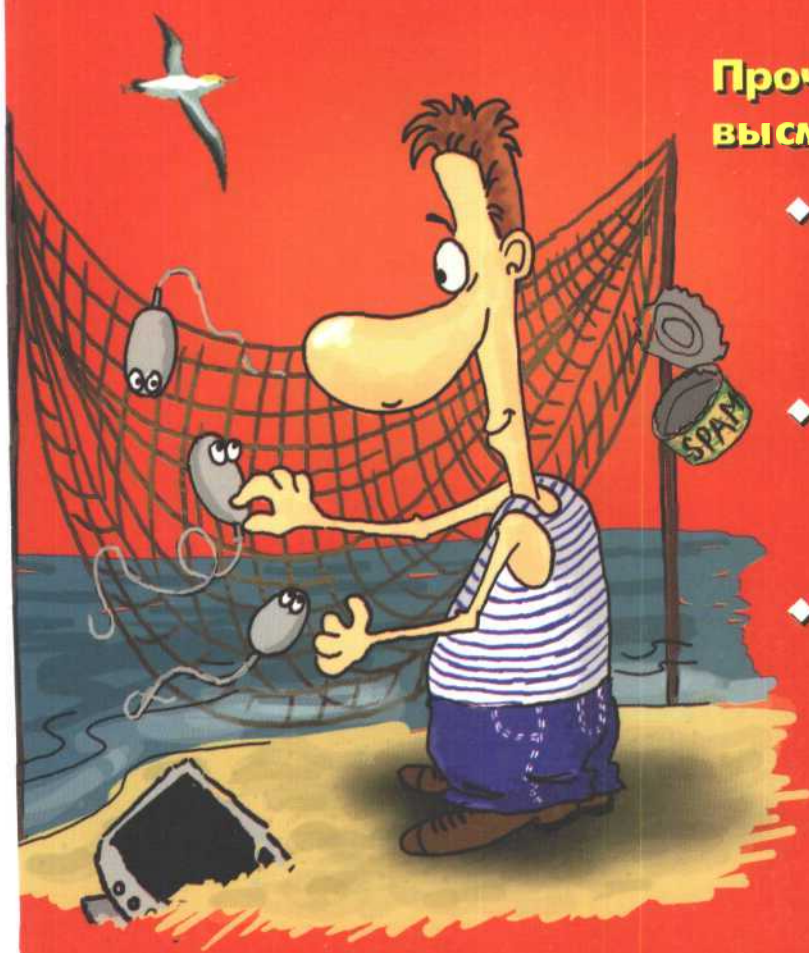
Валентин Холмогоров

САМОУЧИТЕЛЬ

Компьютерная сеть СВОИМИ РУКАМИ



Прочитав эту книгу, вы сможете:

- разработать топологию компьютерной сети
- подобрать оборудование и настроить локальную сеть
- организовать совместную работу в сети

ПИТЕР®

СЕРИЯ

САМОУЧИТЕЛЬ

ПИТЕР®

Валентин Холмогоров

САМОУЧИТЕЛЬ

Компьютерная сеть СВОИМИ РУКАМИ

ПИТЕР®

Москва • Санкт-Петербург • Нижний Новгород • Воронеж
Ростов-на-Дону • Екатеринбург • Самара
Киев - Харьков • Минск
2003

ББК 32.973.202я7
УДК 681.324(075)
Х72

Х72 Компьютерная сеть своими руками. Самоучитель / В. Холмогоров. — СПб.: Питер, 2003. — 171 с.: **ил.**

ISBN 5-Э4723-646-Х

Эта книга посвящена рассмотрению наиболее популярного в нашей стране стандарта организации локальных сетей — Ethernet. Безусловно, охватить в рамках такого небольшого издания все аспекты проектирования и администрирования локальных сетей невозможно, однако настоящий самоучитель содержит именно тот необходимый объем информации, который позволит вам самостоятельно спроектировать и настроить небольшую локальную сеть, состоящую из нескольких компьютеров.

ББК 32.973.202Я7
УДК 681.324(075).

ISBN 5-94723-646-Х

Краткое содержание

Содержание

Предисловие

У вас дома два компьютера? К одному подключен принтер, и вам приходится бегать с дискетой, чтобы распечатать документ, подготовленный на другом компьютере? Или вы хотите сражаться с друзьями в любимые компьютерные игры? А может быть, вам нужно работать в Интернете, но у вас нет модема, а у ближайшего соседа есть?..

Решение очевидно — ведь сегодня уже никому не нужно объяснять, насколько эффективнее можно использовать имеющиеся в распоряжении компьютеры и периферийные устройства, если объединить оборудование в локальную сеть!

В этой книге вы найдете:

- описание основ организации сети Ethernet с использованием коаксиального кабеля и витой пары;
- описания и характеристики основных типов кабелей;
- определение и описание основных типов топологии сети;
- объяснение принципов настройки и эксплуатации оборудования и программного обеспечения.

Кроме того, вы получите множество полезных практических советов по организации и прокладке локальных сетей Ethernet.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу электронной почты comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

Подробную информацию о наших книгах вы найдете на web-сайте издательства http://www.piter.com.

Глава 1

Общие сведения о локальных сетях

- История развития локальных сетей
- Общие сведения о подключении локальных сетей к Интернету
- Существующие сетевые технологии
- Перспективы развития локальных сетей

Сегодня уже трудно представить себе, как люди жили когда-то без столь удобного и полезного инструмента, как локальные сети. Однако знало человечество и такие времена. Впервые идея связать несколько независимо работающих компьютеров в единую распределенную вычислительную систему посетила светлые головы инженеров еще в середине 60-х годов XX века. А если говорить более конкретно, то первый успешный эксперимент по передаче дискретных пакетов данных между двумя компьютерами провел в 1965 году молодой исследователь из лаборатории Линкольна Массачусетского технологического института Лари Роберте. Алгоритмы передачи данных, предложенные Робертсом, во многом послужили основой для построенной в 1969 году по инициативе американского «Агентства перспективных научных исследований» (Advanced Research Projects Agency, ARPA) глобальной вычислительной сети ARPANet, а она впоследствии, объединившись с несколькими другими существовавшими на тот момент сетями, стала фундаментом, на котором вырос современный Интернет.

Однако и широко использовавшиеся в те времена многотерминальные системы, в которых пользователям предоставлялся доступ к одному головному многофункциональному компьютеру посредством нескольких конечных устройств удаленного подключения — терминалов — по принципу разделения процессорного времени, и глобальные сети, объединявшие между собой мейнфреймы крупных вычислительных центров и лабораторий, являлись лишь предтечей локальных сетей в их нынешнем понимании. Существенный толчок в направлении развития малых локальных сетей дало бурное

развитие во второй половине 70-х годов настольных персональных компьютеров. И в авангарде этого процесса стояла фирма Xerox.

Персональные компьютеры Xerox Star были весьма и весьма популярны в начале 80-х годов, во-первых, благодаря сочетанию низкой стоимости и достаточно высокой производительности, во-вторых, потому, что работали они под управлением первой в мире операционной системы с оконным графическим интерфейсом, предоставлявшей пользователю возможность максимально комфортно взаимодействовать с ресурсами ЭВМ, и, наконец, по той простой причине, что разработчики предусмотрели возможность включения нескольких машин Xerox Star в единую сеть. Именно инженер-исследователь фирмы Xerox Роберт Меткалф впервые предложил стандарт организации малых локальных сетей Ethernet, который широко используется при проектировании подобных систем до сих пор.

Тем не менее, несмотря на очевидные достоинства персональных компьютеров от Xerox, они были вскоре окончательно вытеснены с рынка изделиями корпорации IBM, впитавшими в себя все перспективные разработки и лучшие технические решения предшественников. Большие производственные мощности этой компании позволили снизить цены на персональные компьютеры до возможного минимума, и конкурировать с IBM PC стало практически невозможно. Количество локальных сетей росло в геометрической прогрессии, что вскоре привело к необходимости разработки четких стандартов архитектуры распределенных вычислительных систем. Действительно, одна из основных задач локальных сетей заключается не только в передаче данных и организации общего доступа к тем или иным периферийным устройствам, но также и *в обеспечении совместной работы оборудования различных производителей.* Это, естественно, означает необходимость унификации и стандартизации подходов к построению локальных сетей. Именно в 80-х годах окончательно сформировались основные стандарты распределенных вычислительных систем, такие как Ethernet, Token Ring, ArcNet, FDDI и некоторые другие. Все эти стандарты, а также многие смежные вопросы, связанные с теоретическими и практическими аспектами построения локальных сетей, мы подробно рассмотрим на страницах этой книги.

80-е годы можно назвать эпохой расцвета локальных сетей, поскольку как крупные, так и малые предприятия быстро оценили выгоды от использования этой перспективной технологии. Действительно, локальные сети позволяли осуществлять быстрый обмен данными между различными подразделениями и отделами фирмы, заметно уменьшив объем циркулирующей внутри предприятия бумажной документации. Это позволяло, во-первых, экономить на накладных расходах, а во-вторых, существенно повышало производительность труда. В сочетании с уже существовавшей

тогда возможностью передавать данные на значительные расстояния по информационным каналам глобальной сети использование подобных технологий открывало широчайшие возможности не только для оптимизации бизнеса и расширения информационного пространства, но и для осуществления межкорпоративного взаимодействия.

С течением времени стандарты, позволявшие объединять компьютеры в локальные сети, постепенно оптимизировались, увеличивалась пропускная способность каналов связи, эволюционировало программное обеспечение, росла скорость передачи данных. Вскоре локальные сети стали использоваться не только для пересылки между несколькими компьютерами текста и различных документов, но также для передачи мультимедийной информации, такой как звук и изображение. Это открыло возможность организации внутри локальной сети систем видеоконференцсвязи, позволявших пользователям такой системы общаться в режиме реального времени «напрямую», физически находясь в различных помещениях, выполнять совместное редактирование текстов и таблиц, устраивать «виртуальные презентации».

Уже сейчас системы компьютерной видеосвязи широко используются крупными коммерческими предприятиями, где служат для организации связи между различными отделами, в военных комплексах для быстрой передачи информации между несколькими абонентами и целыми подразделениями, а в последнее время — и в домашних «настольных» системах, в качестве средства организации досуга. Среди достоинств КВС можно упомянуть относительно низкую стоимость эксплуатации по сравнению с иными существующими на сегодняшний день системами коммуникаций, их многофункциональность, сравнительную легкость в использовании. В процессе работы абоненты видеоконференции в общем случае видят на экранах своих мониторов изображения собеседника и свое собственное, что необходимо для осуществления визуального контроля установленного соединения. Изображение динамически обновляется со скоростью от 0,5 кадра/с до. 15–25 кадров/с в зависимости от скорости (пропускной способности) канала связи и загрузки канала данными. Участники для проведения переговоров используют миниатюрные видеокамеры и микрофоны с достаточно хорошими характеристиками. Речь для передачи по каналу связи оцифровывается. Основными достоинствами компьютерной видеосвязи являются возможности совместной работы с документами и интегрированной информацией (текст, графика, изображение, получаемое с видеокамер участников), а также дистанционный запуск программных приложений на компьютере собеседника. Изображения, получаемые с помощью видеокамер, могут передаваться не только в динамическом режиме (живое видео), но и в статическом. В последнем случае абонент выбирает необходимый кадр, захватывает и передает его по каналу связи в виде файла. В этом случае время передачи

кадра не является критичным, и он может быть сформирован и передан со значительно более высоким качеством. Таким образом, участники подобного сеанса видеосвязи видят друг друга, могут разговаривать в дуплексном режиме, передавать цветные изображения графических документов и объектов, снимаемых видеокамерой, совместно редактировать документы, а также документировать процесс переговоров и результаты с помощью видеомагнитофонов и цветных принтеров. В итоге можно сделать вывод о том, что видеоконференцсвязь с успехом заменяет телефон, цветной факс и обеспечивает возможность записи сеанса или его части на видеомагнитофон для последующего анализа или демонстрации третьим лицам, не участвовавшим в сеансе видеосвязи.

Исходя из всего отмеченного выше можно сказать, что видеоконференции весьма перспективны для ведения переговоров между различными отделами одной компании, при согласовании технических вопросов, например, руководства промышленного предприятия с руководством производственного отдела без необходимости созывать совещание и с возможностью автоматически документировать весь ход переговоров с момента установления соединения до момента его разрыва.

Наконец, в начале 90-х годов XX века удешевление и расширение ассортимента конечного оборудования позволили локальным сетям выйти за пределы коммерческого сектора рынка. Появились небольшие домашние и частные локальные сети, объединявшие несколько компьютеров в одной семье или в пределах одного дома. В последнее время доля малых локальных сетей заметно выросла по отношению к общему количеству работающих в мире распределенных вычислительных систем, что, впрочем, не удивительно, поскольку такие локальные сети позволяют совместно использовать различные устройства, например принтеры, сканеры, цифровые камеры, а также организовывать подключение к Интернету через единственный канал связи, а значит — экономить на оборудовании и комплектующих. Не говоря уже о том, что практически все современные игры имеют возможность одновременного участия в игровом процессе нескольких пользователей, для чего опять же необходима локальная сеть.

Таким образом, локальная сеть — это *распределенная вычислительная система*, позволяющая всем подключенным к ней компьютерам — *узлам* или *рабочим станциям* — обмениваться данными, а также совместно использовать различные аппаратные и программные ресурсы.

Практически все современные локальные сети используют подключение к Интернету либо по коммутируемым каналам связи, либо через непосредственное соединение с высокоскоростной магистралью передачи данных. Да и само появление Интернета было во многом стимулировано развитием локальных сетей, объединявшихся в глобальную вычислительную систему.

В настоящее время используется несколько вариантов подключения локальной сети к Интернету. Вот основные из них.

