные*, обладающие максимальными привилегиями, и *пользовательские*, набор полномочий для которых позволяет нормально работать в системе, но не разрешает выполнять какие-либо критичные с точки зрения безопасности данных операции, например форматировать разделы жесткого диска или менять настройки сети.

В обсуждаемых нами версиях ОС Windows дополнительно существуют учетные записи с уровнем прав, средним между административным и пользовательским (участники группы «Опытные пользователи»), а также обладающие минимальными полномочиями *гостевые учетные записи* (участники группы «Гости», включая встроенную учетную запись «Гость»).

Кроме того, существует два типа учетных записей — *локальные* из базы данных конкретного компьютера с ОС Windows, и *глобальные учетные записи в домене*, которые хранятся на контроллерах домена (подробнее о них будет сказано далее);

- для входа в компьютер обязательно нужно указать имя и пароль учетной записи, зарегистрированной в системе. Следует подчеркнуть, что понятие «вход в систему» подразумевает

не только непосредственный доступ, но и другие возможности работы с компьютером, например *сетевой* или *терминальный* вход, для которых также требуются пользовательские имя и пароль.

В операционных системах Windows допускается также сетевой вход без указания имени и пароля (*анонимный* вход); такие подключения используются при некоторых взаимодействиях в сетях Microsoft;

- после входа в систему (интерактивного, сетевого и т. д.) пользователь получает доступ к ресурсам того компьютера, в который он вошел (например, доступ к локальным файлам или каталогам). Уровень доступа при этом определяется *списком разрешений*, т. е. возможных действий, которые данный пользователь может осуществлять с защищенным объектом. Например, один пользователь может изменить или удалить файл, другой — только прочитать его, а третьему вообще будет отказано в доступе к этому файлу.

Рабочие группы и домены

Мы уже неоднократно упоминали *рабочие группы* и *домены*. Давайте разберем, чем принципиально отличаются эти две модели сетевого взаимодействия в сетях Microsoft.

Рабочая группа — это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети. Принципиально важно, что каждый компьютер в рабочей группе *равноправен* (т. е. сеть получается одноранговой) и *поддерживает собственную локальную базу данных учетных записей пользователей* (*Security Accounts Manager*, *SAM*).

Отсюда вытекает основная проблема, которая не позволяет использовать рабочие группы в крупных корпоративных сетях. Действительно, если вспомнить, что вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой — удаленным), то, например, пользователю, вошедшему на компьютер `Comp1` под локальной учетной записью `User1`, будет отказано в доступе к принтеру, установленному на компьютере `Comp2`, поскольку в его локальной базе нет пользователя с именем `User1` (рис. 9.1). Таким образом, для обеспечения «прозрачного» взаимодействия в рабочей группе нужно *создавать одинаковые учетные записи с одинаковыми паролями на всех компьютерах*, где работают пользователи и расположены ресурсы.

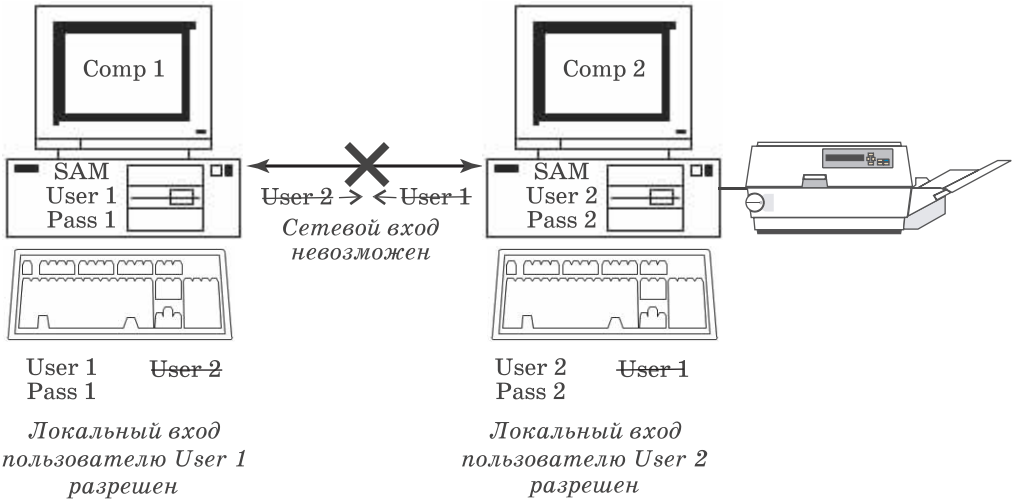


Рис. 9.1. Локальный и сетевой вход в систему в рамках рабочей группы

В ОС Windows XP Professional для рабочих групп предусмотрен специальный режим: «Использовать простой общий доступ к файлам», позволяющий обойти указанную проблему (данный режим включен по умолчанию). В этом случае подключение к любому сетевому компьютеру осуществляется от имени его локальной гостевой учетной записи, которая включается с помощью *Мастера настройки сети* (по умолчанию она отключена) и для которой настраивается нужный уровень доступа.

Для ОС Windows XP Home Edition этот способ сетевого взаимодействия является основным и отключить его нельзя (поэтому компьютеры с данной ОС невозможно сделать участниками домена).

Понятно, что управлять учетными записями и ресурсами в рабочей группе можно только при небольшом количестве компьютеров и пользователей. В крупных сетях следует применять домены.

Домен — это логическая группировка компьютеров, объединенных *общей базой данных пользователей и компьютеров, политикой безопасности и управления.*

Домены создаются на основе сетевых ОС Windows, а база данных, как мы уже говорили, поддерживается *контроллерами домена*. Важным в доменах является то, что все компьютеры здесь не сами осуществляют проверку пользователей при входе, а передоверяют эту процедуру контроллерам (рис. 9.2). Такая организация доступа позволяет легко осуществить однократную проверку пользователя при входе в сеть, а затем уже без проверки предоставлять ему доступ к ресурсам всех компьютеров домена.

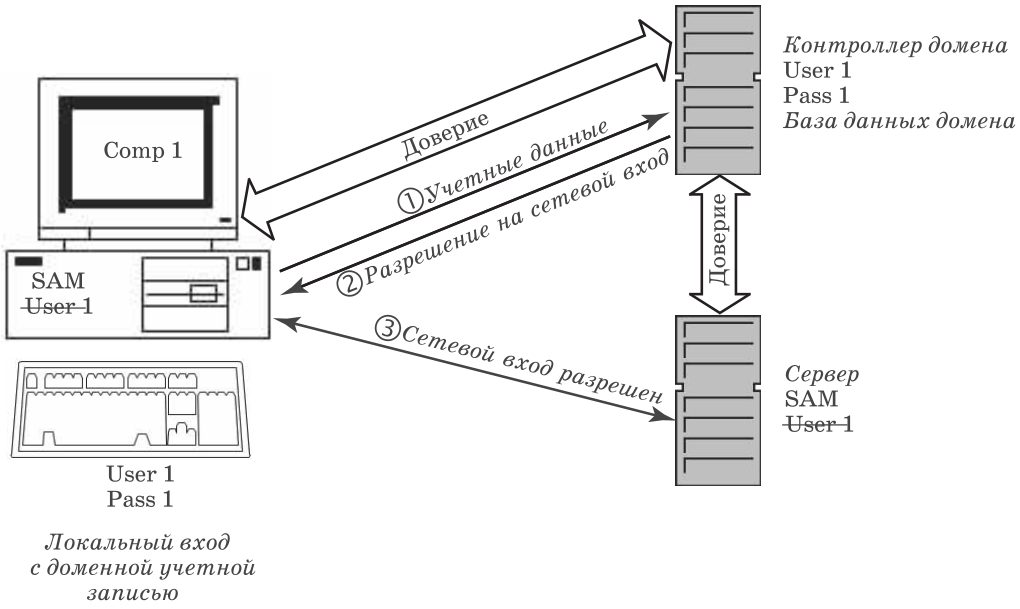


Рис. 9.2. Локальный и сетевой вход в домене

Основные угрозы при работе в сети

Угроз, поджидающих пользователей при подключении компьютера к сети, довольно много. Мы приведем только основные из них:

- *«взлом» компьютера* обычно производится с целью захвата контроля над операционной системой и получения доступа к данным;
- *повреждение системы* чаще всего организуется, чтобы нарушить работоспособность (вызвать отказ в обслуживании — «Denial of Service») каких-либо сервисов или компьютера (чаще сервера) целиком, а иногда — даже всей сетевой инфраструктуры организации;

«Троянские» программы получили свое название «в честь» знаменитого «троянского коня», придуманного хитроумным Одиссеем, чтобы захватить Трою. Типичная «троянская» программа обычно «маскируется» под какую-либо полезную утилиту (или может быть спрятана в какой-либо программе), а если пользователь по незнанию запустит ее на выполнение, такая программа начинает контролировать компьютер, открывая создателю «троянской программы» доступ к данным (так называемый «backdoor» — «черный ход»), похищая и пересылая ему набираемые с клавиатуры пароли и т. п.

- *кража данных* из-за неправильно установленных прав доступа, при передаче данных или «взломе» системы позволяет получить доступ к защищаемой, часто — конфиденциальной информации со всеми вытекающими отсюда неприятными для владельца этих данных последствиями;
- *уничтожение данных* имеет целью нарушить или даже парализовать работу систем, компьютеров, серверов или всей организации.

Атаки на компьютеры или серверы, вирусы, «черви», шпионские и «троянские» программы — все это злонамеренное ПО пишется для того, чтобы осуществить в той или иной степени перечисленные выше угрозы.

Основные меры безопасности при работе в сети довольно просты. Их можно сформулировать в виде следующего набора правил:

- отключайте компьютер, когда вы им не пользуетесь. Как любят говорить эксперты по компьютерной безопасности, «самым защищенным является выключенный компьютер, хранящийся в банковском сейфе»;
- своевременно обновляйте операционную систему. В любой ОС периодически обнаруживаются так называемые «*уязвимости*», снижающие защищенность вашего компьютера. Наличие уязвимостей нужно внимательно отслеживать (в том числе читая «компьютерную» прессу или информацию в Интернете), чтобы вовремя предпринимать меры для их устранения.