- **Непосредственный** доступ к Интернету подразумевает использование самого полного спектра услуг глобальной сети. Локальная сеть, имеющая непосредственный доступ, фактически может пользоваться Сетью с высокой скоростью и высокой эффективностью постоянно, то есть круглые сутки и в непрерывном режиме. Как уже упоминалось ранее, Интернет — это сеть, состоящая из множества локальных сетей. Так вот, непосредственный доступ — это и есть фактически прямое включение локальной сети в состав Интернета через высокоскоростную магистраль передачи данных при помощи соответствующего сетевого оборудования. Существует множество фирм, предлагающих такого рода доступ.
- **Коммутируемый** доступ является наиболее распространенным в нашей стране. Этот вид доступа подразумевает подключение локальной сети к Интернету по коммутируемым телефонным или выделенным линиям при помощи модема. Несмотря на относительно невысокую скорость соединения коммутируемый доступ (Dial-Up Access) не требует значительных финансовых затрат на аренду линии связи или закупку дорогостоящего оборудования. Именно поэтому он наиболее популярен при подключении к Интернету домашних и малых корпоративных сетей.
- Доступ по технологии «**coax** at a home». Технология «coax at a home» подразумевает получение доступа к Интернету с использованием каналов кабельной телевизионной сети. Б обобщенном виде такая информационная структура выглядит следующим образом: стандартное оборудование вещания кабельного телевизионного центра подключается к специальному устройству передачи данных, называемому головным модемом, и далее через маршрутизатор — к высокоскоростному каналу Интернета. После этого абоненту достаточно лишь установить на своем компьютере любую сетевую карту, поддерживающую стандарт 10Base-T, соединив ее с клиентским кабельным модемом, а тот, в свою очередь, подключить к расположенному в квартире антенному выходу, — и компьютер оказывается в Сети. Одним из основных элементов клиентской компьютерной системы в схеме кабельной информационной сети является кабельный модем. Как и модем, предназначенный для соединения по коммутируемым телефонным линиям, это устройство представляет собой двунаправленный аналогово-цифровой преобразователь данных, использующий в процессе передачи информации принцип наложения на несущую частоту модулированного аналогового сигнала. Фундаментальным отличием данного аппаратного средства от обыкновенного модема является то, что кабельный модем не требует установки каких-либо драйверов, поскольку он подключается к компьютеру посредством

сетевой карты и является абсолютно прозрачным для системы: программное обеспечение взаимодействует с Интернетом так же, как и в случае непосредственного подключения по локальной сети. Разумеется, отсюда можно сделать абсолютно справедливое логическое заключение о том, что данному устройству совершенно безразлично, какая операционная система инсталлирована на пользовательском компьютере, необходимо лишь, чтобы эта система поддерживала возможность установки сетевой карты и настройки локальной сети. Не менее очевидно и то, что для работы в Интернете абонент может применять любое стандартное программное обеспечение. Среди очевидных преимуществ доступа к Интернету по методу «coax at a home» можно перечислить высокую стабильность соединения, отсутствие непредвиденных разрывов связи, а также то, что на протяжении всего сеанса работы во Всемирной Сети телефонная линия остается свободной. К сожалению, данный метод связи не имеет сегодня в нашей стране широкого распространения.

В современных локальных сетях используются различные технологии подключения, различное оборудование и различные среды передачи данных. Еще несколько лет назад практически единственным возможным вариантом было объединение компьютеров на основе медного сетевого кабеля с пропускной способностью не более 10 Мбит/с, позже появились сети, в которых в качестве среды передачи информации стали использовать оптическое волокно, активно развиваются беспроводные локальные сети, в которых информация передается посредством инфракрасного излучения или широкополосных радиосигналов. Эволюция сетевых технологий обусловлена, в первую очередь, совершенствованием самих компьютеров. Специалистами подсчитано, что мощность процессоров современных ПК удваивается каждые 18 месяцев, соответственно, растет и трафик, передаваемый по линиям компьютерных коммуникаций *(трафиком* называется общий суммарный поток информации через один сетевой компьютер). Вместе с тем наиболее узкое место в любой распределенной вычислительной системе — это устаревшее оборудование, поскольку уже довольно давно специалистами по компьютерным сетям было сформулировано простое правило: *максимальная пропускная способность локальной сети равна максимальной пропускной способности ее самого медленного компонента.* Из этого можно сделать вполне справедливый вывод, что эволюция сетевых стандартов во многом определяется ростом информационных потоков и производительности компьютеров, причем кривая роста производительности локальных сетей уже сейчас становится похожа на экспоненту: сети с пропускной способностью в 100 Мбит/с появились спустя 15 лет после возникновения 10-мегабитных сетей, сетевые системы с пропускной способностью в 1 Гбит/с были разработаны через 5 лет после 100-мегабитных сетей, первые проекты сетей со скоростью передачи данных в 10 Гбит/с родились спустя еще 2 года (рис. 1.1).

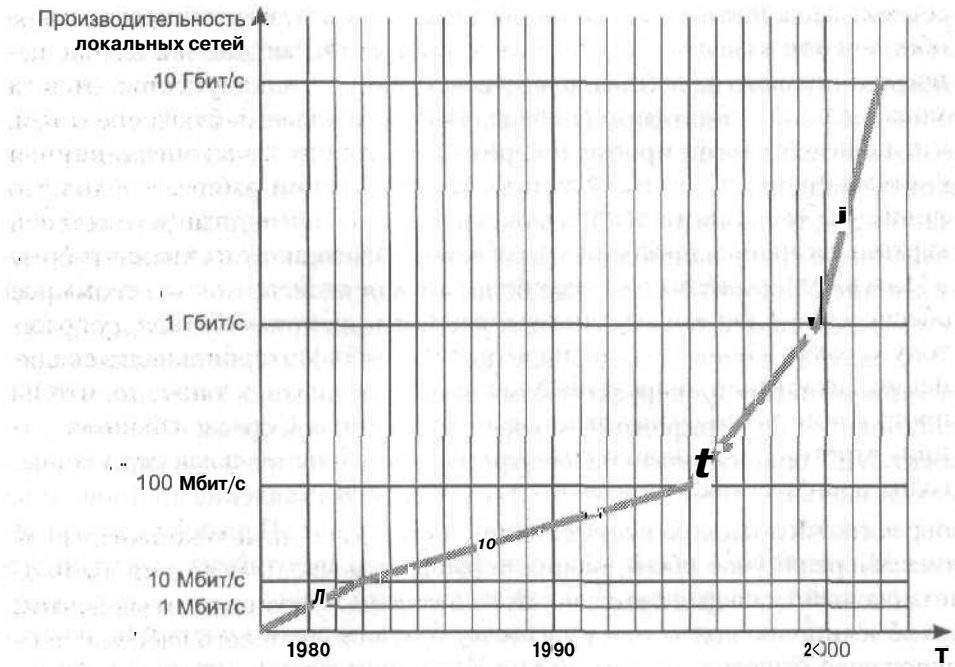


Рис. 1.1. Рост производительности локальных сетей

Тем не менее, несмотря на стремительное совершенствование сетевых технологий, они все же не поспевают за ростом вычислительной мощности современных персональных компьютеров. Для обоснования этою утверждения специалистами приводится два аргумента: во-первых, компьютеры, работающие в сети с вполне современной конфигурацией, обеспечивающей скорость передачи данных до 100 Мбит/с, принципиально способны обрабатывать намного большие потоки входящих и исходящих данных, во-вторых, современные приложения, такие как, например, Microsoft Office XP, способны полностью «утилизировать» эту пропускную способность под собственные потребности.

Разработчики программного обеспечения также стараются идти в ногу со временем. В офисных приложениях, программах обработки баз данных, прочих Intranet-приложениях в последнее время намечается устойчивая тенденция к обеспечению установки, деинсталляции, запуска и совместного использования программ в локальной сети, в них реализуется механизм хранения документов и баз данных на сетевых серверах, использования общих программных компонентов. В то же время с каждой новой версией прикладных программ растет и объем создаваемых этими программами файлов. А для пересылки и обработки таких документов требуется высокая скорость передачи данных.

Аналогичного курса стараются придерживаться и разработчики операционных систем. В частности, в ОС Microsoft Windows XP поддержка локальных сетей организована на небывало высоком уровне. Существует уверенность, что и в системных платформах последующих поколений будут совершенствоваться технологии приема и передачи управляемых мультимедийных потоков, поддержка видеоконференций, совместной работы с файлами. В частности, технология .NET демонстрирует нам очевидные перспективы дальнейшего сращивания локальных сетей с Интернетом. Основное предназначение Microsoft.NET — еще более тесная интеграция операционной системы с сетевыми технологиями и унификация применяемых для работы с сетью стандартов. Если раньше пользователь Интернета являлся просто «приемником» и «передатчиком» информации, то с появлением .NET он становится интегрированным участником сетевой среды. Прежде всего проект .NET ориентирован на электронную коммерцию и создание многофункциональных сетевых служб, а также на предоставление пользователю более широкого спектра возможностей в Интернете. Перспективы применения Microsoft.NET весьма широки. Например, получив из электронного магазина файл, содержащий счет за заказанный товар, пользователь сразу сможет импортировать его в программу бухгалтерского учета и включить в налоговую отчетность; загрузив из Интернета сводку котировок национальных валют, он получит возможность отредактировать ее в Word или Excel без сохранения в промежуточном формате.

Поскольку в основе Microsoft.NET лежит расширяемый язык разметки документов XML (Extensible Markup Language), данная технология может использоваться любыми приложениями и на любом оборудовании, а информация может передаваться по любым каналам связи. Специалисты Microsoft предлагают такой пример «нестандартного» использования Microsoft.NET: если автомобильная сигнализация в оставленной на офисной стоянке машине поддерживает интерфейс .NET, сигнал о попытке ее угона может быть передан непосредственно на компьютер пользователя. Тут же Windows предложит владельцу автомобиля различные варианты действий: автоматически вызвать полицию, заблокировать двигатель или отключить сигнализацию.

Данная технология позволяет организовать коммуникационную систему между компьютером, локальной сетью, мобильным телефоном, портативными устройствами (вроде карманных компьютеров), а также информационными центрами в Интернете. Однако ее полномасштабное применение — пока еще дело будущего.

Заметно упрощаются методы настройки, администрирования и использования локальных сетей. В частности, уже в операционной системе Microsoft Windows XP реализован целый ряд вспомогательных средств, которые

автоматически выполняют большую часть работы по настройке сети. В «домашней» локальной сети возможна организация одновременного доступа в Интернет с использованием одного компьютера, оснащенного обычным или кабельным модемом.

В операционных системах последних поколений значительно улучшена поддержка многосегментных малых сетей. Если один из входящих в сеть компьютеров соединяется с другими посредством беспроводной технологии Radio Ethernet, другой — через инфракрасный порт, а третий — по обычной «витой паре», в Windows 2000 каждый такой сегмент воспринимался как отдельная подсеть. От пользователя требовалось настроить протокол для головной машины каждого сетевого сегмента, назначить номера подсетей, указать алгоритмы передачи информации между сетями. Windows XP воспринимает многосегментные локальные сети как одну сеть, что значительно облегчает их настройку.

Безусловно, упрощенный вариант настройки сетевых подключений хорош для малых «домашних» сетей и не подходит для корпоративных распределенных систем. Именно поэтому в комплекте Windows XP предусмотрены механизмы более тонкой настройки и администрирования локальных сетей.

Также новые стандарты диктуют производители аппаратного обеспечения. В частности, возникновение стандарта Universal Plug&Play (UPnP) автоматически превращает локальные сети в незаменимый инструмент совместного использования конечного оборудования для различных прикладных задач.

Технология Plug&Play, позволяющая быстро подключать и настраивать в операционной системе новые периферийные устройства, уже хорошо знакома пользователям Windows. Universal Plug&Play дает возможность подключать к вашему компьютеру устройства, фактически расположенные на удаленном сетевом компьютере, и пользоваться ими так, словно они работают на вашей машине. При этом у вас не возникнет необходимости изменять какие-либо сетевые настройки: Windows самостоятельно подключит и настроит необходимое устройство. Вся «механика» обмена данными с удаленным оборудованием по сети также скрыта от владельца компьютера — он может просто пользоваться своей системой, не задумываясь о том, как она работает. Каждому сетевому устройству Windows XP динамически назначает собственный IP-адрес, благодаря чему различная периферийная аппаратура может самостоятельно обмениваться данными, получать сведения о характеристиках и состоянии другого работающего в сети устройства, сообщать информацию «о себе» и передавать свои ресурсы в распоряжение других пользователей. Например, если некий компьютер в локальной сети оснащен звуковой картой, поддерживающей Universal Plug&Play, но

его владелец в настоящий момент занят работой в Microsoft Word, пользователь другой сетевой машины может воспользоваться его саундбластером для запуска игры, требующей наличия в системе аудиооборудования. Естественно, при этом нет необходимости вскрывать корпус компьютера для переустановки устройства.

В настоящее время Universal Plug&Play может использоваться для подключения к компьютеру удаленных принтеров, видеокамер, цифровых фотокамер, сканеров. Однако специалисты Microsoft предполагают, что в недалеком будущем список оборудования, которое можно использовать в режиме Universal Plug&Play, будет расти. Самые смелые предположения писателей-фантастов воплотились в реальность: фактически Universal Plug&Play уже сейчас позволяет управлять подключаемой к компьютеру «интеллектуальной» бытовой техникой: программируемыми стиральными машинами, кухонными комбайнами, микроволновыми печами и даже автоматическими воротами гаража; при этом компьютер может играть роль своеобразного «центра управления домашней электроникой», задавая устройствам различные схемы и режимы работы. Дело за малым: дождаться поддержки Universal Plug&Play производителями конечного оборудования. Поскольку предложенный Microsoft стандарт построен по принципу открытой сетевой архитектуры, он независим от операционной системы и сетевой платформы, не привязан к какому-либо конкретному языку программирования или среде, через которую передается информация, будь то беспроводная сеть, оптоволоконная линия или Интернет. В силу того, что Universal Plug&Play не накладывает никаких ограничений на подмножество системных команд интерфейса операционной системы, которое могут использовать работающие с этим стандартом прикладные программы, разработчики программного обеспечения свободны в выборе средств для поддержки Universal Plug&Play.

Дальнейшие перспективы эволюции локальных сетей, видимо, вполне предсказуемы. Уже в ближайшем будущем заметно возрастет скорость передачи данных, будут разработаны новые алгоритмы коррекции ошибок, аутентификации пользователей и шифрования, что должно увеличить надежность соединений, получат более широкое развитие технологии беспроводной связи и локальные сети, построенные на основе оптического волокна. Однако наиболее популярными и недорогими на сегодняшний день все же остаются традиционные сети Ethernet, и именно о них пойдет разговор на страницах этой книги.

Глава 2

Сетевые протоколы

- Стеки протоколов
- Протоколы канального уровня
- Протоколы межсетевого уровня
- Транспортные протоколы
- Прикладные протоколы

Как уже упоминалось ранее, в локальных сетях могут совместно работать компьютеры разных производителей, оснащенные различным набором устройств и обладающие несхожими техническими характеристиками. На практике это означает, что для обеспечения нормального взаимодействия этих компьютеров необходим некий единый унифицированный стандарт, строго определяющий алгоритм передачи данных в распределенной вычислительной системе. В современных локальных сетях, или, как их принято называть в англоязычных странах, LAN (Local Area Network), роль такого стандарта выполняют сетевые протоколы.

Итак, *сетевым протоколом, или протоколом передачи данных, называется согласованный и утвержденный стандарт, содержащий описание правил приема и передачи между несколькими компьютерами команд, файлов, иных данных, и служащий для синхронизации работы вычислительных машин в сети.*

Прежде всего следует понимать, что в локальных сетях передача информации осуществляется не только между компьютерами как физическими устройствами, но и между приложениями, обеспечивающими коммуникации на программном уровне. Причем под такими приложениями можно понимать как компоненты операционной системы, организующие взаимодействие с различными устройствами компьютера, так и клиентские приложения, обеспечивающие интерфейс с пользователем. Таким образом, мы постепенно приходим к пониманию многоуровневой структуры сетевых коммуникаций — как минимум, с одной стороны мы имеем дело с аппаратной конфигурацией сети, с другой стороны — с программной.

Вместе с тем передача информации между несколькими сетевыми компьютерами — не такая уж простая задача, как это может показаться на первый взгляд. Для того чтобы понять это, достаточно представить себе тот круг проблем, который может возникнуть в процессе приема или трансляции каких-либо данных. В числе таких «неприятностей» можно перечислить аппаратный сбой либо выход из строя одного из обеспечивающих связь устройств, например, сетевой карты или концентратора, сбой прикладного или системного программного обеспечения, возникновение ошибки в самих передаваемых данных, потерю части транслируемой информации или ее искажение. Отсюда следует, что в локальной сети необходимо обеспечить жесткий контроль для отслеживания всех этих ошибок, и более того, организовать четкую работу как аппаратных, так и программных компонентов сети. Возложить все эти задачи на один-единственный протокол практически невозможно. Как быть?

Выход нашелся в разделении протоколов на ряд концептуальных уровней, каждый из которых обеспечивает интерфейс между различными модулями программного обеспечения, установленного на работающих в сети компьютерах. Таким образом, механизм передачи какого-либо пакета информации через сеть от клиентской программы, работающей на одном компьютере, клиентской программе, работающей на другом компьютере, можно условно представить в виде последовательной пересылки этого пакета сверху вниз от некоего протокола верхнего уровня, обеспечивающего взаимодействие с пользовательским приложением, протоколу нижнего уровня, организующему интерфейс с сетью, его трансляции на компьютер-получатель и обратной передачи протоколу верхнего уровня уже на удаленной машине (рис. 2.1).

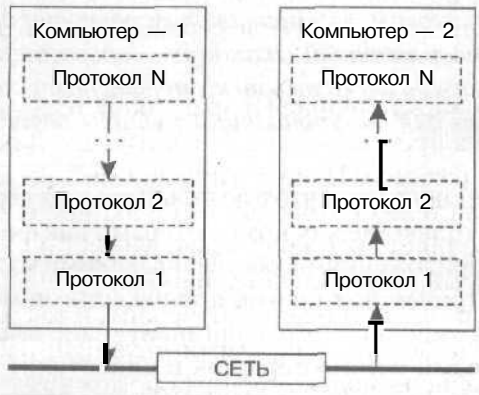


Рис. 2.1. Концептуальная модель многоуровневой системы протоколов

Согласно такой схеме, каждый из уровней подобной системы обеспечивает собственный набор функций при передаче информации по локальной сети.

Например, можно предположить, что протокол верхнего уровня, осуществляющий непосредственное взаимодействие с клиентскими программами, транслирует данные протоколу более низкого уровня, «отвечающему» за работу с аппаратными устройствами сети, преобразовывая их в «понятную» для него форму. Тот, в свою очередь, передает их протоколу, осуществляющему непосредственно пересылку информации на другой компьютер. На удаленном компьютере прием данных осуществляет аналогичный протокол «нижнего» уровня и контролирует корректность принятых данных, то есть определяет, следует ли транслировать их протоколу, расположенному выше в иерархической структуре, либо запросить повторную передачу. В этом случае взаимодействие осуществляется только между протоколами нижнего уровня, верхние уровни иерархии в данном процессе не задействованы. В случае если информация была передана без искажений, она транслируется вверх через соседние уровни протоколов до тех пор, пока не достигнет программы-получателя. При этом каждый из уровней не только контролирует правильность трансляции данных на основе анализа содержимого пакета информации, но и определяет дальнейшие действия исходя из сведений о его назначении. Например, один из уровней «отвечает» за выбор устройства, с которого осуществляется получение и через которое передаются данные в сеть, другой «решает», передавать ли информацию дальше по сети, или она предназначена именно этому компьютеру, третий «выбирает» программу, которой адресована принятая информация. Подобный иерархический подход позволяет не только разделить функции между различными модулями сетевого программного обеспечения, что значительно облегчает контроль работы всей системы в целом, но и дает возможность производить коррекцию ошибок на том уровне иерархии, на котором они возникли. Каждую из подобных иерархических систем, включающих определенный набор протоколов различного уровня, принято называть *стеком протоколов*.

Вполне очевидно, что между теорией и практикой, то есть между концептуальной моделью стека протоколов и его практической реализацией существует значительная разница. На практике принято несколько различных вариантов дробления стека протоколов на функциональные уровни, каждый из которых выполняет свой круг задач. Мы остановимся на одном из этих вариантов, который представляется наиболее универсальным. Данная схема включает четыре функциональных уровня, и так же, как и предыдущая диаграмма, описывает не конкретный механизм работы какого-либо стека протоколов, а общую модель, которая поможет лучше понять принцип действия подобных систем (рис. 2.2).

Самый верхний в иерархической системе, *прикладной уровень* стека протоколов обеспечивает интерфейс с программным обеспечением, организующим

работу пользователя в сети. При запуске любой программы, для функционирования которой требуется диалог с сетью, эта программа вызывает соответствующий протокол прикладного уровня. Данный протокол передает программе информацию из сети в доступном для обработки формате, то есть в виде системных сообщений либо в виде потока байтов. В точности таким же образом пользовательские приложения могут получать потоки данных и управляющие сообщения — как от самой операционной системы, так и от других запущенных на компьютере программ. То есть, обобщая, можно сказать, что протокол прикладного уровня выступает в роли своего рода посредника между сетью и программным обеспечением, преобразуя транслируемую через сеть информацию в «понятную» программе-получателю форму.

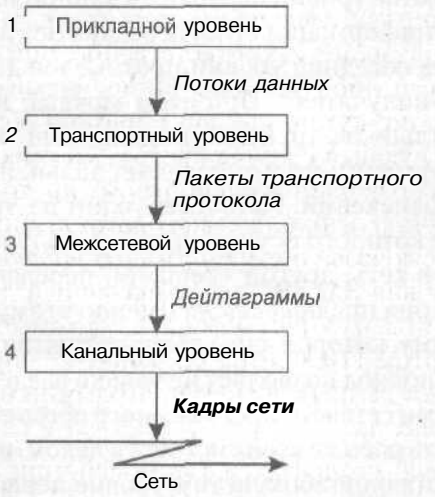


Рис. 2.2. Модель реализации стека протоколов

Основная задача протоколов *транспортного уровня* заключается в осуществлении контроля правильности передачи данных, а также в обеспечении взаимодействия между различными сетевыми приложениями. В частности, получая входящий поток данных, протокол транспортного уровня дробит его на отдельные фрагменты, называемые *пакетами,* записывает в каждый пакет некоторую дополнительную информацию, например идентификатор программы, для которой предназначены передаваемые данные, и контрольную сумму, необходимую для проверки целостности пакета, и направляет их на смежный уровень для дальнейшей обработки. Помимо этого протоколы транспортного уровня осуществляют управление передачей информации — например, могут запросить у получателя подтверждение доставки пакета и повторно выслать утерянные фрагменты транслируемой последовательности данных. Некоторое недоумение может вызвать то обстоятельство, что протоколы транспортного уровня так же, как и про-

токолы прикладного уровня, взаимодействуют с сетевыми программами и координируют передачу данных между ними. Эту ситуацию можно прояснить на следующем примере: предположим, на подключенном к сети компьютере запущен почтовый клиент, эксплуатирующий два различных протокола прикладного уровня — POP3 (Post Office Protocol) и SMTP (Simple Mail Transfer Protocol) — и программа загрузки файлов на удаленный сервер — FTP-клиент, работающий с протоколом прикладного уровня FTP (File Transfer Protocol). Все эти протоколы прикладного уровня опираются на один и тот же протокол транспортного уровня — TCP/IP (Transmission Control Protocol/Internet Protocol), который, получая поток данных от вышеуказанных программ, преобразует их в пакеты данных, где присутствует указание на конечное приложение, использующее эту информацию. Из рассмотренного нами примера следует, что данные, приходящие из сети, могут иметь различное назначение, и, соответственно, они обрабатываются различными программами, либо различными модулями одного и того же приложения. Во избежание путаницы при приеме и обработке информации каждая взаимодействующая с сетью программа имеет собственный идентификатор, который позволяет транспортному протоколу направлять данные именно тому приложению, для которого они предназначены. Такие идентификаторы носят название *программных портов.* В частности, протокол прикладного уровня SMTP, предназначенный для отправки сообщений электронной почты, работает обычно с портом 25, протокол входящей почты POP3 — с портом 110, протокол Telnet — с портом 23. Задача перенаправления потоков данных между программными портами лежит на транспортных протоколах.

На *межсетевом уровне* реализуется взаимодействие конкретных компьютеров распределенной вычислительной системы, другими словами, осуществляется процесс определения маршрута движения информации внутри локальной сети и выполняется отправка этой информации конкретному адресату. Данный процесс принято называть *маршрутизацией.* Получая пакет данных от протокола транспортного уровня вместе с запросом на его передачу и указанием получателя, протокол межсетевого уровня выясняет, на какой компьютер следует передать информацию, находится ли этот компьютер в пределах данного сегмента локальной сети или на пути к нему расположен шлюз, после чего трансформирует пакет в *дейтаграмму* — специальный фрагмент информации, передаваемый через сеть независимо от других аналогичных фрагментов, без образования виртуального канала (специально сконфигурированной среды для двустороннего обмена данными между несколькими устройствами) и подтверждения приема. В заголовок дейтаграммы записывается адрес компьютера-получателя пересылаемых данных и сведения о маршруте следования дейтаграммы. После чего она передается на канальный уровень.

ПРИМЕЧАНИЕ

Шлюз — это программа, при помощи которой можно передавать информацию между двумя сетевыми системами, использующими различные протоколы обмена данными.

Получая дейтаграмму, протокол межсетевого уровня определяет правильность ее приема, после чего выясняет, адресована ли она локальному компьютеру, или же ее следует направить по сети дальше. В случае, если дальнейшей пересылки не требуется, протокол межсетевого уровня удаляет заголовок дейтаграммы, вычисляет, какой из транспортных протоколов данного компьютера будет обрабатывать полученную информацию, трансформирует ее в соответствующий пакет и передает на транспортный уровень. Проиллюстрировать этот на первый взгляд сложный механизм можно простым примером. Предположим, на неком компьютере одновременно используется два различных транспортных протокола: TCP/IP — для соединения с Интернетом и NetBEUI (NetBIOS Extended User Interface) для работы в локальной сети. В этом случае данные, обрабатываемые на транспортном уровне, будут для этих протоколов различны, однако на межсетевом уровне информация будет передаваться посредством дейтаграмм одного и того же формата.

Наконец, на *канальном уровне* осуществляется преобразование дейтаграмм в соответствующий сигнал, который через коммуникационное устройство транслируется по сети. В самом простом случае, когда компьютер напрямую подключен к локальной сети того или иного стандарта посредством сетевого адаптера, роль протокола канального уровня играет драйвер этого адаптера, непосредственно реализующий интерфейс с сетью. В более сложных ситуациях на канальном уровне могут работать сразу несколько специализированных протоколов, каждый из которых выполняет собственный набор функций.

Протоколы канального уровня

Протоколы, обеспечивающие взаимодействие компьютера с сетью на самом низком, аппаратном уровне, во многом определяют топологию локальной сети, а также ее внутреннюю архитектуру. В настоящее время на практике достаточно часто применяется несколько различных стандартов построения локальных сетей, наиболее распространенными среди которых являются технологии Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI) и ArcNet.

На сегодняшний день локальные сети, построенные на основе стандарта Ethernet, являются наиболее популярными как в нашей стране, так и во всем мире. На долю сетей Ethernet приходится почти девяносто процентов всех малых и домашних локальных сетей, что не удивительно, поскольку

именно эта технология позволяет строить простые и удобные в эксплуатации и настройке локальные сети с минимумом затрат. Именно поэтому в качестве основного рассматриваемого нами стандарта будет принята именно технология Ethernet. Протоколы канального уровня поддержки Ethernet, как правило, встроены в оборудование, обеспечивающее подключение компьютера к локальной сети на физическом уровне. Стандарт Ethernet является широковещательным, то есть каждый подключенный к сети компьютер принимает всю следующую через его сетевой сегмент информацию — как предназначенную именно для этого компьютера, так и данные, направляемые на другую машину. Во всех сетях Ethernet применяется один и тот же алгоритм разделения среды передачи информации — множественный доступ с контролем несущей и обнаружением конфликтов (Carrier Sense Multiple Access with Collision Detection, CSMA/CD).

В рамках технологии Ethernet сегодня различается несколько стандартов организации сетевых коммуникаций, определяющих пропускную способность канала связи и максимально допустимую длину одного сегмента сети, то есть расстояние между двумя подключенными к сети устройствами. Об этих стандартах мы побеседуем в следующей главе, посвященной изучению сетевого оборудования, пока же необходимо отметить, что в рамках стандарта Ethernet применяется, как правило, одна из двух различных топологий: конфигурация сети с общей шиной или звездообразная архитектура.

Протоколы межсетевого уровня

Протоколы уровня межсетевого взаимодействия, как уже упоминалось ранее, предназначены для определения маршрутов следования информации в локальной сети, приема и передачи дейтаграмм, а также для трансляции принятых данных протоколам более высокого уровня, если эти данные предназначены для обработки на локальном компьютере. К протоколам межсетевого уровня принято относить протоколы маршрутизации, такие как RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол контроля и управления передачей данных ICMP (Internet Control Message Protocol). Но вместе с тем одним из самых известных протоколов межсетевого уровня является протокол IP.

Протокол IP

Протокол IP (Internet Protocol) используется как в глобальных распределенных системах, например в сети Интернет, так и в локальных сетях. Впервые протокол IP применялся еще в сети ArpaNet, являвшейся предтечей современного Интернета, и с тех пор он уверенно удерживает позиции в качестве одного из наиболее распространенных и популярных протоколов межсетевого уровня.

Поскольку межсетевой протокол IP является универсальным стандартом, он нередко применяется в так называемых составных сетях, то есть сетях, использующих различные технологии передачи данных и соединяемых между собой посредством шлюзов. Этот же протокол «отвечает» за адресацию при передаче информации в сети. Как осуществляется эта адресация?

Каждый человек, живущий на Земле, имеет адрес, по которому его в случае необходимости можно разыскать. Думаю, ни у кого не вызовет удивления то, что каждая работающая в Интернете или локальной сети машина также имеет свой уникальный адрес. Адреса в компьютерных сетях разительно отличаются от привычных нам почтовых. Боюсь, совершенно бесполезно писать на отправляемом вами в Сеть пакете информации нечто вроде «Компьютеру Intel Pentium III 1300 Mhz, эсквайру, Пэнни-Лэйн 114, Ливерпуль, Англия». Увидев такую надпись, ваша персоналка в лучшем случае фундаментально зависнет. Но если вы укажете компьютеру в качестве адреса нечто вроде 195.85.102.14, машина вас прекрасно поймет.

Именно стандарт IP подразумевает подобную запись адресов подключенных к сети компьютеров. Такая запись носит название **IP-адрес.**

Из приведенного примера видно, что IP-адрес состоит из четырех десятичных идентификаторов, или октетов, по одному байту каждый, разделенных точкой. Левый октет указывает тип локальной интрасети (под термином «интрасеть» (intranet) здесь понимается частная корпоративная или домашняя локальная сеть, имеющая подключение к Интернету), в которой находится искомый компьютер. В рамках данного стандарта различается несколько подвидов интрасетей, определяемых значением первого октета. Это значение характеризует максимально возможное количество подсетей и узлов, которые может включать такая сеть. В табл. 2.1 приведено соответствие классов сетей значению первого октета IP-адреса.