Для ОС Windows корпорацией Microsoft создан специальный веб-узел Windows Update, обратившись к которому (например, с помощью программы WUPDMGR.EXE или команды **Windows Update** в меню **Пуск**), нетрудно просмотреть и скачать список *обновлений*, рекомендуемых для вашего компьютера;

- используйте ограниченный набор хорошо проверенных приложений, не устанавливайте сами и не разрешайте другим устанавливать на ваш компьютер программы, взятые из непроверенных источников (особенно из Интернета). Если приложение больше не нужно, удалите его;
- без необходимости не предоставляйте ресурсы своего компьютера в общий доступ. Если же это все-таки потребовалось, обязательно настройте минимально необходимый уровень доступа к ресурсу только для зарегистрированных учетных записей;
- установите (или включите) на компьютере *персональный межсетевой экран* (*брандмауэр*). Если речь идет о корпоративных сетях, установите брандмауэры как на маршрутизаторах, соединяющих вашу локальную сеть с Интернетом, так и на всех компьютерах сети;
- обязательно установите на компьютер специализированное антивирусное и «антишпионское» программное обеспечение. Настройте его на автоматическое получение обновлений как минимум один раз в неделю (лучше — ежедневно или даже несколько раз в день);
- даже если вы единственный владелец компьютера, для обычной работы применяйте *пользовательскую учетную запись*: в этом случае повреждение системы, например, при заражении вирусом, будет неизмеримо меньше, чем если бы вы работали с правами администратора. Для всех учетных записей, особенно административных, установите и запомните сложные пароли.

Сложным считается пароль, содержащий случайную комбинацию букв, цифр и специальных символов, например `jxg1rg$N`. Разумеется, пароль не

должен совпадать с именем вашей учетной записи. В операционных системах Windows сложный пароль можно *сгенерировать* автоматически, используя команду NET USER с ключом /RANDOM, например:

```
NET USER Имя_Пользователя /RANDOM
```

Пароль в виде случайной последовательности символов нелегко запомнить, поэтому часто используют следующую технику — пароль набирается в английской раскладке русскими буквами. Например, слово «Пароль» тогда будет выглядеть как «Gfhjkm». Однако этот способ следует применять с осторожностью — взломщики давно имеют целые словари подобным образом преобразованных слов, так что желательно вставлять в такие пароли специальные символы и цифры.

Пароли для доступа в различные системы должны быть разными. Недопустимо использовать один и тот же пароль для администрирования вашего компьютера и для входа, например, на игровой веб-сайт;

«Фишинг» («рыбная ловля») — так называется распространенный сегодня вид мошенничества в Интернете. Злоумышленники создают сайты, внешне похожие на сайты Интернет-магазинов, банков и пр., а затем «заманивают» на них посетителей (например, с помощью рекламных баннеров) и предлагают «подтвердить свои персональные данные». Иногда злоумышленники с той же целью рассылают электронные письма якобы от имени администрации почтового сервера с просьбой «подтвердить пароль доступа к почтовому ящику».

- при работе с электронной почтой никогда сразу не открывайте вложения, особенно полученные от неизвестных отправителей. Сохраните вложение на диск, проверьте его антивирусной программой и только затем откройте. Если есть такая возможность, включите в вашей почтовой программе защиту от потенциально опасного содержимого и отключите поддержку HTML;
- при работе с веб-сайтами соблюдайте меры разумной предосторожности: старайтесь избегать регистрации, не передавайте никому персональные сведения о себе и внимательно работайте с Интернет-магазинами и другими службами, где применяются онлайновые способы оплаты с помощью кредитных карт или систем типа WebMoney, Яндекс-Деньги и т. д.

При резервном копировании полезно использовать утилиты для создания «образов» жесткого диска (такие, как Norton Ghost). Резервную копию можно снять с «системного» жесткого диска после правильной установки на него всех требуемых программ и антивирусной проверки и хранить ее на другом жестком диске (сетевом или съемном), чтобы в случае повреждения системы быстро восстановить ее работоспособность.

При проведении оплаты убедитесь, что соединение защищено шифрованием с помощью технологии *Secure Sockets Layer* (*SSL*) — в этом случае адресная строка обязательно должна начинаться с «`https://`»;

- перечисленные выше меры лишь повышают общую защищенность системы и данных, но не дают никакой гарантии от их повреждения или даже полной потери. Поэтому обязательно следует создавать *резервные копии* системы и данных на съемном жестком диске или на DVD-RW — это позволит вам легко восстановить их в случае утери. При этом одну копию имеет смысл хранить вне дома, например, в сейфе;
- исключительно важную роль играет обучение всех пользователей основам безопасной работы в сетях — как в домашних, так и в корпоративных, — ведь нарушение правил одним пользователем ставит под угрозу всю систему защиты.

Итак, для работы в сети нужны сетевые операционные системы, которые принято делить на клиентские и серверные. Клиентские ОС отличаются небольшим набором служб, но включают в себя спектр сетевых приложений. Серверные системы бывают различных типов и предназначены для обслуживания тех или иных запросов сетевых клиентов.

Для организации работы в сетях Microsoft применяются две модели: рабочие группы, используемые при небольшом числе компьютеров, и домены, позволяющие легко объединять большое число пользователей, рабочих станций и серверов.

Все сетевые ОС и хранящиеся на компьютерах данные должны быть надежно защищены, причем желательно, чтобы применяемая система безопасности была многоуровневой.

Вопросы и задания

1. Для чего нужны сетевые операционные системы? Чем они отличаются от «несетевых»? Какие возможны типы сетевых операционных систем?
2. Чем различаются клиентские и серверные сетевые операционные системы?
3. Какие сетевые сервисы и службы предоставляются в Windows 2000 и XP?
4. Какие возможны виды серверов? Каково их назначение? Чем они различаются?
5. В чем заключается проблема безопасности при работе в сети? Чем она вызвана?
6. Каковы принципы организации работы пользователей в защищенных ОС?
7. В чем заключается *авторизация* (идентификация) пользователей? Как она реализуется?
8. Какие возможны виды учетных записей? Какая информация входит в учетную запись? Какие права доступа могут обеспечиваться для пользователя учетной записи в ОС Windows?
9. Что такое рабочая группа? Что такое домен? В чем заключается их основное различие?
10. Каковы основные угрозы при работе в сети? Каковы, по вашему мнению, основные причины (мотивы), побуждающие злоумышленников осуществлять подобные действия?
11. Каковы основные правила (меры) безопасности при работе в сети?
12. Какие дополнительные меры безопасности, по вашему мнению, необходимы при работе в сети (в частности, в Интернете) несовершеннолетних? Как вы организовали бы работу с Интернетом для своего ребенка на своем домашнем компьютере? в школьном компьютерном классе?

Глава 10

Подключаем сеть к Интернету. Начинаем работать в сети

В этой главе вы найдете ответы на следующие вопросы:

- ***Какие возможны способы доступа в Интернет?***
- ***Как в Интернете решается проблема нехватки реальных IP-адресов?***
- ***Что такое транслятор сетевых адресов?***
- ***Как построена и как работает система DNS?***
- ***Как построена и как работает Всемирная паутина (WWW)?***
- ***Как создаются веб-сайты?***
- ***Как работать с веб-браузером?***
- ***Как работать с веб-браузером?***

Теперь, когда наша сеть полностью настроена и защищена, можно подключить ее к Интернету. Напомним, что Интернет — это весьма агрессивная среда, так что настраивать соединение с ним без надежного обеспечения безопасности в локальной сети более чем рискованно. В этой главе мы изучим основные способы доступа в Интернет (на физическом и канальном уровне), обсудим, как подобное подключение осуществляется на сетевом уровне и как решаются вопросы разрешения имен на сеансовом уровне. Вы узнаете также, какая служба в Интернете наиболее популярна, как она организована и какие программы прикладного уровня используются для работы с ней.

Начнем с выбора *способа доступа в Интернет*. Их сейчас предлагается очень много.

- *Аналоговые модемы* в нашей стране до сих пор остаются самыми распространенными устройствами, обеспечивающими домашним пользователям связь с Интернетом. Их популярность объясняется широкой доступностью телефонных каналов как среды передачи данных и их дешевизной (недорогой внутренний модем стоит сегодня примерно 350–400 руб.). Недостатки использования модемов — сравнительно низкая скорость передачи (теоретически — не больше

Слово «модем» — это сокращение от названия «МОдулятор-ДЕМодулятор», прекрасно описывающее принцип функционирования данного устройства. На одной стороне телефонной линии модем преобразует (*модулирует*) полученные от компьютера цифровые сигналы в аналоговые (в звуковые сигналы — хорошо знакомый всем пользователям модемов «шум») и передает их модему на другой стороне линии, где происходит обратное преобразование (*демодуляция*).

В Москве наиболее известным примером реализации доступа в Интернет по технологии ASDL является интернет-канал СТРИМ, предоставляемый интернет-оператором «МТУ-Интел».

56 Кбит/с, реально еще меньше) и занятость домашней телефонной линии при работе в Интернете. В корпоративной среде аналоговые модемы в настоящее время применяются редко, в основном только в мелких офисах небольших фирм.

- *Цифровые модемы различных типов — xDSL-, ISDN- и кабельные модемы*. Из приведенного списка наибольшую популярность в последнее время получили *ADLS-модемы* (*Asymmetric Digital Subscriber Line*). В них скорость передачи данных из Интернета на клиентский компьютер («скачивание», download) выше, чем скорость передачи данных от клиентского компьютера в Интернет (отправка, upload), поэтому они хорошо подходят большинству домашних пользователей и даже небольшим организациям, подключающимся к Интернету. При не очень высокой стоимости ADSL-модемы обеспечивают намного большую, по сравнению с аналоговыми, скорость передачи данных (например, в ADSL2+ входящий поток данных может достигать скорости 24 Мбит/с, исходящий — 1 Мбит/с), а в качестве физической среды используются все те же телефонные линии (однако эти линии должны быть современными, поэтому даже в Москве ADSL-связь доступна не везде). Еще одним существенным преимуществом ADLS-модемов перед обычными является то, что они благодаря использованию более высокой частоты передачи сигналов не мешают обычной телефонии, что весьма важно для домашних пользователей (при работе в Интернете телефон остается свободным для разговоров).

ISDN-модемы еще несколько лет назад были одним из самых распространенных способов решения «*проблемы последней мили*», т. е. непосредственного подключения организаций к Интернету. Однако вследствие довольно высокой стоимости они сейчас применяются все реже и реже.

Кабельные модемы позволяют подключаться к Интернету через системы кабельного телевидения, отличаются сравнительно невысокой ценой и способны обеспечить скорость связи до нескольких десятков Мбит/с. Однако провайдеров Интернет-услуг по кабельным сетям в России совсем немного.

Подключения к Интернету при помощи модема бывают *коммутируемыми*, когда для работы используется обычная телефонная линия, и *постоянными* — в этом случае для них требуется так называемая *выделенная линия*. Выделенные линии раньше часто использовались организациями для обеспечения модемной связи с Интернетом, но сейчас их осталось немного.

- Многие коллективные домашние и крупные корпоративные сети используют *постоянное подключение к Интернету*. Такое подключение физически может осуществляться различными способами, от модемных подключений по выделенным линиям до спутниковых или наземных радиоканалов. В последнее время в городах большинство крупных абонентов (предприятия и домашние сети) используют обычное Ethernet-подключение к Интернету, где в качестве среды передачи применяются оптоволоконные каналы. Такой способ, конечно, обходится достаточно дорого, но зато обеспечивает максимальную скорость и надежность связи.