Таблица 2.1. Соответствие классов сетей значению первого октета IP-адреса

Класс сети	Диапазон значений первого октета	Возможное количество подсетей	Возможное количество узлов
A	1–126	126	16777214
B	128–191	16382	65534
C	192–223	2097150	254
D	224–239	—	2–28
E	240–247	—	2–27

Адреса класса A используются в крупных сетях общего пользования, поскольку позволяют создавать системы с большим количеством узлов. Адреса класса B, как правило, применяют в корпоративных сетях средних размеров, адреса класса C — в локальных сетях небольших предприятий. Для обращения к группам машин предназначены широковещательные

адреса класса D, адреса класса E пока не используются: предполагается, что со временем они будут задействованы с целью расширения стандарта. Значение первого октета 127 зарезервировано для служебных целей, в основном для тестирования сетевого оборудования, поскольку IP-пакеты, направленные на такой адрес, не передаются в сеть, а ретранслируются обратно управляющей надстройке сетевого программного обеспечения как только что принятые. Кроме того, существует набор так называемых «выделенных» IP-адресов, имеющих особое значение. Эти адреса приведены в табл. 2.2.

Таблица 2.2. Значение выделенных IP-адресов

IP-адрес	Значение
0.0.0.0	Данный компьютер
Номер сети.0.0.0	Данная IP-сеть
0.0.0.номер хоста	Конкретный компьютер в данной локальной IP-сети
1.1.1.1	Все компьютеры в данной локальной IP-сети
Номер сети.1.1.1	Все компьютеры в указанной IP-сети

ПРИМЕЧАНИЕ

Хостом принято называть любой подключенный к Интернету компьютер независимо от его назначения.

Как уже упоминалось ранее, небольшие локальные сети могут соединяться между собой, образуя более сложные и разветвленные структуры. Например, локальная сеть предприятия может состоять из сети административного корпуса и сети производственного отдела, сеть административного корпуса, в свою очередь, может включать в себя сеть бухгалтерии, планово-экономического отдела и отдела маркетинга. В приведенном выше примере сеть более низкого уровня является *подсетью* системы более высокого уровня, то есть локальная сеть бухгалтерии — подсеть для сети административного корпуса, а та, в свою очередь, — подсеть для сети всего предприятия в целом.

Однако вернемся к изучению структуры IP-адреса. Последний (правый) идентификатор IP-адреса обозначает номер компьютера в данной локальной сети. Все, что расположено между правым и левым октетами в такой записи, — номера подсетей более низкого уровня. Непопятно? Давайте разберем на примере. Положим, мы имеем некий адрес в Интернете, на который хотим отправить пакет с набором свеженьких анекдотов. В качестве примера возьмем тот же IP-адрес — 195.85.102.14. Итак, мы отправляем пакет в 195-ю подсеть сети Интернет, которая, как видно из значения первого октета, относится к классу C. Допустим, 195-я сеть включает в себя еще 902 подсети, но наш пакет высылается в 85-ю. Она содержит 250 подсетей

более низкого порядка, но нам нужна 102-я. Ну и, наконец, к 102-й сети подключено 40 компьютеров. Исходя из рассматриваемого нами адреса, подборку анекдотов получит машина, имеющая в этой сетевой системе номер 14. Из всего сказанного выше становится очевидно, что IP-адрес каждого компьютера, работающего как в локальной сети, так и в глобальных вычислительных системах, должен быть уникален.

Централизованным распределением IP-адресов в локальных сетях занимается государственная организация — Стенфордский международный научно-исследовательский институт (Stanford Research Institute, SRI International), расположенный в самом сердце Силиконовой долины — городе Мэнло-Парк, штат Калифорния, США. Услуга по присвоению новой локальной сети IP-адресов бесплатная, и занимает она приблизительно неделю. Связаться с данной организацией можно по адресу SRI International, Room EJ210, 333 Ravenswood Avenue, Menlo Park, California 94025, USA, по телефону в США 1-800-235-3155 или по адресу электронной почты, который можно найти на сайте http://www.sri.com. Однако большинство администраторов небольших локальных сетей, насчитывающих 5-10 компьютеров, назначают IP-адреса подключенным к сети машинам самостоятельно, исходя из описанных выше правил адресации в IP-сетях. Такой подход вполне имеет право на жизнь, но вместе с тем произвольное назначение IP-адресов может стать проблемой, если в будущем такая сеть будет соединена с другими локальными сетями или в ней будет организовано прямое подключение к Интернету. В данном случае случайное совпадение нескольких IP-адресов может привести к весьма неприятным последствиям, например к ошибкам в маршрутизации передаваемых по сети данных или отказу в работе всей сети в целом.

Небольшие локальные сети, насчитывающие ограниченное количество компьютеров, должны запрашивать для регистрации адреса класса C. При этом каждой из таких сетей назначаются только два первых октета IP-адреса, например 197.112.X.X, на практике это означает, что администратор данной сети может создавать подсети и назначать номера узлов в рамках каждой из них произвольно, исходя из собственных потребностей.

Большие локальные сети, использующие в качестве базового межсетевой протокол IP, нередко применяют чрезвычайно удобный способ структуризации всей сетевой системы путем разделения общей IP-сети на *подсети*. Например, если вся сеть предприятия состоит из ряда объединенных вместе локальных сетей Ethernet, то в ней может быть выделено несколько структурных составляющих, то есть подсетей, отличающихся значением третьего октета IP-адреса. Как правило, в качестве каждой из подсетей используется физическая сеть какого-либо отдела фирмы, скажем, сеть Ethernet, объединяющая все компьютеры бухгалтерии. Такой подход, во-первых, позволяет

излишне не расходовать IP-адреса, а во-вторых, предоставляет определенные удобства с точки зрения администрирования: например, администратор может открыть доступ к Интернету только для одной из вверенных ему подсетей или на время отключить одну из подсетей от локальной сети предприятия. Кроме того, в случае если сетевой администратор решит, что третий октет IP-адреса описывает номер подсети, а четвертый — номер узла в ней, то такая информация записывается в локальных таблицах маршрутизации сети вашего предприятия и не видна извне. Другими словами, данный подход обеспечивает большую безопасность.

Для того чтобы программное обеспечение могло автоматически выделять номера конкретных компьютеров из используемых в данной сетевой системе IP-адресов, применяются так называемые *маски подсети*. Принцип, по которому осуществляется распознавание номеров узлов в составе IP-адреса, достаточно прост: биты маски подсети, обозначающие номер самой IP-сети, должны быть равны единице, а биты, определяющие номер узла, — нулю. Именно поэтому в большинстве локальных IP-сетей класса С в качестве маски подсети принято значение 255.255.255.0: при такой конфигурации в состав общей сети может быть включено до 256 подсетей, в каждой из которых работает до 254 компьютеров. В ряде случаев это значение может изменяться, например, если возникла необходимость использовать в составе сети количество подсетей большее, чем 256, можно использовать маску подсети формата 255.255.255.195. В этой конфигурации сеть может включать до 1024 подсетей, максимальное число компьютеров в каждой из которых не должно превышать 60.

В локальных сетях, работающих под управлением межсетевого протокола IP, помимо обозначения IP-адресов входящих в сеть узлов принято также символьное обозначение компьютеров: например, компьютер с адресом 192.112.85.7 может иметь сетевое имя localhost. Таблица соответствий IP-адресов символьным именам узлов содержится в специальном файле hosts, хранящемся в одной из системных папок; в частности, в операционной системе Microsoft Windows XP этот файл можно отыскать в папке flHCK:\Windows\system32\drivers\etc\.Синтаксисзаписитаблицысопоставлений имен узлов локальной сети IP-адресам достаточно прост: каждый элемент таблицы должен быть расположен в новой строке, IP-адрес располагается в первом столбце, а за ним следует имя компьютера, при этом IP-адрес и имя должны быть разделены как минимум одним пробелом. Каждая из строк таблицы может включать произвольный комментарий, обозначаемый символом *n*. Пример файла hosts приведен ниже:

```
192.112.85.7       localhost  # этот компьютер
192.112.85.1       server     # сервер сети
192.112.85.2       director   # компьютер приемной директора
192.112.85.5       admin       # компьютер системного администратора
```

Как правило, файл hosts создается для какой-либо конкретной локальной сети, и его копия хранится на каждом из подключенных к ней компьютеров. В случае, если один из узлов сети имеет несколько IP-адресов, то в таблице соответствий обычно указывается лишь один из них, вне зависимости от того, какой из адресов реально используется. При получении из сети IP-пакета, предназначенного для данного компьютера, протокол IP сверится с таблицей маршрутизации и на основе анализа заголовка IP-пакета автоматически опознает любой из IP-адресов, назначенных данному узлу.

Помимо отдельных узлов сети собственные символьные имена могут иметь также входящие в локальную сеть подсети. Таблица соответствий IP-адресов именам подсетей содержится в файле networks, хранящемся в той же папке, что и файл hosts. Синтаксис записи данной таблицы сопоставлений несколько отличается от предыдущего, и в общем виде выглядит следующим образом:

```
<сетевое имя>  <номер сети>  [псевдонимы...]  [#<комментарий>]
```

где сетевое имя — имя, назначенное каждой подсети, номер сети — часть IP-адреса подсети (за исключением номеров более мелких подсетей, входящих в данную подсеть, и номеров узлов), псевдонимы — необязательный параметр, указывающий на возможные синонимы имен подсетей: они используется в случае, если какая-либо подсеть имеет несколько различных символьных имен; и, наконец, комментарий — произвольный комментарий, поясняющий смысл каждой записи. Пример файла networks приведен ниже:

```
loopback   127
marketing  192.112.85     # отдел маркетинга
buhgalteria   192.112.81   # бухгалтерия
workshop  192.112.80      # сеть производственного цеха
workgroup 192.112.10   localnetwork   # основная рабочая группа
```

Обратите внимание на то обстоятельство, что адреса, начинающиеся на 127, являются зарезервированными для протокола IP, а подсеть с адресом 192.112.10 в нашем примере имеет два символьных имени, используемых совместно.

Файлы hosts и networks не оказывают непосредственного влияния на принципиальный механизм работы протокола IP и используются в основном прикладными программами, однако они существенно облегчают настройку и администрирование локальной сети.

Протокол IPX

Протокол IPX (Internet Packet Exchange) является межсетевым протоколом, используемым в локальных сетях, узлы которых работают под управлением операционных систем семейства Nowell Netware. Данный протокол обеспечивает передачу дейтаграмм в таких сетях без организации

логического соединения — постоянного двустороннего обмена данными между двумя узлами сети, которое организуется протоколом транспортного уровня. Разработанный на основе технологий Nowell, этот некогда популярный протокол в силу несовместимости с чрезвычайно распространенным стеком протоколов TCP/IP в настоящее время медленно, но верно утрачивает свои позиции.

Как и межсетевой протокол IP, IPX способен поддерживать широковещательную передачу данных посредством дейтаграмм длиной до 576 байт, 30 из которых занимает заголовок пакета. В сетях IPX используются составные адреса узлов, состоящих из номера сети, адреса узла и адреса прикладной программы, для которой предназначен передаваемый пакет информации, который также носит наименование *гнезда* или *сокета*. Для обеспечения обмена данными между несколькими сетевыми приложениями в многозадачной среде на узле, работающем под управлением протокола IPX, должно быть одновременно открыто несколько *сокетов*.

Поскольку в процессе трансляции данных протокол IPX не запрашивает подтверждения получения дейтаграмм, доставка данных в таких сетях не гарантируется, и потому функции контроля над передачей информации возлагаются на сетевое программное обеспечение. Фактически IPX обеспечивает только инкапсуляцию транслируемых по сети потоков данных в дейтаграммы, их маршрутизацию и передачу пакетов протоколам более высокого уровня.

Протоколам канального уровня IPX передает пакеты данных, имеющие следующую логическую структуру:

- контрольная сумма, предназначенная для определения целостности передаваемого пакета (2 байта);
- указание на длину пакета (2 байта);
- данные управления транспортом (1 байт);
- адрес сети назначения (4 байта);
- адрес узла назначения (6 байт);
- номер сокета назначения (2 байта);
- адрес сети-отправителя (4 байта);
- адрес узла-отправителя (6 байт);
- номер сокета-отправителя (2 байта);
- передаваемая информация (0-546 байт).

Протоколы канального уровня размещают этот пакет внутри кадра сети и передают его в распределенную вычислительную систему.

Транспортные протоколы

Как уже упоминалось ранее, протоколы транспортного уровня обеспечивают контроль над передачей данных между межсетевыми протоколами и приложениями уровня операционной системы. В настоящее время в локальных сетях наиболее распространено несколько разновидностей транспортных протоколов.

Протокол TCP

Протокол IP позволяет только транслировать данные. Для того чтобы управлять этим процессом, служит протокол **TCP** (Transmission Control Protocol), опирающийся на возможности протокола IP. Как же контролируется передача информации?

Положим, вы хотите переслать по почте вашему другу толстый журнал, не потратив при этом денег на отправку бандероли. Как решить эту проблему, если почта отказывается принимать письма, содержащие больше нескольких бумажных листов? Выход простой: разделить журнал на страницы и отправлять их отдельными письмами. По номерам страниц ваш друг сможет собрать журнал целиком. Приблизительно таким же способом работает протокол TCP. Он дробит информацию на несколько частей, присваивает каждой части номер, по которому данные впоследствии можно будет соединить воедино, добавляет к ней «служебную» информацию и укладывает все это в отдельный «IP-конверт». Далее этот «конверт» отправляется по сети — ведь протокол межсетевого уровня умеет обрабатывать подобную информацию. Поскольку в такой схеме протоколы TCP и IP тесно связаны, их часто объединяют в одно понятие: **TCP/IP.** Размер передаваемых в Интернете TCP/IP-пакетов составляет, как правило, от 1 до 1500 байт, что связано с техническими характеристиками сети.

Наверняка, пользуясь услугами обычной почтовой связи, вы сталкивались с тем, что обычные письма, посылки и иные почтовые отправления теряются и приходят совсем не туда, куда нужно. Те же проблемы характерны и для локальных сетей. На почте такие неприятные ситуации решают руководители почтовых отделений, а в сетевых системах этим занимается протокол TCP. Если какой-либо пакет данных не был доставлен получателю вовремя, TCP повторяет пересылку до тех пор, пока информация не будет принята корректно и в полном объеме.

В действительности данные, передаваемые по электронным сетям, не только теряются, но зачастую искажаются из-за помех на линиях связи. Встроенные в TCP алгоритмы контроля корректности передачи данных решают и эту проблему. Одним из самых известных механизмов контроля правильности пересылки информации является метод, согласно которому в заголовок

каждого передаваемого пакета записывается некая контрольная сумма, вычисленная компьютером-отправителем. Компьютер-получатель по аналогичной системе вычисляет контрольную сумму и сравнивает ее с числом, имеющимся в заголовке пакета. Если цифры не совпадают, TCP пытается повторить передачу.

Следует отметить также, что при отправке информационных пакетов протокол TCP требует от компьютера-получателя подтверждения приема информации. Это организуется путем создания временных задержек при приеме-передаче — тайм-аутов, или ожиданий. Тем временем отправитель продолжает пересылать данные. Образуется некий объем уже переданных, но еще не подтвержденных данных. Иными словами, TCP организует двунаправленный обмен информацией, что обеспечивает более высокую скорость ее трансляции.

При соединении двух компьютеров их модули TCP следят за состоянием связи. При этом само соединение, посредством которого осуществляется обмен данными, носит название виртуального или логического канала.

Фактически протокол TCP является неотъемлемой частью стека протоколов TCP/IP, и именно с его помощью реализуются все функции контроля над передачей информации по сети, а также задачи ее распределения между клиентскими приложениями.

Протокол SPX

В точности так же, как протокол TCP для IP-сетей, для сетей, построенных на базе межсетевого протокола IPX, транспортным протоколом служит специальный протокол SPX (Sequenced Pocket eXchange). В таких локальных сетях протокол SPX выполняет следующий набор функций:

- инициализация соединения;
- организация виртуального канала связи (логического соединения);
- проверка состояния канала;
- контроль передачи данных;
- разрыв соединения.

Поскольку транспортный протокол SPX и межсетевой протокол IPX тесно связаны между собой, их нередко объединяют в общее понятие — семейство протоколов IPX/SPX. Поддержка данного семейства протоколов реализована не только в операционных системах семейства Nowell Netware, но и в ОС Microsoft Windows 9x/Me/NT/2000/XP, Unix/Linux и OS/2.

Протоколы NetBIOS/NetBEUI

Разработанный компанией IBM транспортный протокол NetBIOS (Network Basic Input/Output System) является базовым протоколом для локальных

сетей, работающих под управлением операционных систем семейств Nowell Netware и OS/2, однако его поддержка реализована также и в ОС Microsoft Windows, и в некоторых реализациях Unix-совместимых операционных систем. Фактически можно сказать, что данный протокол работает сразу на нескольких логических уровнях стека протоколов: на транспортном уровне он организует интерфейс между сетевыми приложениями в качестве надстройки над протоколами IPX/SPX, на межсетевом — управляет маршрутизацией дейтаграмм, на канальном уровне — организует обмен сообщениями между различными узлами сети.

В отличие от других протоколов, NetBIOS осуществляет адресацию в локальных сетях на основе уникальных имен узлов и практически не требует настройки, благодаря чему остается весьма привлекательным для системных администраторов, управляющих сетями с небольшим числом компьютеров. В качестве имен хостов протоколом NetBIOS используются значащие последовательности длиной в 16 байт, то есть каждый узел сети имеет собственное уникальное имя (permanent name), которое образуется из сетевого адреса машины с добавлением десяти служебных байтов. Кроме этого, каждый компьютер в сетях NetBIOS имеет произвольное символьное имя, равно как произвольные имена могут иметь логические рабочие группы, объединяющие несколько работающих совместно узлов — такие имена могут назначаться и удаляться по желанию системного администратора. Имена узлов служат для идентификации компьютера в сети, имена рабочих групп могут служить, в частности, для отправки данных нескольким компьютерам группы или для обращения к целому ряду сетевых узлов одновременно.

При каждом подключении к распределенной вычислительной системе протокол NetBIOS осуществляет опрос локальной сети для проверки уникальности имени узла; поскольку несколько узлов сети могут иметь идентичные групповые имена, определение уникальности группового имени не производится.

Специально для локальных сетей, работающих на базе стандарта NetBIOS, корпорацией IBM был разработан расширенный интерфейс для этого протокола, который получил название NetBEUI (NetBIOS Extended User Interface). Этот протокол рассчитан на поддержку небольших локальных сетей, включающих не более 150-200 машин, и по причине того, что данный протокол может использоваться только в отдельных сегментах локальных сетей (пакеты NetBEUI не могут транслироваться через мосты — устройства, соединяющие несколько локальных сетей, нередко использующих различную среду передачи данных или различную топологию), этот стандарт считается устаревшим и более не поддерживается операционной системой Microsoft Windows XP, хотя его поддержка имеется в ОС семейства Windows 9x/ME/2000.

Прикладные протоколы

Протоколы прикладного уровня служат для передачи информации конкретным клиентским приложениям, запущенным на сетевом компьютере. В IP-сетях протоколы прикладного уровня опираются на стандарт TCP и выполняют ряд специализированных функций, предоставляя пользовательским программам данные строго определенного назначения. Ниже мы кратко рассмотрим несколько прикладных протоколов стека TCP/IP.

Протокол FTP

Как следует из названия, протокол FTP (File Transfer Protocol) предназначен для передачи файлов через Интернет. Именно на базе этого протокола реализованы процедуры загрузки и выгрузки файлов на удаленных узлах Всемирной Сети. FTP позволяет переносить с машины на машину не только файлы, но и целые папки, включающие поддиректории на любую глубину вложений. Осуществляется это путем обращения к системе команд FTP, описывающих ряд встроенных функций данного протокола.

Протоколы POP3 и SMTP

Прикладные протоколы, используемые при работе с электронной почтой, называются SMTP (Simple Mail Transfer Protocol) и POP3 (Post Office Protocol), первый «отвечает» за отправку исходящей корреспонденции, второй — за доставку входящей.

В функции этих протоколов входит организация доставки сообщений e-mail и передача их почтовому клиенту. Помимо этого, протокол SMTP позволяет отправлять несколько сообщений в адрес одного получателя, организовывать промежуточное хранение сообщений, копировать одно сообщение для отправки нескольким адресатам. И POP3, и SMTP обладают встроенными механизмами распознавания адресов электронной почты, а также специальными модулями повышения надежности доставки сообщений,

Протокол HTTP

Протокол HTTP (Hyper Text Transfer Protocol) обеспечивает передачу с удаленных серверов на локальный компьютер документов, содержащих код разметки гипертекста, написанный на языке HTML или XML, то есть веб-страниц. Данный прикладной протокол ориентирован прежде всего на предоставление информации программам просмотра веб-страниц, веб-браузерам, наиболее известными из которых являются такие приложения, как Microsoft Internet Explorer и Netscape Communicator.

Именно с использованием протокола HTTP организуется отправка запросов удаленным http-серверам сети Интернет и обработка их откликов; помимо

этого HTTP позволяет использовать для вызова ресурсов Всемирной сети адреса стандарта доменной системы имен (DNS, Domain Name System), то есть обозначения, называемые URL (Uniform Resource Locator) вида http://www.domain.zone/page.htm (.html).

Протокол TELNET

Протокол TELNET предназначен для организации терминального доступа к удаленному узлу посредством обмена командами в символьном формате ASCII. Как правило, для работы с сервером по протоколу TELNET на стороне клиента должна быть установлена специальная программа, называемая telnet-клиентом, которая, установив связь с удаленным узлом, открывает в своем окне системную консоль операционной оболочки сервера. После этого вы можете управлять серверным компьютером в режиме терминала, как своим собственным (естественно, в очерченных администратором рамках). Например, вы получите возможность изменять, удалять, создавать, редактировать файлы и папки, а также запускать на исполнение программы на диске серверной машины, сможете просматривать содержимое папок других пользователей. Какую бы операционную систему вы ни использовали, протокол Telnet позволит вам общаться с удаленной машиной «на равных». Например, вы без труда сможете открыть сеанс UNIX на компьютере, работающем под управлением MS Windows.

Протокол UDP

Прикладной протокол передачи данных UDP (User Datagram Protocol) используется на медленных линиях для трансляции информации как дейтаграмм.

Дейтаграмма содержит полный комплекс данных, необходимых для ее отсылки и получения. При передаче дейтаграмм компьютеры не занимаются обеспечением стабильности связи, поэтому следует принимать особые меры для обеспечения надежности.

Схема обработки информации протоколом UDP, в принципе, такая же, как и в случае с TCP, но с одним отличием: UDP всегда дробит информацию по одному и тому же алгоритму, строго определенным образом. Для осуществления связи с использованием протокола UDP применяется система отклика: получив UDP-пакет, компьютер отсылает отправителю заранее обусловленный сигнал. Если отправитель ожидает сигнал слишком долго, он просто повторяет передачу.

На первый взгляд может показаться, что протокол UDP состоит сплошь из одних недостатков, однако есть в нем и одно существенное достоинство: прикладные интернет-программы работают с UDP в два раза быстрее, чем с его более высокотехнологичным собратом TCP.

Сквозные протоколы и шлюзы

Интернет — это единая глобальная структура, объединяющая на сегодня около 13 000 различных локальных сетей, не считая отдельных пользователей. Раньше все сети, входившие в состав Интернета, использовали сетевой протокол **IP.** Однако настал момент, когда пользователи локальных систем, не использующих IP, тоже попросились в лоно Интернета. Так появились шлюзы.

Поначалу через шлюзы транслировалась только электронная почта, но вскоре пользователям и этого стало мало. Теперь посредством шлюзов можно передавать любую информацию — и графику, и гипертекст, и музыку, и даже видео. Информация, пересылаемая через такие сети другим сетевым системам, транслируется с помощью сквозного протокола, обеспечивающего беспрепятственное прохождение IP-пакетов через не IP-сеть.

Глава 3

Архитектура сетей Ethernet

- Топология локальных сетей Ethernet
- Классификация сетей Ethernet
- Технические характеристики локальных сетей
- Некоторые особенности различных сетевых стандартов

В рамках этой книги мы рассмотрим локальные сети, созданные с использованием наиболее популярной и распространенной в наши дни технологии — Ethernet. Данная технология появилась в 70-е годы XX века, когда инженер-исследователь из Массачусетского технологического института Билл Меткалф, сотрудничавший также с исследовательским центром компании Xerox в г. Пало-Альто, подготовил докторскую диссертацию, посвященную методикам организации компьютерных коммуникаций. Вскоре совместно со специалистами из корпораций Intel и DEC (Digital Equipment Corporation) фирма Xerox разработала па основе этой диссертации коммерческий стандарт, который и получил название Ethernet. Чуть позже, в 1980 году, стандарт Ethernetлег в основу универсальной спецификации для локальных сетей, построенных по принципу множественного доступа, определения несущей частоты и автоматического обнаружения сбоев (Carrier Sense Multiple Access/Collision Detection, CSMA/CD); эта спецификация, разработанная Институтом инженеров по радиотехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE), получила название IEEE 802.3. Поскольку стандарты IEEE 802.3 и Ethernet крайне близки не только по своей идеологии, но и с точки зрения технической совместимости, в современной литературе их традиционно принято называть общим термином – Ethernet. Далее мы также будем придерживаться этой традиции.

Очевидно, что технология Ethernet накладывает собственные ограничения не только на архитектуру локальной сети, но и на ее технические характеристики. Причем подобные ограничения имеют несколько своеобразных логических уровней: с одной стороны, они определяют способ подключения

компьютеров к сети, с другой — подчеркивают различия между разными типами сетей по признаку используемого оборудования, типу кабеля или скорости передачи данных. Об этом мы и поговорим далее в этой главе.

Топология сетей Ethernet

В рамках стандарта Ethernet принято различать несколько типов построения распределенной вычислительной системы, исходя из ее топологической структуры. Фактически можно сказать, что топология локальной сети — это конфигурация кабельных соединений между компьютерами, выполненных по некоему единому принципу. Какая-либо конкретная топология сети выбирается, во-первых, исходя из используемого оборудования, которое, как правило, поддерживает некий строго определенный вариант организации сетевых подключений; во-вторых, на основе имеющихся требований к мобильности, масштабируемости и вычислительной мощности всей системы в целом. В ряде ситуаций возможна организация нескольких подсетей, построенных с использованием различных топологий и связанных впоследствии в единую сеть. В частности, применительно к стандарту Ethernet возможна организация локальных сетей с топологией «общая шина» или «звезда».

Топология «общая шина»

Технология построения локальной сети на основе топологии «общая шина» подразумевает последовательное соединение компьютеров в цепочку наподобие «гирлянды» с использованием специальных Т-образных разъемов (Т-коннекторов), подключаемых к соответствующему порту сетевого адаптера каждого из узлов сети. В качестве физической линии передачи данных применяется коаксиальный кабель с пропускной способностью 10 Мбит/с. Оконечности «цепочки», то есть ответвления Т-образных разъемов, к которым не подводится кабель для подсоединения к соседним компьютерам, ограничиваются специальными металлическими колпачками, создающими в сети необходимое сопротивление нагрузки, — они называются заглушками или терминаторами (рис. 3.1).

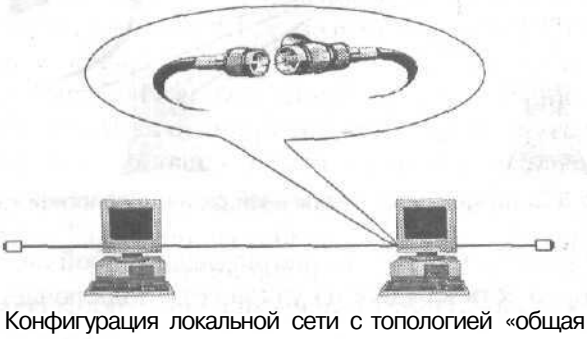


Рис. 3.1. Конфигурация локальной сети с топологией «общая шина»

Следует отметить, что некогда весьма популярные локальные сети с топологией «общая шина» в настоящее время все больше и больше утрачивают свои позиции. Причина снижения их популярности вполне очевидна. Несмотря на видимую простоту прокладки и монтажа, — а для постройки такой сети необходимы лишь минимальные навыки обращения с пассатижами или паяльником — и относительную мобильность с точки зрения изменения конфигурации всей системы (ведь для того, чтобы переставить сетевой компьютер с места на место, достаточно лишь открутить и закрутить соответствующий разъем), такие сети имеют множество очевидных недостатков. И самый существенный из них — крайне низкая надежность. Достаточно произойти потере контакта в одном из терминаторов или многочисленных Т-коннекторов, что на практике случается достаточно часто, и целый сегмент локальной сети выходит из строя. В такой ситуации все сетевые компьютеры продолжают работать вполне стабильно, но неожиданно перестают «видеть» друг друга, вследствие чего системному администратору приходится последовательно проходить всю сеть, проверяя наличие контакта в разъемах, что занимает порой очень много времени. Именно поэтому топология «общая шина» идеально подходит для создания малой домашней сети «точка—точка», то есть для объединения двух компьютеров, но в случае более сложной и разветвленной сетевой структуры следует поразмыслить о возможности использования иной конфигурации.

Топология «звезда»

Альтернативой топологии «общая шина» в сетях Ethernet является звездообразная конфигурация локальной сети (рис. 3.2).

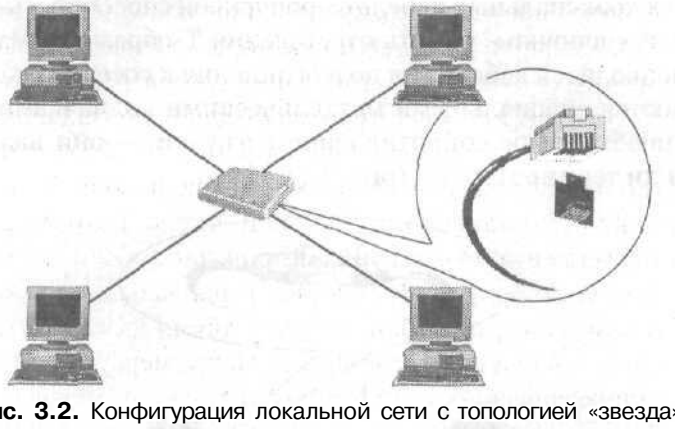


Рис. 3.2. Конфигурация локальной сети с топологией «звезда»

В этом случае компьютеры соединяются между собой не последовательно, а параллельно, то есть каждый из узлов сети подключается собственным

отрезком провода к соответствующему порту некоего устройства, называемого концентратором, или хабом (от англ. *hub* — центр). В качестве линии передачи данных используется специальный неэкранированный кабель «витая пара» (twisted pair), который обеспечивает соединение со скоростью до 10 Мбит/с, Посредством «витой пары» возможна также организация сети из двух компьютеров по принципу «точка—точка», при этом машины можно подключать друг к другу напрямую, без использования концентратора, однако порядок монтажа контактов в разъемах сетевого шнура в этом случае несколько отличается от стандартного.