- В последнее время становятся все более популярными беспроводные технологии подключения к Интернету, такие как GPRS, Wi-Fi или WiMAX. Их главное преимущество — возможность работы с Интернетом на различных *мобильных компьютерах* (ноутбуках, карманных компьютерах (КПК), «смартфонах» и пр.) без »привязки» к конкретному рабочему месту. Такой способ доступа сегодня часто реализован в аэропортах, ресторанах, кафе и других общественных местах, где организуются *общедоступные «Wi-Fi-зоны»*; его все чаще начинают использовать в учебных заведениях и крупных организациях для обеспечения

Многие современные модели сотовых телефонов содержат в себе встроенный модем и позволяют дозвониться к любому провайдеру, дополнительно оплачивая время соединения по обычным тарифам сотовой связи. В отличие от этого, *технология GPRS* предполагает оплату только *трафика* — объема принятой информации, вне зависимости от длительности работы в Интернете.

сотрудникам возможности работы в локальной сети и/или в Интернете при сохранении полной свободы перемещения по территории «Wi-Fi-зоны».

Технология GPRS (*General Packet Radio Service*) обеспечивает полноценный доступ в Интернет по сетям сотовой связи. При этом мобильный телефон подключается к компьютеру (обычно — к ноутбуку или КПК) при помощи кабеля через порт USB (реже — через порт COM) либо беспроводным способом (при помощи Bluetooth или инфракрасной связи) и фактически выполняет роль модема, работающего со скоростью до 170 кбит/с. Современные же модели сотовых телефонов и «смартфоны» (устройства, сочетающие в себе функции мобильного телефона и карманного компьютера) позволяют работать с Интернетом через GPRS при помощи встроенного программного обеспечения (программ для обмена электронной почтой, браузеров и пр.).

Технология Wi-Fi обеспечивает возможность доступа в Интернет путем соединения с *беспроводной точкой доступа*, подключенной к серверу локальной сети с выходом в Интернет или непосредственно к кабельному Интернет-каналу, на расстоянии в несколько сотен метров.

Технология WiMAX в настоящее время активно развивается как за рубежом, так и в России. Она во многом аналогична Wi-Fi, но, в отличие от нее, обеспечивает связь с точками доступа (*базовыми станциями*) на больших расстояниях — порядка нескольких миль. Поэтому технология WiMAX представляет собой весьма перспективное решение для России, обладающей значительными территориями (особенно в сельской местности), в том числе не оснащенными телефонной связью.

Подключение на сетевом уровне

Напомним, что для работы в Интернете все компьютеры должны иметь *уникальные публичные IP-адреса*.

Поэтому нам желательно знать, какими способами обеспечивается *подключение к Интернету на уровне протокола IP*.

Как уже говорилось, первоначально всем подключавшимся к Интернету компьютерам выделялись *реальные IP-адреса*, а само такое подключение, естественно, осуществлялось с помощью обычных *маршрутизаторов*. Этот способ взаимодействия с Интернетом был самым простым, эффективным и к тому же обеспечивал быстрый доступ *ко всем компьютерам Интернета*. Однако у него была и «обратная сторона медали». Во-первых, требовалось большое количество публичных IP-адресов, что приводило к все возрастающему их дефициту и довольно крупным счетам за пользование Интернетом (так как большинству коммерческих организаций приходилось оплачивать каждый адрес для каждого компьютера). Но самое главное — все компьютеры локальной сети становились *доступными* для всего остального Интернета, а значит — легко *уязвимыми*. Последнее обстоятельство стало особенно очевидным в ноябре 1988 г., когда первый компьютерный «червь» Морриса вывел из строя каждый десятый (!) компьютер тогдашнего Интернета, на пару дней практически полностью парализовав работу Сети.

Для обеспечения защиты при подключении к Интернету локальных сетей с реальными IP-адресами на маршрутизаторах обычно настраивают так называемые *IP-фильтры* (или *списки доступа*, *IP Access Lists*), которые разрешают пересылать во внутреннюю сеть пакеты только к определенным компьютерам и только по определенным протоколам.

Чтобы решить обе проблемы — защиты локальных сетей и нехватки реальных IP-адресов — с 90-х гг. стала интенсивно применяться уже разработанная к тому времени *технология трансляции сетевых адресов* (*Network Address Translation*, *NAT*; см. RFC 1631 от 1984 г.). При ее использовании у провайдера можно получить *единственный* публичный IP-адрес

(хотя обычно их получают несколько, чтобы иметь возможность публиковать внутренние почтовые и веб-серверы под разными реальными IP-адресами). Этот IP-адрес назначается *внешнему интерфейсу NAT-маршрутизатора*, используемого для подключения сети к Интернету.

Во внутренней же сети применяются IP-адреса, разрешенные для локальных сетей (например, из диапазона `192.168.0.0`), так что в пределах сети организации компьютеры взаимодействуют по IP совершенно нормально.

Однако *непосредственная работа с Интернетом при использовании внутренних адресов невозможна* (вспомните, что пакеты с IP-адресами источника из диапазонов для локальных сетей в Интернет *не маршрутизируются*). Поэтому NAT-маршрутизатору при отправке каждого IP-пакета в Интернет нужно заменить (*транслировать*) IP-адрес источника (т. е. адрес внутреннего компьютера) в разрешенный, маршрутизируемый интернетовский IP-адрес, которым является один из адресов его внешнего интерфейса. Пакет уходит в Интернет с реальным IP-адресом и, следовательно, доставляется по назначению — например, доходит до веб-сервера. Сервер же в Интернете отвечает на запрос пакетом, в котором в качестве IP-адреса назначения указан адрес внешнего интерфейса NAT-маршрутизатора, и этот пакет также доставляется без проблем. Получив его из Интернета, NAT-маршрутизатор производит обратное преобразование, заменяя IP-адрес назначения в пакете (т. е. адрес своего внешнего интерфейса) адресом требуемого внутреннего компьютера, после чего отправляет пакет во внутреннюю сеть (рис. 10.1).

В результате внутренний и внешний компьютеры «считают», что общаются друг с другом непосредственно, «не подозревая» о существовании посредника, роль которого выполняет маршрутизатор с поддержкой NAT.

Среди преимуществ использования NAT основным является то, что внешние компьютеры ничего

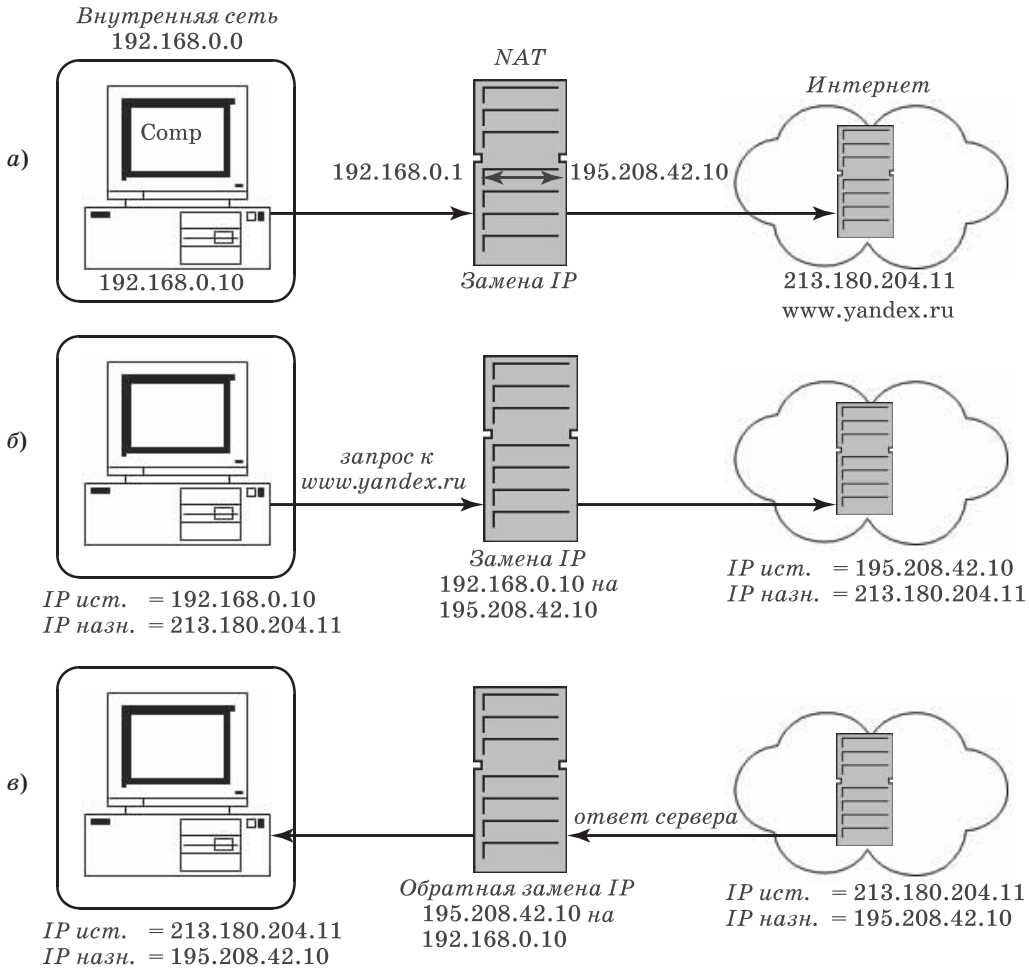


Рис. 10.1. Работа транслятора сетевых адресов при взаимодействии с Интернетом

«не знают» о внутренней системе IP-адресации, применяемой в локальной сети, и *не могут напрямую получить доступ к находящимся в ней компьютерам*. Это делает технологию NAT очень привлекательной именно для обеспечения защиты локальных сетей.

Как же все это работает для разных типов подключений? При использовании модемов все достаточно просто. После установки связи с модемом *провайдера* — поставщика услуг Интернета (*ISP*, *Internet Service Provider*) клиентский модем автоматически получает *один из реальных IP-адресов*, зарегистрированных провайдером (заметим, что некоторые провайдеры выдают клиентам IP-адреса, предназначенные для локальных сетей, а затем применяют NAT-маршрутизаторы).

Важно!

Чтобы в такой ситуации защитить свой компьютер от «взлома» и потери данных, следует *обязательно пользоваться персональным брандмауэром*, включив его в свойствах вашего модемного подключения к Интернету.