Преимущества топологии «звезда» по сравнению с «общей шиной» заключаются в более высокой надежности и отказоустойчивости локальной сети, в ней значительно реже возникают «заторы», да и конечное оборудование работает по «витой паре» на порядок быстрее. При этом в случае выхода из строя одного из узлов сети вся остальная система продолжает работать стабильно: полный отказ такой локальной сети происходит только при поломке концентратора. Безусловно, организация сетевой системы на основе топологии «звезда» требует значительно больших финансовых затрат, но они целиком и полностью оправдываются, когда речь заходит о необходимости обеспечить надежную связь между работающими в сети компьютерами.

Классы сетей Ethernet

Прежде чем мы перейдем к непосредственному рассмотрению принципов организации локальной сети, необходимо сказать несколько слов о технологических классах, на которые делятся сети стандарта Ethernet. Данные классы различаются, прежде всего, пропускной способностью линий, типом используемого кабеля, топологией и некоторыми иными характеристиками, Каждый из классов сетей Ethernet имеет собственное обозначение, отражающее его технические характеристики, такое обозначение имеет вид *XBase/BroadY*, где X — пропускная способность сети, обозначение *Base* или *Broad* говорит о методе передачи сигнала — основополосный (baseband) или широкополосный (broadband), и, наконец, число У отображает максимальную длину сегмента сети в сотнях метров, либо обозначает тип используемого в такой системе кабеля, который и накладывает ограничения на максимально возможное расстояние между двумя узлами сети, исходя из собственных технических характеристик. Например, сеть класса *10Base2* имеет пропускную способность 10 Мбит/с, использует метод передачи данных baseband и допускает максимальную длину сегмента в 200 м. Далее мы рассмотрим несколько существующих классов сетей Ethernet и поговорим об их особенностях и возможностях.

Класс 10Base5 (Thick Ethernet)

Класс 10Base5, который также иногда называют «толстым Ethernet», — это один из наиболее старых стандартов локальных сетей. Сегодня уже очень трудно отыскать в продаже оборудование этого типа, тем более трудно найти действующую сеть, работающую с данным типом устройств.

Сети стандарта 10Base5 использовали топологию «общая шина» и создавались на основе коаксиального кабеля с волновым сопротивлением 50 Ом и пропускной способностью 10 Мбит/с. Общая шина локальной сети ограничивалась с обеих сторон терминаторами, однако помимо Т-коннекторов в подобных системах использовались специальные устройства, получившие общее название «трансиверы», которое произошло от совмещения английских понятий *transmitter* (передатчик) и *receiver (приемник)*. Собственно, трансиверы являлись приемниками и передатчиками данных между работающими в сети компьютерами и самой сетью (рис. 3.3).

Помимо функций собственно приемника-передатчика информации, трансиверы обеспечивали надежную электроизоляцию работающих в сети компьютеров, а также выполняли функции устройства, снижающего уровень посторонних электростатических помех. Максимальная длина коаксиального кабеля, протянутого между трансивером и сетевым адаптером компьютера (трансиверного кабеля) в таких сетях может достигать 25 м, максимальная длина одного сегмента сети (отрезка сети между двумя терминаторами) - 500 м, а минимальное расстояние между точками подключения — 2,5 м. Всего в одном сегменте сети 10Base5 может работать не более 100 компьютеров, при этом количество совместно работающих сегментов сети не должно превышать пяти.

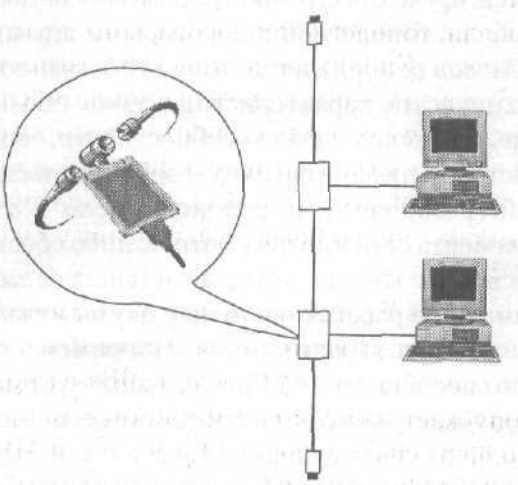


Рис. 3.3. Конфигурация локальной сети класса 10Base5

Класс 10Base2

Локальные сети, относящиеся к классу 10Base2, который также иногда называют Thin Ethernet, являются прямыми «наследницами» сетей 10Base5. Как и в предыдущем случае, для соединения компьютеров используется тонкий экранированный коаксиальный кабель с волновым сопротивлением 50 Ом, оснащенный Т-коннекторами и терминаторами, однако в такой конфигурации Т-коннекторы подключаются к разъему сетевой карты напрямую, без использования каких-либо промежуточных устройств (рис. 3.1). Соответственно, такая сеть имеет стандартную конфигурацию «общая шина».

Максимальная длина одного сегмента сети 10Base2 может достигать 185 м, при этом минимальное расстояние между точками подключения составляет 0,5 м. Наибольшее число компьютеров, подключаемых к одному сегменту такой сети, не должно превышать 30, максимально допустимое количество сегментов сети составляет 5. Пропускная способность данной сети, как это следует из обозначения ее класса, составляет 10 Мбит/с.

Класс lOBaseT (Ethernet на «витой паре»)

Одним из наиболее распространенных сегодня классов локальных сетей Ethernet являются сети lOBaseT. Как и стандарт 10Base2, такие сети обеспечивают передачу данных со скоростью 10 Мбит/с, однако используют в своей архитектуре топологию «звезда» и строятся с применением специального кабеля, называемого twisted pair, или «витая пара» (рис. 3.2).

Фактически витая пара представляет собой восьмижильный провод, в котором для обмена информации по сети используется лишь две пары проводников: одна — для приема сигнала, и одна — для передачи.

В качестве центрального звена в звездообразной структуре локальной сети lOBaseT применяется специальное устройство, называемое хабом, или концентратором. Для построения распределенной вычислительной системы, состоящей из нескольких сетевых сегментов, возможно подключение нескольких хабов в виде каскада, либо присоединение через хаб к сети lOBaseT локальной сети другого класса (рис. 3.4), однако следует учитывать то обстоятельство, что общее число точек подключения в такой системе не должно превышать 1024.

Максимально допустимое расстояние между узлами сети lOBaseT составляет 100 м, но можно сказать, что это значение взято скорее из практики построения таких сетей, поскольку стандарт lOBaseT предусматривает иное ограничение: затухание сигнала на отрезке между приемником и источником не должно превышать порога в 11,5 децибела. Именно данный класс локальных сетей наравне с 10Base2 будет подробно рассматриваться далее на страницах этой книги.

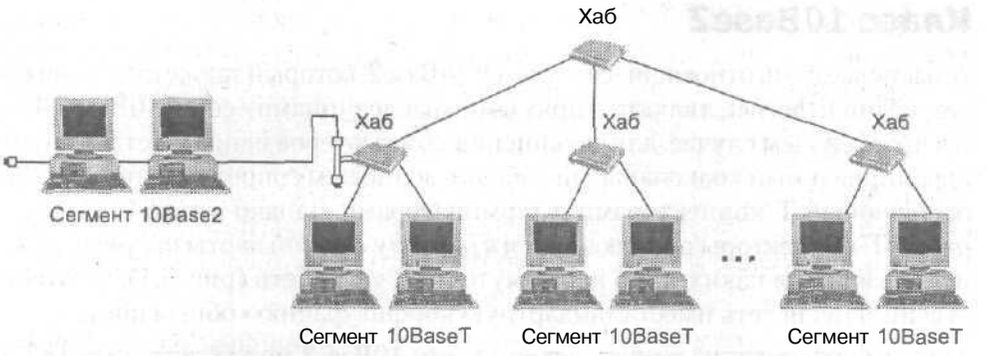


Рис. 3.4. Пример реализации многосегментной локальной сети Ethernet

Класс lOBaseF (Fiber Optic)

К классу lOBaseF (другое название — Fiber Optic) принято относить распределенные вычислительные сети, сегменты которых соединены посредством магистрального оптоволоконного кабеля, длина которого может достигать 2 км. Очевидно, что в силу высокой стоимости такие сети используются в основном в корпоративном секторе рынка и по карману они достаточно крупным предприятиям, располагающим необходимыми средствами для организации подобной системы.

Сеть lOBaseF имеет звездообразную топологию, которая, однако, несколько отличается от архитектуры, принятой для сетей lOBaseT (рис. 3.5).

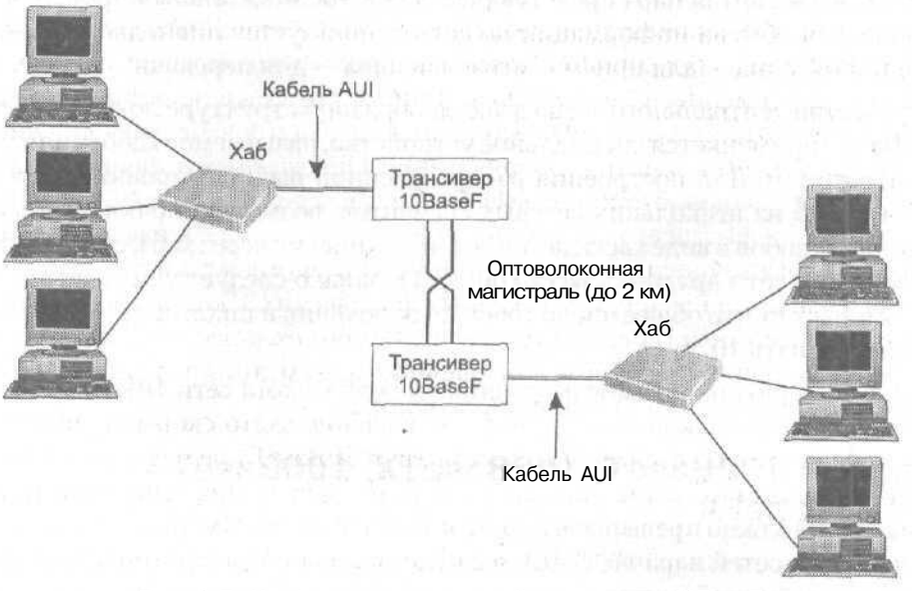


Рис. 3.5. Конфигурация локальной сети класса lOBaseF

Компьютеры каждого сегмента такой сети подключаются к ха.бу, который, в свою очередь, соединяется с внешним трансивером сети 10BaseF посредством специального коммуникационного шнура, подключаемого к 15-контактному разъему AUI (Attachment Unit Interface). Задача трансивера состоит в том, чтобы, получив из своего сегмента сети электрический сигнал, трансформировать его в оптический и передать в оптоволоконный кабель. Приемником оптического сигнала является аналогичное устройство, которое превращает его в последовательность электрических импульсов, направляемых в удаленный сегмент сети.

Преимущества оптических линий связи перед традиционными неоспоримы. Прежде всего диэлектрическое волокно, используемое в оптоволоконных кабелях в качестве волноводов, обладает уникальными физическими свойствами, благодаря которым затухание сигнала в такой линии крайне мало: оно составляет величину порядка 0,2 дБ на километр при длине волны 1,55 мкм, что потенциально позволяет передавать информацию на расстояния до 100 км без использования дополнительных усилителей и ретрансляторов. Кроме того, в оптических линиях связи частота несущего сигнала достигает 10^{14} Гц, а это означает, что скорость передачи данных по такой магистрали может составлять 10^{12} бит в секунду. Если принять во внимание тот факт, что несколько световых волн может одновременно распространяться в световоде в различных направлениях, то эту скорость можно значительно увеличить, организовав между конечными точками оптоволоконного кабеля двунаправленный обмен данными. Другой способ удвоить пропускную способность оптической линии связи заключается в одновременной передаче по оптоволокну нескольких волн с различной поляризацией. Фактически можно сказать, что на сегодняшний день максимально возможная скорость передачи информации по оптическим линиям пока еще не достигнута, поскольку достаточно жесткие ограничения на «быстродействие» подобных сетей накладывает конечное оборудование. Оно же «ответственно» и за относительно высокую стоимость всей системы в целом, поскольку диэлектрический кварцевый световод сам по себе значительно дешевле традиционного медного провода. В завершение можно упомянуть и тот факт, что оптическая линия в силу естественных физических законов абсолютно не подвержена воздействию электромагнитных помех, а также обладает существенно большим ресурсом долговечности, чем линия, изготовленная из стандартного металлического проводника.

Классы 100BaseT, 100BaseTX, 100BaseT4 и 100BaseFX

Класс локальных сетей 100BaseT, называемый также Fast Ethernet, появился относительно недавно: он был создан в 1992 году группой разработчиков,

называемой Fast Ethernet Alliance (FEA). Фактически Fast Ethernet является «наследником» сетей стандарта 10BaseT, однако в отличие от них позволяет передавать данные со скоростью до 100 Мбит/с.

Так же как и сети 10BaseT, локальные сети Fast Ethernet имеют звездообразную топологию и могут быть собраны с использованием кабеля различных типов, наиболее часто применяемым из которых является все та же пресловутая витая пара. В 1995 году данный стандарт был одобрен Институтом инженеров по радиотехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE) и вошел в спецификацию IEEE 802.3 (это расширение спецификации получило обозначение IEEE 802.3u), обретя тем самым официальный статус.

Поскольку класс сетей 100BaseT является прямым потомком класса 10BaseT, в таких системах используются стандартные для Ethernet протоколы передачи данных, а также стандартное прикладное программное обеспечение, предназначенное для администрирования локальной сети, что значительно упрощает переход от одного типа сети к другому. Предполагается, что в не столь отдаленном будущем эта технология вытеснит большинство существующих на сегодняшний день «устаревших» стандартов.

Поскольку в процессе разработки данной спецификации одной из основных задач являлось сохранение совместимости новой разновидности локальных сетей с различными типами кабеля, используемого в сетях старого образца, было создано несколько модификаций стандарта Fast Ethernet. Технология 100BaseTX подразумевает использование стандартной витой пары пятой категории, в которой задействовано только четыре проводника из восьми имеющихся: два — для приема данных, и два — для передачи. Таким образом, в сети обеспечивается двунаправленный обмен информацией и, кроме того, остается потенциальная возможность для дальнейшего наращивания производительности всей распределенной вычислительной системы. В сетях 100BaseT4 также используется витая пара, однако в ней задействованы все восемь жил проводника: одна пара работает только на прием данных, одна — только на передачу, а оставшиеся две обеспечивают двунаправленный обмен информацией. Поскольку технология 100BaseT4 подразумевает разделение всех транслируемых по сети данных на три независимых логических канала (прием, передача, прием-передача), пропорционально уменьшается частота сигнала, что позволяет прокладывать такие сети с использованием менее качественного и, следовательно, более дешевого кабеля 3 или 4 категории.

И, наконец, последний стандарт в семействе Fast Ethernet носит наименование 100BaseFX. Предназначен он для работы с оптоволоконными линиями связи.

Максимальная длина одного сегмента в сетях 100BaseT (кроме подкласса 100BaseFX) не превышает 100 м, в качестве конечного оборудования используются сетевые адаптеры и концентраторы, поддерживающие этот стандарт. Существуют также универсальные сетевые адаптеры 10BaseT/100BaseT. Принцип их работы состоит в том, что в локальных сетях этих двух классов используются одинаковые линии с одним и тем же типом разъемов, а задача автоматического распознавания пропускной способности каждой конкретной сети (10 Мбит/с или 100 Мбит/с) возлагается на протокол канального уровня, являющийся частью программного обеспечения самого адаптера. Алгоритм работы такого устройства можно проиллюстрировать на простом примере. При включении компьютера, оснащенного сетевым адаптером 10BaseT/100BaseT, последний выдает в сеть сигнал, информирующий другие сетевые устройства о том, что он способен поддерживать скорость передачи данных до 100 Мбит/с. Если оборудование локальной сети (например, хаб, к которому подключен данный компьютер) обеспечивает аналогичную скорость соединения, оно генерируют ответный сигнал, после чего адаптер продолжает работать в режиме 100BaseT. Если отклика не поступает, сетевая карта автоматически переходит в режим передачи данных со скоростью 10 Мбит/с, то есть переключается на работу в стандарте 10BaseT.

Несмотря на все преимущества спецификации 100BaseT, такие сети по сравнению с более старыми реализациями Ethernet не лишены и ряда недостатков, унаследованных ими от своего прародителя — стандарта 10BaseT. Прежде всего в моменты пиковой нагрузки, то есть в случае возникновения ситуации, при которой к ресурсам сети одновременно обращается более 50% всех узлов, на линии образуется хорошо знакомый пользователям 10BaseT «затор» — другими словами, сеть начинает заметно «тормозить». И во-вторых, если в распределенной вычислительной системе применяется комбинированная технология (одна часть сети работает со стандартом 10BaseT, другая — со стандартом 100BaseT), высокая скорость соединения будет возможна только па участке, поддерживающем пропускную способность в 100 Мбит/с. Поэтому даже если ваш компьютер оснащен сетевым адаптером 100BaseT, при обращении к удаленному узлу, оборудованному сетевой картой 10BaseT, скорость соединения не превысит 10 Мбит/с.

Класс 1000BaseT (Gigabit Ethernet)

Чем быстрее растут вычислительные мощности современных персональных компьютеров, тем больше становится среднестатистический объем обрабатываемых с их помощью файлов. Соответственно возникает потребность в пропорциональном увеличении пропускной способности линий

связи. В итоге это заметно ускорило процесс эволюции сетевых технологий: не успел окончательно прижиться стандарт 100BaseT, как ему на смену подоспел новый класс локальных сетей, позволяющих передавать информацию со скоростью до гигабита в секунду. Эти сети получили обозначение 1000BaseT и альтернативное название Gigabit Ethernet.

В архитектуре сетей lOOOBaseT используется топология «звезда» на базе высококачественного кабеля «витая пара» категории 5, в котором задействованы все восемь жил, причем каждая из четырех пар проводников используется как для приема, так и для передачи информации. По сравнению с технологией 100BaseT, несущая частота в сетях lOOOBaseT увеличена вдвое, благодаря чему достигается десятикратное увеличение пропускной способности линии связи. При переходе от стандарта lOBaseT или 100BaseT к l OOOBaseT особые требования предъявляются к качеству монтажа сетевых розеток и разъемов: если сеть проложена в полном соответствии с существующими стандартами, она, скорее всего, сможет обеспечить требуемую скорость передачи данных, если же монтаж был выполнен с отклонениями от требований спецификации Ethernet, возникающие в соединениях помехи не позволят добиться расчетных характеристик. Как и в более ранних классах сетей XBaseT, длина одного сегмента Gigabit Ethernet не должна превышать 100 м.

Стандарт lOOOBaseT был официально подтвержден Институтом инженеров по радиотехнике и электропике (Institute of Electrical and Electronic Engineers, IEEE) в 1999 году, и включен в спецификацию IEEE 802.3. В настоящее время оборудование для данного типа сетей выпускается несколькими независимыми производителями компьютерного «железа».

Устройства switch в сетях lOBaseT

Одновременно с разработкой новых, более высокоскоростных технологий передачи данных, перед производителями компьютерного оборудования по-прежнему стояла задача найти какие-либо способы увеличения производительности локальных сетей Ethernet старого образца, минимизировав при этом как финансовые затраты на приобретение новых устройств, так и технологические затраты на модернизацию уже имеющейся сети. Поскольку класс 10Base2 был единодушно признан всеми разработчиками «вымирающим», эксперты сосредоточились на технологии lOBaseT. И подходящее решение вскоре было найдено.

Как известно, стандарт Ethernet подразумевает использование алгоритма широковещательной передачи информации. Это означает, что в заголовке любого пересылаемого по сети блока данных присутствует информация

о конечном получателе этого блока, и программное обеспечение каждого компьютера локальной сети, принимая такой пакет, всякий раз анализирует его содержимое, пытаясь «выяснить», стоит ли передать данные протоколам более высокого уровня (если принятый блок информации предназначен именно этому компьютеру) или ретранслировать его обратно в сеть (если блок данных направляется на другую машину). Уже одно это заметно замедляет работу всей локальной сети. А если принять во внимание тот факт, что устройства, используемые в качестве центрального модуля локальных сетей с топологией «звезда» — концентраторы, или хабы — обеспечивают не параллельную, а последовательную передачу данных, то мы обнаруживаем еще одно «слабое звено», которое не только снижает скорость всей системы, но и нередко становится причиной «заторов» в случаях, когда, например, на один и тот же узел одновременно отсылается несколько потоков данных от разных компьютеров-отправителей. Если возложить задачу первоначальной сортировки пакетов на хаб, то эту проблему можно было бы частично решить. Что и было проделано. Так появилось на свет устройство, впоследствии названное switch, или коммутатор.

Switch полностью заменяет в структуре локальной сети 10BaseT хаб, да и выглядят эти два устройства практически одинаково, однако принцип работы коммутатора имеет целый ряд существенных различий. Основное различие заключается в том, что встроенное в switch программное обеспечение способно самостоятельно анализировать содержимое пересылаемых по сети блоков данных и обеспечивать прямую передачу информации между любыми двумя из своих портов независимо от всех остальных портов устройства. Давайте проиллюстрируем эту ситуацию на простом примере (рис. 3.6). Предположим, у нас имеется switch, оснащенный 16 портами. К порту 1 подключен компьютер А, который передает некую последовательность данных компьютеру С, присоединенному к 16-му порту. Б отличие от хаба, получив этот пакет данных, switch не ретранслирует его по всем имеющимся в его распоряжении портам в надежде, что рано или поздно он достигнет адресата, а проанализировав содержащуюся в пакете информацию, передает его непосредственно на 16-й порт. В то же самое время на порт 9 коммутатора приходит блок информации из другого сегмента локальной сети lOBaseT, подключенного к устройству через собственный хаб. Поскольку этот блок адресован компьютеру В, он сразу отправляется на порт 3, к которому тот присоединен. Следует понимать, что эти две операции switch выполняет одновременно и независимо друг от друга. Очевидно, что при наличии 16 портов мы можем одновременно направлять через switch 8 пакетов данных, поскольку порты задействуются парами. Таким образом, суммарная пропускная способность данного устройства составит 8 х 10 = 80 Мбит/с,

что существенно ускорит работу сети, в то время как па каждом отдельном подключении сохранится стандартное значение 10 Мбит/с. Другими словами, при использовании коммутатора мы уменьшаем время прохождения пакетов через сетевую систему, не увеличивая фактическую скорость соединения.

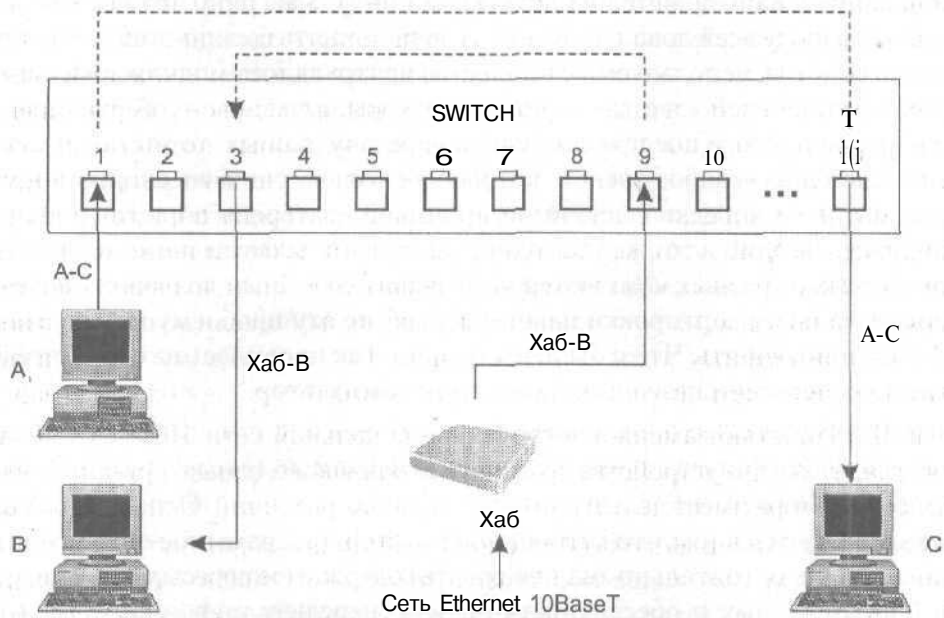


Рис. 3.6. Принцип работы устройства switch

Репитеры (повторители)

Ранее уже упоминалось о том, что в локальных сетях любого класса предусмотрены жесткие ограничения на длину участка сети между двумя точками подключения. Данные ограничения связаны, прежде всего, с коэффициентом затухания сигнала в линии передачи данных, который не должен превышать определенного порогового значения: в противном случае уверенный прием информации станет невозможен. Больше всего в этом случае выигрывают сети, построенные с применением линий из оптического волокна. Поскольку коэффициент затухания в этой среде очень мал, оптоволоконный кабель можно прокладывать на значительные расстояния без потери качества связи. Вместе с тем, упомянутый способ объединения удаленных сегментов LAN в единую систему достаточно дорог. Как быть, если на каком-либо предприятии эксплуатируется стандартная локальная сеть с пропускной способностью в 10 Мбит/с, отдельные участки которой,

например сеть бухгалтерии и склада, находятся на значительном удалении друг от друга, а перед руководством фирмы возникла необходимость объединить их между собой? Здесь нам на помощь приходят специальные устройства, называемые репитерами или повторителями.

Репитеры оснащены как минимум двумя, а иногда и большим числом сетевых портов с одним из стандартных интерфейсов, и присоединяются они непосредственно к локальной сети на максимально допустимом расстоянии от ближайшей точки подключения (для сетей класса lOBaseT оно составляет 100 м). Получив сигнал с одного из своих портов, репитер формирует его заново с целью исключить любые потери и искажения, произошедшие в процессе его передачи, после чего ретранслирует результирующий сигнал на все остальные порты. Таким образом, при прохождении сигнала через репитер происходит его усиление и очистка от посторонних помех. В некоторых случаях повторитель выполняет также функцию разделения ретранслируемых сигналов: если на одном из портов постоянно фиксируется поступление данных с ошибками, это означает, что в сегменте сети, подключенном через данный порт, произошла авария, и репитер перестает принимать сигналы с этого порта, чтобы не передавать ошибки всем остальным сетевым сегментам, то есть не транслировать их на всю сеть.

Вместе с тем при практическом использовании репитеров вступают в силу достаточно жесткие правила, регламентирующие их число и расположение в локальной сети. Основной недостаток повторителей заключается в том, что в момент прохождения сигналов через это устройство происходит заметная задержка при пересылке данных. Протоколы канального уровня Ethernet, использующие стандарт CSMA/CD, отслеживают сбои в процессе передачи информации, и если коллизия была зафиксирована, передача повторяется через случайный промежуток времени. В случае если число репитеров на участке между двумя компьютерами локальной сети превысит некоторое значение, задержки между моментом отправки и моментом приема данных станут настолько велики, что протокол попросту не сможет проконтролировать правильность пересылки данных, и обмен информацией между этими компьютерами станет невозможен. Отсюда возникло правило, которое принято называть «правилом 5-4-3». Формулируется оно следующим образом: на пути следования сигнала в сети Ethernet не должно встречаться более 5 сегментов и более 4 репитеров, причем только к 3 из них могут быть подключены конечные устройства (рис. 3.7, *а*).

При этом в целом в локальной сети может присутствовать более 4 повторителей, правило регламентирует только количество репитеров между двумя

любыми точками подключения. В некоторых случаях повторители устанавливают парами и объединяют между собой проводом, в этом случае между двумя компьютерами в сети не может присутствовать более двух таких пар (рис. 3.7, *б)*.

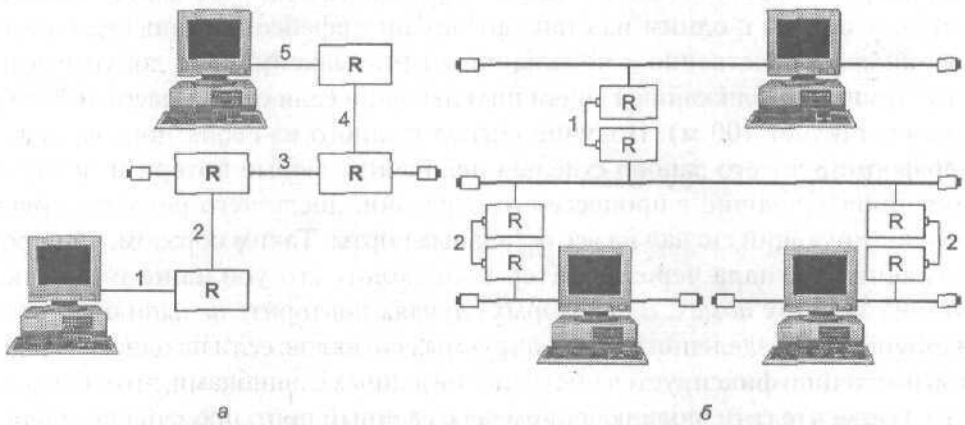


Рис. 3.7. Варианты подключения повторителей согласно «правилу 5-4-3»

Глава 4

Оборудование

- Общие сведения о сетевых адаптерах
- Установка и настройка сетевых адаптеров
- Сетевой кабель
- Концентраторы

Настало время побеседовать об оборудовании, используемом при построении локальных сетей. В этой главе мы обсудим технические особенности современных сетевых адаптеров, концентраторов, характеристики кабеля, изучим различные типы разъемов, с помощью которых выполняются соединения элементов локальной сети. А начнем мы, пожалуй, с рассмотрения самого важного компонента любой распределенной вычислительной системы — сетевой карты.

Сетевые адаптеры

Сетевые адаптеры, или сетевые карты, — это специальные устройства, основное назначение которых состоит в обеспечении двунаправленного обмена данными между персональным компьютером и локальной сетью. Являясь одним из элементов аппаратной конфигурации компьютера, таким же, как, например, модем, видеоадаптер или звуковая карта, сетевые адаптеры подключаются к ПК через один из стандартных портов, и настраиваются аналогично прочему оборудованию. В настоящее время принято различать несколько типов сетевых адаптеров по принципу используемого ими интерфейса как для соединения с компьютером, так и для подключения сетевого кабеля.