Если при этом в свойствах модемного подключения на компьютере с ОС Windows 2000 или XP разрешить *общий доступ к подключению к Интернету* (*Internet Connection Sharing*, *ICS*), то ваш компьютер становится еще и маршрутизатором с поддержкой NAT, обеспечивающим *взаимодействие всей домашней сети с Интернетом*. Сетевому интерфейсу при этом назначается IP-адрес `192.168.0.1`, и на вашем компьютере начинают работать *службы DHCP* и *DNS-прокси*. Первая из них выдает всем остальным компьютерам домашней сети такие параметры, как IP-адрес из диапазона `192.168.0.0`, маску подсети (`255.255.255.0`), адрес шлюза (`192.168.0.1`) и адрес DNS-сервера (`192.168.0.1`), а вторая — обслуживает запросы DNS-клиентов из домашней сети, пересылая их серверу DNS провайдера. Более того, предоставляется возможность обеспечить доступ из Интернета к внутренним компьютерам, например, чтобы опубликовать в Интернете ваш домашний веб- или почтовый сервер.

Подобным образом работает и подавляющее большинство современных скоростных модемов, применяемых в домашних сетях и небольших организациях. Как правило, они являются *гибридными устройствами* (*шлюзами*), объединяющими в себе функциональность модемов и NAT-маршрутизаторов, а некоторые — еще и выступают в качестве беспроводных точек доступа и брандмауэров.

При подключении же к Интернету крупных коллективных домашних или корпоративных сетей используют в основном *коммутаторы третьего уровня* или *маршрутизаторы*, а защиту внутренней сети организуют с помощью специализированных *полнофункциональных брандмауэров* (конечно, с поддержкой NAT). В отличие от персональных межсетевых экранов, такие брандмауэры могут осуществлять контроль передаваемых данных не только на уровне IP-фильтров или установленных соединений TCP, но и на более высоком уровне приложений. Например, они умеют анализировать команды таких протоколов, как HTTP, FTP или SMTP, и блокировать передачу данных, если используются запрещенные команды. Часто такие брандмауэры объединяют с *прокси-серверами*.

Доменная система имен (DNS) в Интернете

Мы уже говорили о том, что компьютеры в Интернете (их принято называть *узлами*) используют для взаимодействия числовые IP-адреса, тогда как людям удобнее работать со словесными именами. Чтобы в сетевых приложениях можно было применять словесные имена, требуется *механизм преобразования имен в IP-адреса*.

Таких способов возможно два: можно использовать текстовый файл, в котором записывать все соответствия имен IP-адресам, а можно воспользо-

Файл HOSTS, только уже без расширения, до сих пор существует и работает во всех операционных системах Windows, поддерживающих протокол TCP/IP (его можно найти в каталоге %Windir%\System32\Drivers\Etc). Правда, по умолчанию он содержит только одну запись, связывающую имя localhost с адресом 127.0.0.1.

ваться специальной службой — *системой DNS*. Первоначально, когда узлов в Интернете было еще не так много, применялся именно файл с именем HOSTS.TXT, который поддерживался сетевым центром Стэнфордского университета (Stanford Research Institute's Network Information Center). Изменения в него (фактически — *регистрация* имен компьютеров) вносились только там, а затем этот файл скачивался на все остальные узлы Интернета.

Когда в начале 80-х гг. начался бурный рост числа узлов Интернета, такая система просто перестала нормально работать — в файл приходилось постоянно вносить изменения, добавляя все новые и новые узлы, да и копирование измененных файлов на все узлы в Интернете занимало все больше и больше времени.

В результате было принято решение отказаться от единого файла и перейти к *распределенной базе данных имен*, в которой были выделены *зоны ответственности*. Такая система получила название *DNS* (*Domain Name System*), она имеет древовидную структуру, в соответствии с которой строится структура самих доменных имен (рис. 10.2).

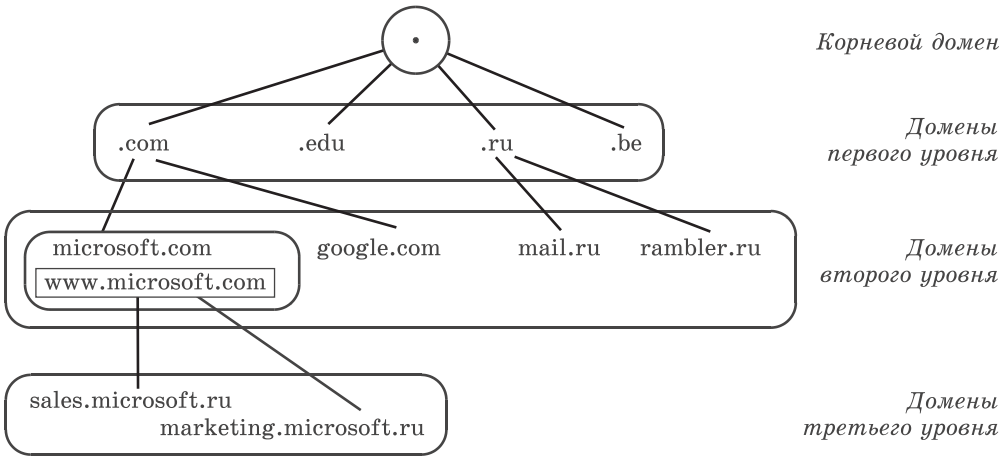


Рис. 10.2. Пример структуры доменных имен

Разумеется, крупные фирмы вовсю стремятся заполучить «престижные» доменные имена, отражающие их название или сферу деятельности. Иногда это приводит к курьезам: например, ничем не примечательное островное государство Тувалу, недавно получившее собственный домен верхнего уровня (tv), вполне может стать главным «экспортером» (с весьма немалым ежегодным доходом) доменных имен более низких уровней для сайтов телекомпаний и иных фирм «телевизионного бизнеса».

С тех пор *сетевой информационный центр* (теперь он носит название «InterNIC») отвечает только за «корень» системы (его обычно обозначают одной точкой — «.» и в именах узлов просто опускают), за соответствующие *корневые серверы* (*Root Servers* или *Root Hints*) и за регистрацию *доменов верхнего уровня* (*Top Level Domains*, *TLD*). Домены верхнего уровня обычно именуются по типам организаций, в частности, для США (com — для коммерческих, edu — для образовательных, gov — для правительственных и т. д.), или по странам (ru — Россия, be — Бельгия и пр.).

Ниже располагаются *домены второго уровня*, регистрируемые в доменах верхнего уровня, и в них уже допускается регистрация как узлов, так и *дочерних доменов* (*SubDomain*). При этом важно, что администратор, зарегистрировавший, скажем, домен company.ru, имеет *полные права на свой домен* — может создавать дочерние домены и регистрировать узлы без уведомления доменов верхних уровней. Однако он отвечает за правильное функционирование системы DNS в рамках своей зоны ответственности.

Служба DNS работает весьма эффективно. Для нахождения любого зарегистрированного в DNS компьютера (например, www.company.ru) достаточно обратиться к одному из *корневых серверов*, который возвратит список DNS-серверов, отвечающих за домен .ru. Запрос к ним позволит выяснить список DNS-серверов, поддерживающих домен company.ru, обратившись к которым можно будет уже выяснить IP-адрес компьютера www.company.ru. Именно такой алгоритм действий применяется для большинства DNS-серверов при *разрешении имен*.

Всемирная паутина (World Wide Web)

Теперь, когда наша сеть построена, защищена, подключена к Интернету и настроена для работы с именами узлов, нам остается только узнать, какие *службы* предоставляет нам Интернет и какие программы нужно использовать для работы с этими службами.

Начнем с самого популярного сегодня сервиса Интернета — *Всемирной паутины*, или *World Wide Web* (*WWW, W*^{3}). Заметим, что WWW является только одной из множества служб, работающих в Интернете, однако именно из-за нее к Интернету подключается подавляющее большинство пользователей (многие из них даже полагают, что понятия «WWW» и «Интернет» совпадают).

Основы WWW были заложены в конце 80-х гг. XX века в Европейском центре ядерных исследований (CERN) в Женеве. Служба WWW задумывалась как универсальная среда, с помощью которой ученые могли бы быстро обмениваться информацией любого типа; среда, в которой *ссылки* могли бы указывать на *гипертекстовые объекты*, находящиеся *в любом месте нашей планеты*. В результате были разработаны сама система WWW, *язык разметки веб-страниц HTML* (*HyperText Markup Language*) и *способ адресации с помощью универсального идентификатора ресурса* (*URL*, *Uniform Resource Locator*). Кроме того, была создана первая *программа просмотра веб-страниц* (*браузер*), первый *веб-сервер* и разработан *протокол их взаимодействия — HTTP* (*HyperText Transfer Protocol*). В 1991 г. все это было опубликовано в Интернете для свободного использования.

World Wide Web можно определить как *распределенную информационную систему*, основанную на *гипертексте*. Слово «распределенная» в данном случае означает, что данные, которые отображаются вашим веб-браузером, могут располагаться как на соседнем компьютере, так и на сервере на другом

В Интернете существуют специальные *общедоступные серверы для размещения веб-сайтов* (*хостинга*), например Narod.Ru или Chat.Ru. Здесь (после выполнения несложной процедуры регистрации) любой желающий может бесплатно получить возможность разместить свой собственный сайт.

конце земного шара. Например, в пределах *веб-страницы*, размещенной на одном сервере, может отображаться рисунок, хранящийся на совершенно другом сервере, на который в исходном тексте веб-страницы (на языке HTML) сделана соответствующая ссылка с указанием точного адреса размещения этого рисунка.

Информация в WWW представляется в виде *веб-страниц*, которые могут содержать обычный текст, или же *гипертекст*, а также *практически любые другие данные*, в том числе графику, музыкальные или видео-ролики. Кроме того, на веб-страницах могут размещаться *ссылки* на другие веб-страницы, хранящиеся на том же самом или на любом другом сервере в Интернете.

Ссылки на веб-страницах отображаются как выделенный (обычно цветом и подчеркиванием) текст или как графические изображения (рис. 10.3). Если навести на ссылку указатель мыши, он из стрелки обычно преобразуется в изображение «руки с поднятым указательным пальцем». Любая такая ссылка реализует *переход* к другому гипертекстовому документу, который может оказаться не просто веб-страницей, а, например, исполняемой программой или мультимедийным файлом; тогда щелчок мышью по ссылке открывает этот документ.

Рис. 10.3. Типичная ссылка на веб-странице

Веб-страницы размещаются в WWW на *веб-серверах* в виде связанных друг с другом наборов, называемых *сайтами*. Сайты могут принадлежать какому-либо конкретному лицу или организации и поддерживаются разработчиками (*веб-мастерами*).

При обращении к веб-сайту всегда открывается его *главная страница*, иногда также называемая

домашней (*home page*). Главная страница (рис. 10.4) — это почти то же самое, что обложка журнала или первая страница газеты. Обычно на ней публикуется наиболее привлекательная информация (иногда — просто картинка или мультимедийный ролик), символизирующая содержание сайта. Для удобства работы на главной странице часто размещают колонку оглавления, *карту сайта*, либо *навигационную панель*, позволяющие посетителям сайта быстро найти требуемую информацию.

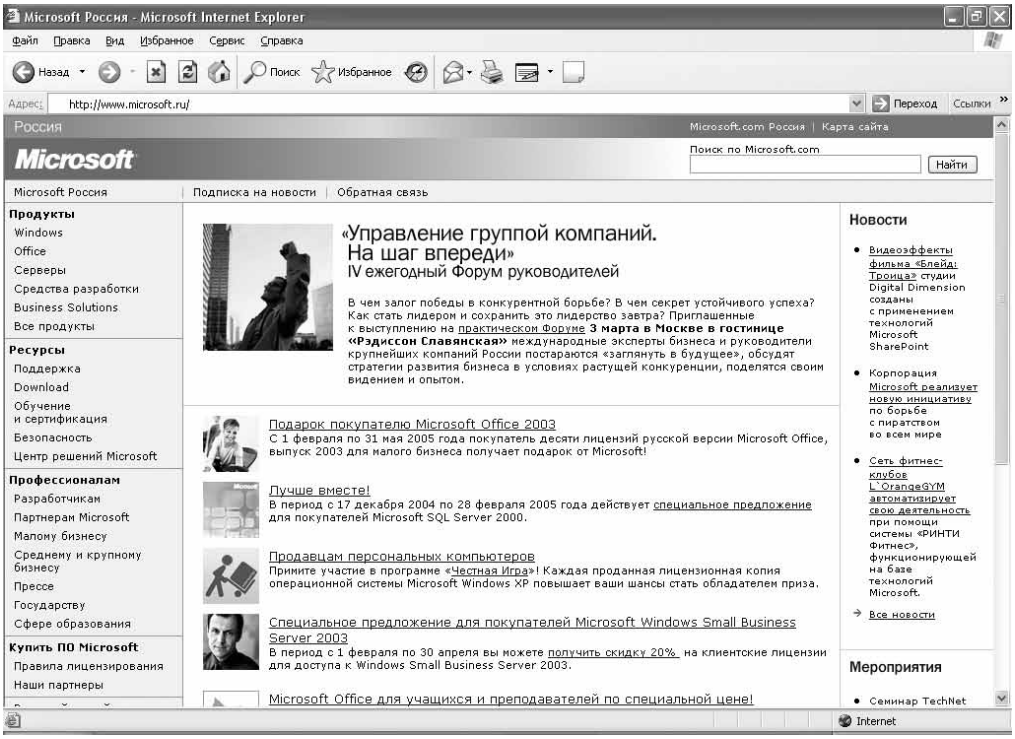


Рис. 10.4. Пример главной страницы сайта корпорации Microsoft

Страницы веб-сайтов обычно структурируют одним из следующих трех способов: линейным, древовидным или произвольно.

Линейный веб-сайт (*Linear Web Site*) подобен обычной книге: вы начинаете с первой (главной) страницы, затем переходите ко второй, третьей, четвертой и так далее (рис. 10.5). Такие сайты удобны тем, что в них трудно «заблудиться» — вы всегда можете легко вернуться не только к предыдущей и следующей страницам, но и, если это предусмотрено создателями сайта, к любой другой. Такой способ представления информации часто используют, чтобы последовательно провести читателя по целой серии связанных друг с другом материалов или статей.

Рис. 10.5. Линейный веб-сайт

Веб-сайт с древовидной структурой (*Tree Web Site*) организован подобно «генеалогическому древу». Вы начинаете с главной страницы, а затем можете выбрать один из нескольких *разделов* сайта (рис. 10.6). Такая структура характерна для сайтов многопрофильных организаций или компаний (например, производителей программного обеспечения или оборудования, которые хотели бы представить различные линейки своей продукции), для Интернет-магазинов, торгующих разнообразными товарами, и пр. Типичным примером такой организации сайта является веб-сайт корпорации Microsoft (`www.microsoft.com`).

Веб-сайт с произвольной структурой (*Random Web Site*) практически не имеет четкой организации и часто представляет собой хаотичный массив информации, соединенной перекрестными ссылками. Вы можете переходить со страницы на страницу, но

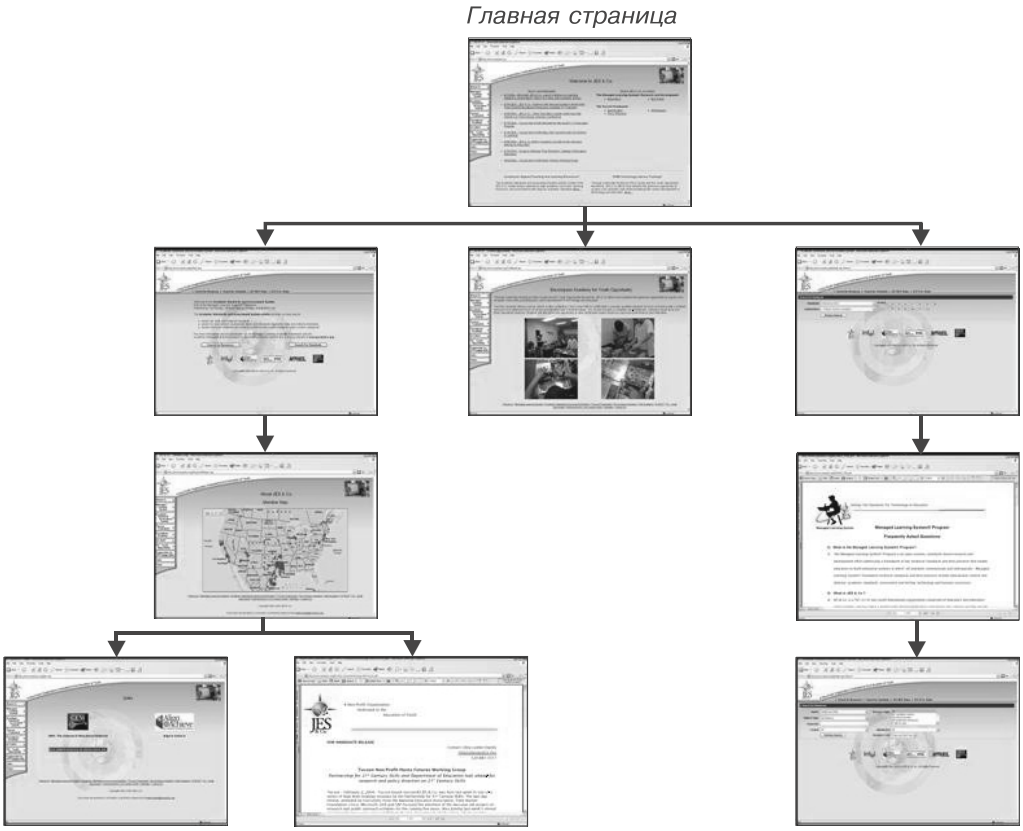


Рис. 10.6. Веб-сайт с древовидной структурой

отыскать, в каком месте сайта вы сейчас находитесь, или вернуться на главную страницу будет не так-то просто (рис. 10.7). Такая непрофессиональная структура характерна для начинающих вебмастеров или для организаций, не имеющих четкого представления о том, какую информацию и в каком виде они хотят разместить на своем веб-сайте.

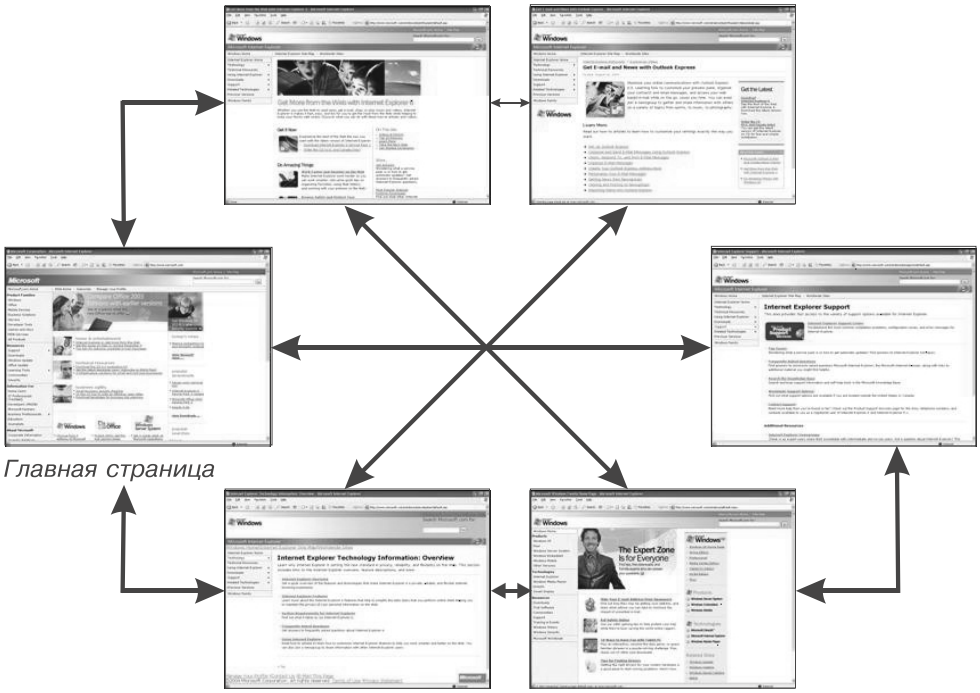


Рис. 10.7. Веб-сайт с произвольной структурой

Наконец, следует упомянуть о так называемых *веб-порталах* и *поисковых системах* (эти функции нередко объединяют). Типичными примерами веб-порталов являются сайты `www.rambler.ru` и `www.yandex.ru`. С головной страницы портала новичок в Интернете может перейти на сайты, посвященные практически всем областям жизни, причем, как правило, это будут наиболее посещаемые сайты. Самое главное при этом — «не заблудиться в Сети», т. е. всегда помнить, какую информацию вы хотели найти в Интернете, и постараться не обращать внимания на другие, может быть, даже более интересные вещи. Реализованы на порталах также и поисковые системы, позволяющие искать информацию в Интернете по запросу (*ключевому слову* или фразе). Примерами чисто поисковых систем являются, например, `www.google.ru`, `search.msn.com` и другие.

Скрипт — это небольшая программа, реализующая те или иные действия на веб-странице, например интерактивное взаимодействие с пользователем, и представляющая собой текст (*листинг*) на особом языке программирования (*JavaScript* или *VBScript*). Извлечение листинга скрипта из текста веб-страницы и его выполнение осуществляет веб-браузер.

Как мы уже говорили, просмотр веб-страниц производится с помощью специальных программ — *веб-браузеров*. Браузеры обеспечивают взаимодействие с веб-серверами по протоколу HTTP и, получив данные в формате HTML, правильно отображают их на экране (а также воспроизводят, если это музыкальный или видеофайл, или запускают на исполнение, если это программа или *скрипт*). Они также позволяют легко переходить от страницы к странице, от сайта к сайту — такие путешествия часто называют «сетевым сёрфингом» (*web surfing*).

Несмотря на то, что сегодня существует множество различных браузеров, все они имеют общие черты. На рис. 10.8 показаны основные компоненты окна браузера Internet Explorer — подобные им вы найдете практически в любом другом современном браузере.

Рис. 10.8. Компоненты окна браузера Internet Explorer

Панель инструментов браузера содержит различные кнопки, которые делают путешествие по Всемирной Паутине более удобным (рис. 10.9).

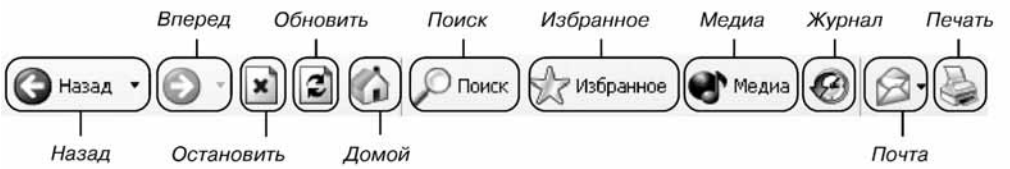


Рис. 10.9. Стандартная панель инструментов браузера Internet Explorer

Каждая кнопка здесь выполняет особую функцию:

- **Назад (Back)** — возвращает вас на предыдущую просмотренную веб-страницу;
- **Вперед (Forward)** — перемещает вас на следующую страницу, если перед этим была нажата кнопка **Назад**;
- **Остановить (Stop)** — прекращает загрузку текущей веб-страницы;
- **Обновить (Refresh/Reload)** — заново загружает текущую страницу в этом же окне, обновляя ее содержимое;
- **Домой (Home)** — показывает страницу, которую вы настроили в качестве «*домашней*»;
- **Поиск (Search)** — открывает специальную страницу (или панель браузера), где можно ввести поисковый запрос к службе `search.msn.com`;
- **Избранное (Favorites)** — открывает список страниц, ссылки на которые вы сохранили ранее (своего рода «записная книжка» адресов веб-сайтов);

Сегодня «домашней страницей» обычно называют произвольный веб-сайт (либо просто «чистый лист» без какой-либо информации), с которого по умолчанию всегда начинается работа в Интернете после запуска браузера. Адрес этого сайта можно указать в настройках браузера, например, сделать «домашней страницей» портал `www.yandex.ru`.

- **Мультимедиа (Media)** — ссылка на мультимедийный сайт `WindowsMedia.com`;
- **Журнал (History)** — открывает список веб-страниц, посещенных вами в последние дни (по умолчанию — за последние 20 дней);
- **Почта (Mail)** — открывает вашу программу электронной почты, позволяя отправить кому-либо сообщение, копию просматриваемой веб-страницы или ссылку на нее;
- **Печать (Print)**: позволяет распечатать текущую веб-страницу на бумаге.

Для связи с Интернетом домашних пользователей в основном применяются различные модемные решения. Коллективные домашние сети и корпоративные клиенты, как правило, используют скоростное постоянное подключение по выделенной линии или по оптоволоконным каналам.

На уровне протокола IP для работы с Интернетом используются либо обычные маршрутизаторы, что требует большого количества реальных IP-адресов и не обеспечивает должной защиты внутренних компьютеров, либо маршрутизаторы с поддержкой технологии трансляции сетевых адресов (NAT).

Для удобной работы с Интернетом следует установить и настроить в сети сервер системы доменных имен DNS, который будет преобразовывать имена узлов в IP-адреса.

Наиболее популярной службой Интернета является WWW, представляющая собой глобальную распределенную систему веб-серверов с самой разнообразной гипертекстовой информацией, доступ к которой осуществляется с помощью специальных программ-браузеров.

Вопросы и задания

1. Какие возможны способы доступа в Интернет? Каковы их основные различия?
2. Какие виды модемов вы знаете? В чем сходство и различия их функционирования при работе с Интернетом?
3. В чем разница между технологиями выделения реальных IP-адресов и трансляции сетевых адресов? Какая из них является более предпочтительной и почему?
4. В чем сущность трансляции сетевых адресов? Какие преимущества она обеспечивает? Есть ли у нее недостатки по сравнению с выделением реальных IP-адресов?
5. Можно ли «превратить» свой компьютер, подключенный к Интернету через провайдера, в «сервер доступа к Интернету» для всей домашней компьютерной сети? Что для этого требуется?
6. Что такое DNS? Как она работает?
7. Как структура записи доменного имени (несколько «слов», записанных через символ «точки») связана с древовидной структурой службы DNS? (Поясните на примере в виде условной схемы.)
8. В чем заключается основное преимущество DNS?
9. Почему появление новых доменных имен верхнего уровня всегда вызывает заметный ажиотаж во всем мире?
10. Как вы считаете, какие преимущества и недостатки могла бы дать возможность регистрации доменных имен не только на английском, но и на национальном языке (например, русском)?
11. Около 10 лет назад одна из российских фирм предложила создать «службу русских доменных имен» (правда, так и не «прижившуюся»), позволяющую регистрировать «русскоязычные» адреса сайтов. При этом никак не затрагивался

существующий механизм DNS, а для работы с «русскими» адресами сайтов каждому клиенту предлагалось установить на свой компьютер специальную программу-утилиту. Как, по вашему мнению, могла бы быть организована работа такой «службы имен»? Почему она не нашла широкого применения?

12. Что такое «Всемирная Паутина»? Какова история ее появления? Какие основные компоненты потребовались для ее реализации?
13. Что означает термин «распределенная» в определении WWW как «распределенной информационной системы»? Какие преимущества и недостатки связаны с этим свойством WWW?
14. В чем заключается идея гипертекстового представления информации? Каковы ее преимущества?
15. Что такое веб-страница? веб-сайт? веб-сервер? Как взаимосвязаны эти понятия?
16. Какой может быть типичная структура веб-сайта? В чем заключаются преимущества и недостатки каждого из трех видов структуры веб-сайта? В каких случаях имеет смысл применять ту или иную структуру?
17. Каково назначение веб-порталов и поисковых систем? (Приведите примеры.)
18. Что такое браузер? Каково его назначение? Как вы считаете, почему именно Internet Explorer является наиболее популярным браузером, хотя при желании можно установить практически любой браузер из нескольких других их «семейств»?
19. Каковы основные функциональные возможности браузера Internet Explorer? Как ими управлять?

Глава 11

Средства общения и обмена данными. Правила поведения в Интернете

В этой главе вы найдете ответы на следующие вопросы:

- ***Как работает электронная почта?***
- ***Как создать учетную запись электронной почты?***
- ***Как получать и отправлять электронные сообщения?***
- ***Каковы правила вежливости при общении в Интернете?***
- ***Для чего создаются дискуссионные группы (форумы)?***
- ***Что такое мгновенные сообщения?***
- ***Как принимать и отправлять мгновенные сообщения?***
- ***В чем заключается совместное использование файлов?***
- ***Как определить, легально ли совместное использование файлов?***

Ранее мы познакомились с Всемирной паутиной (WWW) — одним из основных информационных ресурсов, ради которого большинство пользователей и подключается к Интернету. Однако Интернет как глобальная среда передачи информации предоставляет и другие интересные возможности: электронную почту, обмен мгновенными сообщениями, обмен файлами и множество других. Знакомству с ними посвящена эта глава.

Электронная почта

Электронная почта, *e-mail* — одна из наиболее часто используемых (после WWW) возможностей Интернета. Каждый день сотни миллионов электронных сообщений отправляются и принимаются по всему миру. Любой пользователь, имеющий доступ к Интернету, может легко зарегистрировать бесплатный почтовый ящик на одном из общедоступных серверов электронной почты, сообщить друзьям и знакомым свой адрес и почти сразу начать отправлять и получать сообщения e-mail (рис. 11.1). А в корпоративной среде электронная почта уже давно стала одним из основных методов взаимодействия между сотрудниками.

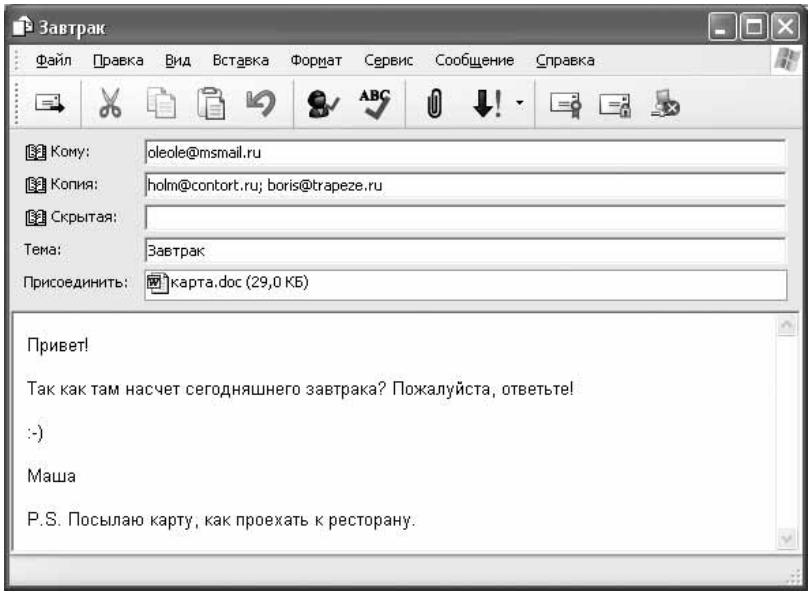


Рис. 11.1. Пример электронного сообщения

Работает электронная почта практически так же, как и обычная. В ней тоже есть письма, конверты с адресами, служба доставки, почтовые ящики. Однако доставка электронного письма, в отличие от обычного «бумажного», редко занимает больше минуты.

Чтобы отправлять и принимать электронные сообщения, вам потребуется *клиентское программное обеспечение для работы с электронной почтой*. Это может быть, например, Microsoft Outlook, Outlook Express или любой другой *почтовый клиент*, или же просто *браузер*, поскольку многие почтовые серверы, особенно общедоступные, предоставляют пользователям веб-интерфейс для работы со своими почтовыми ящиками.

Большинство клиентских почтовых программ использует протоколы POP3 и IMAP4 для подключения к пользовательскому почтовому ящику и считывания почты, и протокол SMTP — для отправки писем. Веб-доступ к почтовым ящикам осуществляется по протоколу HTTP.

Для обеспечения защиты при приеме и передаче почтовых сообщений рекомендуется использовать *протокол SSL* (*Secure Sockets Layer*).

Программа Microsoft Outlook для работы с почтовым сервером Exchange использует *протокол RPC*, включающий в себя встроенные механизмы обеспечения безопасности канала.

Напомним, что при работе с электронной почтой следует обязательно пользоваться современными антивирусными программами и, желательно, средствами защиты от нежелательной почты — *спама*.

Спам (*SPAM*, «*Shoulder Pork and haM*»/«*SPiced hAM*») — в буквальном переводе «прессованная ветчина с пряностями» (когда-то рекламой именно этого товара его фирма-изготовитель буквально «заваливала» почтовые ящики — тогда еще обычные, не электронные, — многих американских граждан). Сегодня это понятие обозначает бесполезные сообщения электронной почты, принудительно рассылаемые большому числу абонентов. Такие сообщения обычно содержат рекламные объявления, описания «способов быстрого обогащения» и пр. К сожалению, сегодня более 80% электронных писем в Интернете является спамом.

В любом случае принципы функционирования электронной почты следующие:

- вы набираете свое письмо, обязательно указывая электронный адрес получателя сообщения (например, `myfriend@mail.ru`);
- после нажатия кнопки **Отправить** почтовая программа (или браузер) конвертирует сообщение в нужный формат и отправляет его вашему почтовому серверу.

Дальше начинает работать почтовый сервер:

- путем обращения к DNS-серверу домена, в который направлено ваше письмо (для этого в DNS регистрируется специальная запись типа «*почтовый обменник*» — *Mail Exchanger*, или *MX*), ваш сервер определяет имя и IP-адрес почтового сервера получателя;
- между обоими почтовыми серверами устанавливается соединение по *протоколу SMTP* (*Simple Mail Transfer Protocol*, или «простой протокол передачи почты»), и ваше письмо передается удаленному серверу получателя.

Сервер адресата принимает письмо, определяет, существует ли на этом сервере требуемый почтовый ящик, проводит другие проверки (например, не переполнен ли почтовый ящик получателя) и, если все в порядке, доставляет письмо. Теперь получатель письма, используя свою почтовую программу, может просмотреть ваше сообщение.

Несмотря на довольно большое количество задействованных здесь клиент-серверных и сервер-серверных операций, доставка электронного письма, как мы уже говорили, происходит очень быстро, иногда в считанные секунды.

Чтобы отправлять и получать электронные письма, необходима *учетная запись электронной почты*. Ее можно получить в учебном заведении, на работе или у провайдера, либо, как уже говорилось, зарегистрировать на бесплатном общедоступном почтовом сервере.

При создании учетной записи для вас будет зарегистрирован уникальный *электронный адрес*, состоящий из имени пользователя (его, как правило, можно выбрать по своему желанию), знака «@» и названия домена: например, `myname@hotmail.ru`. Кроме того, вы получите уникальное имя пользователя (*account*, *login name*) и *пароль*, которые понадобятся вам для подключения к серверу, когда вы будете проверять (получать и отправлять) свою электронную почту.

Необычный символ «@», называемый в просторечии «собакой», в компьютерный обиход ввел создатель одной из первых почтовых программ для ARPANet, Рэй Томлинсон. В английском языке символ «@» («коммерческое эт») часто используется в ценниках (например, запись «10 items @ $5.28» означает: «10 штук по 5.28 доллара»). Томлинсон выбрал этот символ потому, что он не употребляется ни в каких именах и, соответственно, не может вызвать путаницы.

Все системы передачи электронных сообщений, хотя и характеризуются различными внутренними форматами писем и «электронных конвертов» (напомним, что для взаимодействия разных почтовых систем применяются *почтовые шлюзы*), но тем не менее используют похожие базовые элементы сообщения (рис. 11.2). Поэтому, если вы поймете назначение каждого из этих элементов, вы сможете получать и отправлять электронные сообщения в любой почтовой системе.

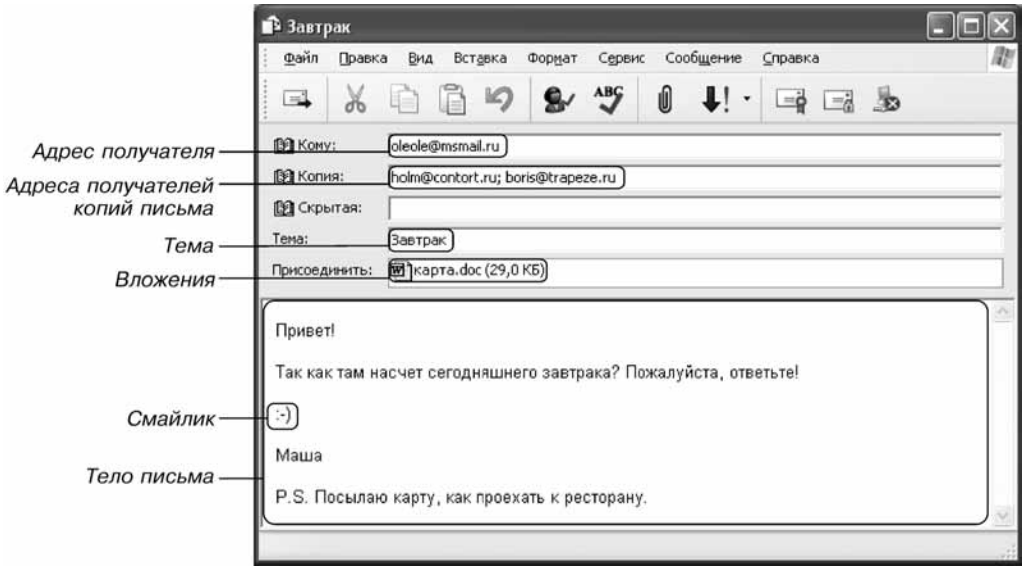


Рис. 11.2. Типичные элементы электронного сообщения

Большинство почтовых программ содержат в своем составе *адресную книгу*, позволяющую сохранять часто используемые адреса электронной почты для последующей быстрой подстановки в соответствующие поля письма.

Базовые элементы электронного сообщения:

- *имя и адрес получателя* — точно так же, как и при отправке обычного письма, ***обязательно*** (иначе письмо невозможно будет доставить) следует указать электронный адрес того, кому вы посылаете это сообщение;
- *имя и адрес отправителя* — ваши собственные имя и адрес. Эти параметры обычно автоматически подставляются при отправке письма почтовой программой или сервером;
- *тема* — краткая формулировка содержания вашего письма;
- *время и дата* — как правило, автоматически заполняются программой электронной почты или сервером при отправке письма;

- *тело письма* — собственно текстовое сообщение;
- *вложения* — вложенные в электронное сообщение файлы, в том числе графические изображения, цифровые звукозаписи, программы и документы;
- *копия* (*cc*, сокращение от «carbon copy», «копирка») — в этом поле можно ввести электронный адрес еще одного получателя, если вы хотите, чтобы ему была отправлена копия данного письма;
- *«слепая копия»* (*bcc*, или «*blind cc*») — то же, что и обычная копия, но «основной» адресат *не будет знать*, что копия письма была отправлена другому получателю.

Правила вежливости при работе с почтой

Электронная почта предоставила людям новую возможность общения и возродила эпистолярный жанр, чуть было не забытый после изобретения и повсеместного распространения телефонов. Однако чтобы такое общение было взаимно вежливым и безопасным, следует запомнить некоторые простые правила. Полный список этих *правил сетевого этикета*, или «*нетикета*» (*Netiquette*), нетрудно найти в Интернете, например, на странице `http://www.albion.com/netiquette/` или в переводе на русский язык — на сайте `http://www.helios-tv.ru/rules/netiquette/`.

1. Всегда помните, что *вы общаетесь с людьми, а не с компьютерами*. Это, пожалуй, самое главное, что нужно не забывать при работе в Интернете.
2. Старайтесь всегда указывать в поле **Тема**, о чем идет речь в письме, чтобы получатель сразу мог узнать о его содержании.

Некоторые сокращения, часто используемые в поле **Тема** (и вообще при общении в Интернете):

FYI («For your info») — «К сведению»;
ASAP («As soon as possible») — «Как можно быстрее»;
IMO («In my opinion») — «По моему мнению»;
IMHO («In my humble opinion») — «По моему скромному мнению»;
AFAIK («As far as I know») — «Насколько мне известно»;
BTW («By the way») — «Кстати»;
BBL («Be back late(r)») — «Буду поздно», «Вернусь поздно»;
TTYL («Talk to you later») — «Потом поговорим»;
SIT («Stay in touch») — «Оставайся на связи»;
BCNU («Be seeing you») — «Увидимся».

Эти «смайлики» помогут вам выразить свои эмоции в электронных сообщениях:

`:-)` — улыбка;
`;-)` — подмигивание;
`:-*` — поцелуй;
`:-(` — грусть;
`:-o` — изумление;
`:-O` — крик;
`:-D` — смех;
`{}` — зевота;
`:-P` — показывать язык;
`:-|` — быть в раздумьях;
`:->` — злая ухмылка;
`:-/` — непонимание;
`8-)` — довольство;
и т. д.

3. Избегайте использования прописных букв в тексте письма: это часто воспринимается как невоспитанность (все равно, что громко кричать при обычном разговоре).

4. Чтобы сделать общение со знакомыми и близкими людьми более «эмоциональным», можно использовать так называемые «*смайлики*» — рожицы, составленные из нескольких символов.

5. Старайтесь писать короткие сообщения, а длинные — разбивайте на части пустыми строчками, чтобы облегчить их понимание.

6. Пишите грамотно, корректно составляйте фразы, иначе возможно неправильное истолкование ваших слов.

7. При ответе на письмо включайте в него (*цитируйте*) только те части исходного сообщения, которые нужны для понимания вашего ответа.

8. Избегайте лишнего украшательства — большое количество картинок, шрифты различных цветов и размеров и т. д. часто лишь затрудняют чтение письма и увеличивают его объем (а значит, и время пересылки). Это оправданно разве лишь в электронных поздравительных открытках. Устаревшие же почтовые программы вовсе не воспринимают такие сообщения.

9. Всегда подписывайте свое письмо, включая в подпись свое имя и другую существенную для общения с вами информацию (например, телефон, адрес, должность и пр.).

10. Помните, что обычно письма передаются по сети в незашифрованном виде, поэтому *никогда не включайте в электронные сообщения информацию об именах, паролях доступа, номерах кредитных карт и т. д.*

Гостевая книга — один из возможных «сервисов», размещаемых на сайте для того, чтобы его посетители могли оставлять свои пожелания, похвалы или, возможно, критические замечания.

Дискуссионные группы (форумы)

Кроме отправки электронных сообщений одному или нескольким адресатам, электронную почту можно также использовать для общения в *дискуссионной группе* (*форуме*, *группе новостей*).

Дискуссионная группа — это сообщество пользователей Интернета, имеющих какие-то общие интересы и общающихся с помощью электронной почты или, что в последнее время бывает гораздо чаще, через специальный веб-сайт. Вы можете отправить электронное сообщение на главный адрес группы, а почтовый сервер автоматически разошлет копии этого письма каждому члену группы, используя их адреса из *списка рассылки*. Например, если группа учащихся посещает летние занятия, организация, проводящая это мероприятие, может создать для всех посетителей таких занятий отдельную дискуссионную группу. После того как желающие из числа учащихся подпишутся на список рассылки, они смогут посылать сообщения как друг другу в отдельности, так и всем членам группы сразу.

В Интернете существуют тысячи дискуссионных групп, посвященных самым разнообразным темам. Когда вы находите группу, посвященную интересующей вас теме, прежде всего вы должны отправить в эту группу сообщение с просьбой о подписке. Обычно в ответ вам приходит сообщение, что вы стали членом группы, или же что кто-то из уже имеющихся участников группы должен подтвердить вашу регистрацию и добавить вас в список подписчиков. Каждая дискуссионная группа имеет свой набор правил добавления новых пользователей; перед началом работы в интересующей вас группе обязательно ознакомьтесь с этими правилами и соблюдайте их.

Другой возможный вариант дискуссионной группы (форума) может быть реализован в виде веб-сайта (аналогично *гостевой книге*). В этом случае все участники форума, зарегистрированные для общения по интересующей их теме, могут добавлять в об-

щий список свои сообщения или ответы и комментарии на уже имеющиеся сообщения. Все остальные посетители такого сайта могут свободно читать эти сообщения (возможно, кроме некоторых фрагментов текста), но не могут добавлять свои сообщения, пока не пройдут процедуру регистрации.

Обмен мгновенными сообщениями в Интернете

Слова «в реальном времени» означают, что, как только вы вводите свое сообщение в программу обмена мгновенными сообщениями и нажимаете кнопку **Отправить**, все ваши собеседники, работающие в данный момент в сети, могут прочитать его практически сразу.
Поэтому, прежде чем нажать эту кнопку, еще раз перечитайте все свое сообщение, проверьте корректность выражений и исправьте допущенные ошибки.

Несмотря на то, что электронная почта работает быстрее, чем обычная, нет никакой гарантии, что адресат немедленно ответит на ваше электронное письмо. Для общения через Интернет *в реальном времени* можно использовать множество способов, однако одним из самых популярных является использование мгновенных сообщений.

Мгновенное сообщение — это текст, который вы вводите в окне специальной программы. Человек, с которым вы общаетесь, получит ваше сообщение уже через секунду. Разумеется, для обмена мгновенными сообщениями оба собеседника должны быть в этот момент подключены к Интернету и использовать совместимое программное обеспечение. Вы можете также одновременно беседовать с несколькими людьми в *чат-группе* (от английского «chat» — «болтать»). Каждый находящийся в чат-группе пользователь мгновенно видит все сообщения, которые отправлены любым из других пользователей. С помощью специальных программ вы можете присоединиться к открытым чат-группам, которые обычно посвящены определенным темам и интересам, или создать свою собственную чат-группу, в которой будете встречаться и беседовать со своими друзьями.

Существует несколько популярных приложений для обмена мгновенными сообщениями, одним из которых является предлагаемая Microsoft программа MSN Messenger (рис. 11.3).

Другая популярная программа для обмена мгновенными сообщениями — ICQ, или, в просторечии, «Аська». Говорят, что ее название — это «перифраз» аббревиатуры английской фразы «I Seek You» — «Я ищу тебя». Однако программу ICQ необходимо скачивать из Интернета и устанавливать отдельно, тогда как MSN Messenger является стандартным приложением Windows (в частности, в версии XP).

Чтобы использовать мгновенные сообщения, сначала нужно зарегистрироваться в службе, предоставляющей данный сервис, получить имя пользователя и пароль, а также установить на свой компьютер специальное программное обеспечение. Большинство программ обмена мгновенными сообщениями позволяет вам создать список знакомых, с которыми вы часто беседуете. Одной из важных особенностей систем обмена мгновенными сообщениями является возможность видеть в этом списке *текущую информацию о присутствии ваших друзей и знакомых в сети*, т. е. всегда можно проверить, подключены ли они в данный момент к Интернету, находятся ли за своим компьютером или, например, ушли пообедать. Свою программу можно настроить так, чтобы только ваши знакомые знали, подключены ли вы в данный момент к Интернету.

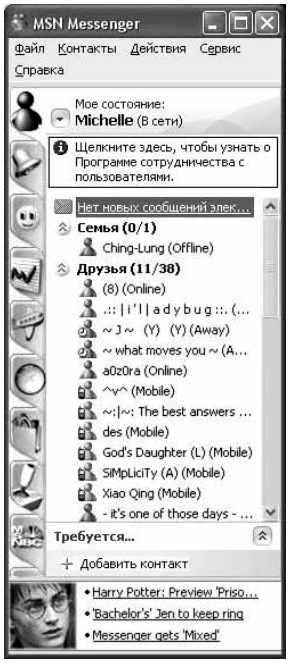


Рис. 11.3.
Окно программы MSN Messenger

После того как вы создали учетную запись, можно выбрать в списке имя человека, с которым хотите пообщаться, и ввести текст послания в окне программы на вашем компьютере, а затем нажать кнопку отправки. В тот же момент пользователь с выбранным именем получит ваше сообщение и сможет вам ответить.

Если вы должны на время отойти от компьютера или просто хотите, чтобы вас не беспокоили, измените в программе *свое состояние в сети*, и ваши знакомые сразу увидят, что вы ушли или заняты.

Одной из первых широко известных программ совместного доступа к файлам была программа KAZAA, однако ее сервер позже был закрыт по требованию целого ряда фирм из-за многочисленных нарушений авторских прав пользователями этой программы. Поэтому существующие сегодня программы совместного доступа к файлам (eMule, eDonkee и др.) работают *децентрализованно* (для них отсутствует какой-либо единый сервер, закрытие которого может прекратить работу сервиса), фактически образуя «на базе» Интернета отдельную, так называемую «*пиринговую*» сеть.

При этом они все равно смогут отправить вам сообщение, которое будет ждать, когда вы вернетесь или освободитесь (точно так же, как письмо электронной почты).

Обмен файлами в Интернете

Передача файлов всегда была одним из самых распространенных способов обмена информацией в Интернете. Достаточно сказать, что первая версия протокола передачи файлов FTP была разработана еще в 1971 г. С тех пор принципы файлового обмена несколько изменились, и в настоящее время наиболее популярными являются программы, обеспечивающие *совместный доступ к файлам* (*peer-to-peer file sharing*). Во многом это связано с появлением и широким распространением таких форматов, как JPEG, MP3, WMA, MPEG4 и др., которые позволяют в компактном виде хранить графику, аудио- и видеоданные.

Когда эти форматы стали популярными, некоторые компании разработали специальное программное обеспечение для совместного доступа к таким файлам. Это позволило пользователям сохранять музыкальные файлы на своем компьютере и делать их общедоступными в Интернете. Изначально общий доступ применялся в основном для цифровой музыки, однако сегодня совместное использование распространилось практически на все виды файлов, в том числе на табличные и текстовые документы, программы, графику и видеофильмы.

Чтобы совместно использовать файлы, вам понадобится специальная программа. После ее установки производится соединение вашего компьютера с сервером, управляющим *списками общих файлов*, расположенных на множестве таких же пользовательских компьютеров в Интернете. Сервер также поддерживает список всех пользователей и может управлять доступом к общим файлам.

Получив информацию от этого сервера, ваш компьютер с помощью программы обмена соединяется с одним из компьютеров, на котором хранится интересующий вас файл (или какая-либо его часть). Программа отправляет туда адрес вашего компьютера, вашу идентификационную информацию и запрашивает нужный файл. Если все проверки завершились успешно, удаленный компьютер пересылает данные через Интернет непосредственно вашему компьютеру. Таким образом, система совместного использования позволяет вам напрямую соединяться с другими пользовательскими компьютерами в Интернете и обмениваться с ними файлами.

Легальность использования информации из Интернета

При пересылке файлов, а особенно при совместном доступе к файлам, следует всегда иметь в виду, что подавляющее большинство представленной в Интернете информации защищено *законами об авторских правах* (даже если на соответствующих веб-страницах об этом прямо не сообщается). Из того, что файлы легко доступны для всех пользователей Интернета, вовсе не следует, что их можно свободно копировать и распространять. Даже если вы не извлекаете никакой выгоды из такого копирования или распространения, это в подавляющем большинстве случаев незаконно. Чтобы использовать какую-либо информацию из Интернета — например, в качестве иллюстрации в своем школьном докладе, презентации или реферате, — следует обязательно получить разрешение от владельца информации или веб-сайта и указать ссылку на страницы в Интернете, откуда были взяты эти материалы. (Кстати, большинство владельцев с удовольствием предоставят вам такое разрешение — для них это будет хорошим признаком, что опубликованные ими в Интернете материалы действительно интересны и полезны.)

Использовать же без разрешения и свободно распространять можно только такую информацию или данные, о которых их владельцем четко указано, что они *предназначены для свободного распространения*. Но и в этом случае данные, как правило, нельзя модифицировать и распространять без ссылки на их первоисточник.

Итак, кроме Всемирной паутины, Интернет предоставляет своим пользователям широкие возможности общения. Основными из них являются электронная почта, работающая благодаря целой системе почтовых серверов, передача мгновенных сообщений и дискуссионные группы. Кроме того, в Интернете функционирует множество систем совместного доступа к файлам, позволяющих пользователям обмениваться музыкальными и другими данными.

Однако при работе и обмене информацией следует не забывать, что размещенные в Интернете файлы и другие данные защищены законом об охране авторских прав, поэтому их копирование и распространение без разрешения владельца может быть неправомерным.

Вопросы и задания

1. Какие сервисы и службы в Интернете вы знаете?
2. Каковы принципы функционирования электронной почты?
3. Для чего нужны протоколы IMAP, POP3, SMTP, SSL, RPC?
4. Почему электронную почту называют «средством асинхронного общения» (т. е. общения, разделенного во времени)?
5. Что такое учетная запись электронной почты? Как ее получить?
6. Из каких элементов состоит электронное сообщение?

7. Какие правила «сетевого этикета» вы знаете? Объясните их смысл.
8. Что такое дискуссионная группа (в форме почтовой рассылки)? В чем сходство и различие между работой в составе такой дискуссионной группы и обычной почтовой перепиской?
9. Что такое обмен мгновенными сообщениями? В чем сходство и различие между этой технологией и электронной почтой?
10. Почему программы MSN, ICQ и другие аналогичные им часто называют «Интернет-пейджерами», а работу с ними — «общением в реальном времени»?
11. Что понимается под совместным доступом к файлам? Каково основное отличие работы с этими сервисами от обычного скачивания файлов из Интернета по протоколу FTP?
12. В чем заключается проблема легальности использования информации из Интернета?

Оглавление