Моноинтерфейсные и комбинированные сетевые адаптеры

Как уже говорилось в предыдущей главе, сегодня самыми распространенными классами локальных сетей Ethernet являются 10Base2 и lOBaseT. Первые

создаются на основе коаксиального кабеля, и потому сетевые адаптеры, работающие с этим типом сетей, оснащены разъемами Bayonet Network Connector (BNC) (рис. 4.1).

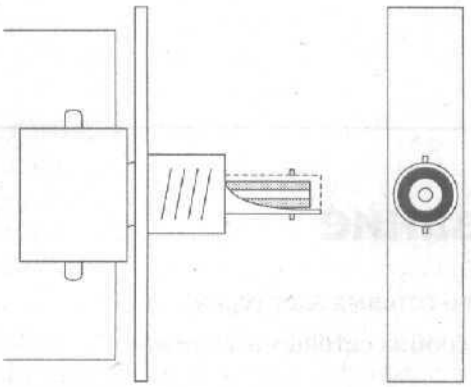


Рис. 4.1. Разъем BNC для локальных сетей 10Base2

Данные разъемы имеют цилиндрическую форму и внешне отдаленно напоминают приемное гнездо штекера телевизионной антенны. На внешней поверхности цилиндрической части разъема, как правило, имеется два небольших выступа высотой приблизительно в миллиметр, предназначенных для фиксации замка Т-коннектора.

Вторая разновидность сетевых карт рассчитана на работу с сетями класса lOBaseT и комплектуется разъемами RJ-45 (рис, 4.2).

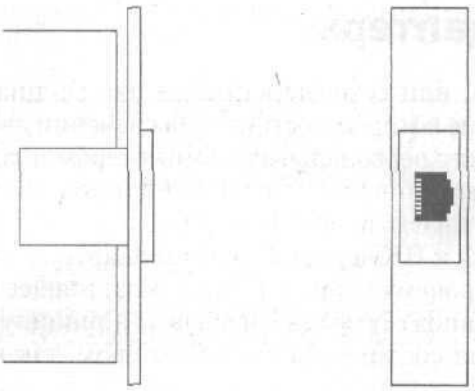


Рис. 4.2. Разъем RJ-45 для локальных сетей lOBaseT

Этот тип разъемов хорошо знаком владельцам модемов, современных телефонов и факсимильных аппаратов — внешне он очень похож на контактные гнезда данных устройств, к которым подключается телефонная линия. Разъем RJ-45 имеет вид углубления прямоугольной формы с небольшим

пазом для замка сетевой вилки, в нижней части гнезда расположено восемь контактов, соединяющихся с соответствующими контактами вилки сетевого кабеля.

Сетевые адаптеры, оборудованные разъемом только какого-либо одного типа, например, BNC или RJ-45, принято называть моноинтерфейсными. Существуют также сетевые карты, на которых присутствуют разъемы обоих типов — их называют комбинированными.

Ответ на вопрос о том, сетевые карты какого типа следует приобретать при проектировании небольшой локальной сети, очевиден: комбинированные адаптеры позволяют планировать прокладку сети с большей гибкостью при выборе различных вариантов — в случае необходимости вы можете без всякого труда заменить витую пару на коаксиальный кабель и наоборот. Для крупных современных локальных сетей, которые должны отвечать критериям высокой надежности и масштабируемости, вполне подойдут **моноинтерфейсные** сетевые адаптеры с разъемом стандарта RJ-45, поскольку такие сети относятся, как правило, к классу lOBaseT и не используют другие сетевые интерфейсы.

Сетевые адаптеры ISA, PCI и USB

Другой критерий, согласно которому принято классифицировать сетевые карты, подразумевает различие всех имеющихся на современном рынке адаптеров по простому признаку — а именно, порту, посредством которого сетевая карта соединяется с компьютером. Всего существует три наиболее широко распространенных варианта, и первый из них — это сетевые адаптеры, подключаемые к материнской плате ПК через шину ISA (рис. 4.3).

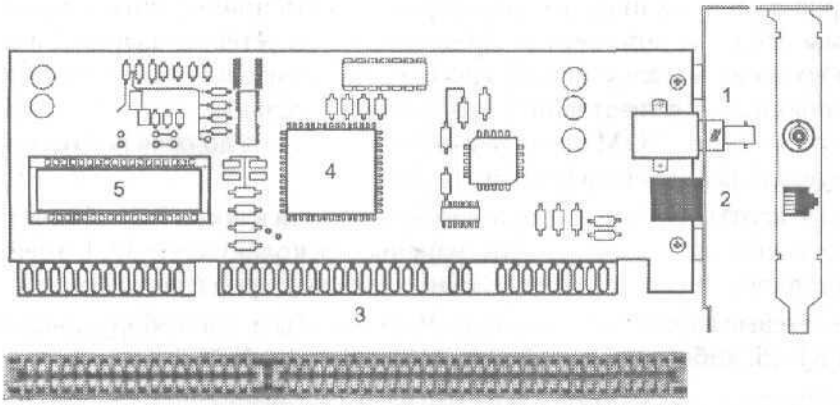


Рис. 4.3. Сетевой адаптер ISA:
1 — разъем BNC для сетей 10Base; *2* — разъем RJ-45 для сетей lOBaseT;
3— шина ISA; *4*— микропроцессор сетевого адаптера (чипсет);
5— панель для подключения микросхемы BootROM

Основной отличительной особенностью сетевых карт этого типа, позволяющей определить возможность ее подключения к слоту ISA, что называется, «на глаз», является удлиненная нижняя часть платы, на которой расположены контакты для соединения с портом — контактная площадка на сетевых адаптерах PCI заметно короче. Карты ISA бывают как моноинтерфейсными, так и комбинированными.

Сетевые адаптеры данного класса в настоящее время встречаются все реже и реже, поскольку большинство материнских плат современной конфигурации более не поддерживает шину ISA, считающуюся к настоящему времени «устаревшей». Связано это с некоторыми техническими характеристиками данного стандарта. Например, устройства ISA не позволяют автоматически перераспределять аппаратные прерывания, вследствие чего нередко становятся виновниками конфликтов оборудования. Именно поэтому такие сетевые платы стоят сейчас в магазинах очень дешево — всего лишь от пяти до пятнадцати долларов. По этой же причине прежде, чем приобретать подобный сетевой адаптер, следует убедиться, что на материнской плате вашего компьютера присутствует слот ISA.

Как правило, практически все современные сетевые адаптеры имеют на своей плате специальный разъем, позволяющий подключать микросхему BootROM. BootROM — это специальная микросхема постоянной памяти, при использовании которой становится возможна загрузка операционной системы на компьютер с удаленного узла локальной сети. Подобный подход позволяет подключать к сети компьютеры, не оснащенные дисковыми накопителями, такими как дисководы, приводы CD-ROM и жесткие диски, что, во-первых, означает экономию средств, а во-вторых не позволяет пользователям работать с машиной напрямую, то есть вставлять диски, копировать на них информацию или запускать принесенные с собой программы. Нередко компьютеры, оборудованные сетевым адаптером с такой микросхемой, используются в качестве повторителей или аппаратно-программных маршрутизаторов в небольших локальных сетях. При покупке микросхемы BootROM следует учитывать, что она должна подходить к используемой вами модели сетевого адаптера.

Сетевые карты другой категории подключаются к шине PCI. На сегодняшний день они наиболее распространены, поскольку слот PCI имеется на материнских платах всех современных компьютеров (рис. 4.4).

Как и сетевые карты ISA, адаптеры PCI могут быть либо оборудованы разъемом RJ-45, либо иметь комбинированный интерфейс.

К отдельному классу можно отнести сетевые адаптеры, подключаемые к шине USB (Universal Serial Bus, рис. 4.5). Такие сетевые адаптеры реализованы в виде внешнего устройства, присоединяющегося к USB-порту компьютера посредством специального кабеля и не требующие отдельного питания.

Практически все они ориентированы на использование в локальных сетях стандарта lOBaseT/lOOBaseT и оборудованы разъемом RJ-45 для витой пары.

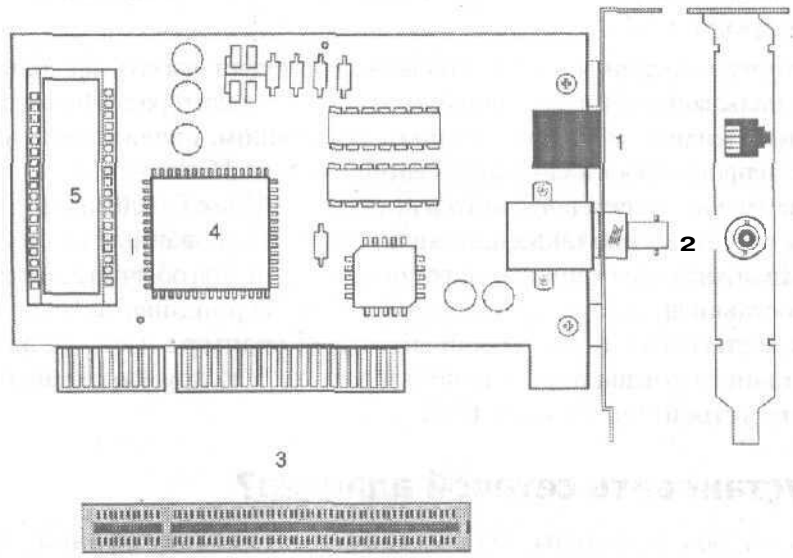


Рис. 4.4. Сетевой адаптер PCI:
1 — разъем RJ-45 для сетей 10BaseT; *2*— разъем BNC для сетей 10Base2;
3— шина PCI; *4*— микропроцессор сетевого адаптера (чипсет);
5— панель для подключения микросхемы BootROM

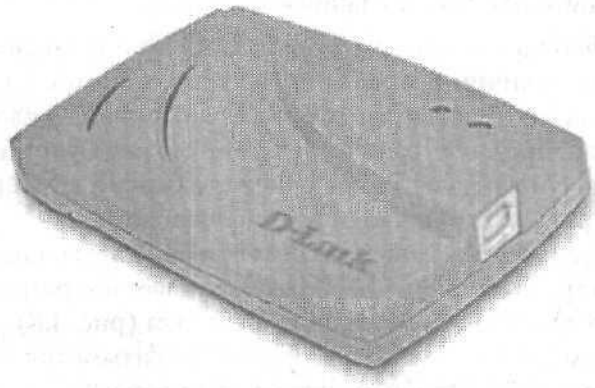


Рис. 4.5. Сетевой адаптер USB

Поскольку сетевые адаптеры USB появились в продаже относительно недавно, по крайней мере, по сравнению с их предшественниками, поддерживающими стандарты ISA и PCI, их технические характеристики выглядят гораздо более привлекательно. Данные устройства практически не требуют настройки (за исключением необходимости установки соответствующих

драйверов), работают достаточно быстро, автоматически выбирают свободное аппаратное прерывание, что позволяет избежать конфликтов с другим оборудованием, используют 32-битный доступ к шине данных и, как правило, не требуют I/O адресации.

Рассматривая различные типы сетевых карт, следует сказать несколько слов и о так называемых интегрированных сетевых адаптерах. Некоторые современные модели материнских плат, в основном, предназначенных для установки процессоров класса Intel Pentium IV и Intel Celeron 1400-2400 MHz, имеют встроенный сетевой адаптер стандарта 10BaseT/100BaseT. Отличительной особенностью таких плат является смонтированный на них разъем RJ-45. Драйверы интегрированного сетевого адаптера обычно входят в комплект поставки драйверов материнской платы. В принципе, ничто не мешает пользователю отключить встроенный сетевой адаптер в настройках CMOS персонального компьютера и использовать любую другую сетевую карту, например устройство PCI или USB.

Как установить сетевой адаптер?

Для того чтобы установить на своем компьютере «внутренний» сетевой адаптер, подключаемый к шине ISA или PCI, вам необходимо проделать предложенную далее последовательность действий.

1. Выключите питание компьютера.
2. Откройте корпус компьютера, открутив фиксирующие винты боковой стенки системного блока и удалив его крышку.
3. Выберите свободный слот, в который вы будете устанавливать сетевой адаптер. При наличии нескольких свободных слотов одного типа (например, на плате имеется 3 незанятых разъема PCI) слот выбирается, исходя из вашего удобства: впоследствии можно будет без всяких проблем извлечь сетевой адаптер из одного разъема и вставить в соседний, причем настройки устройства от этого не изменятся. Определить, какой тип слота подходит для вашей модели сетевой карты, также не составляет большого труда: разъемы ISA более длинные, чем разъемы PCI, и они, как правило, выполнены из черного пластика (рис. 4.6). Не опасайтесь ошибочно поместить сетевой адаптер не в тот разъем, поскольку контактная часть платы всех подобных устройств имеет специальный вырез или «ключ», который, во-первых, позволяет надежнее зафиксировать устройство в порту, а во-вторых, исключает его неправильную установку. Следует иметь в виду, что большинство современных материнских плат не имеет разъемов ISA, вместо этого на них расположен дополнительный, еще более короткий, чем PCI, разъем AGP, предназначенный для подключения ряда специфических устройств, например видеоадаптеров.

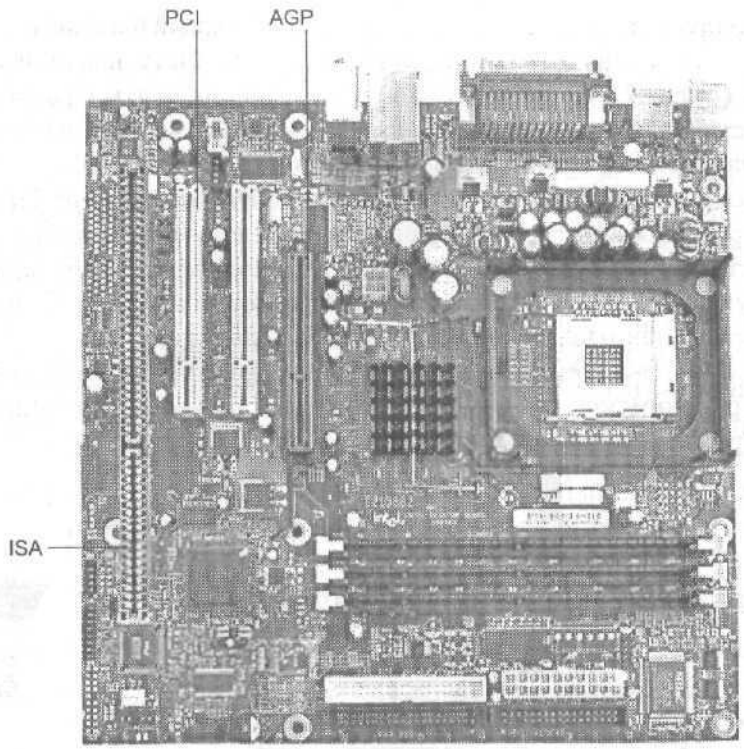


Рис. 4.6. Расположение слотов ISA и PCI на материнской плате компьютера

4. В случае, если расположенное на задней стенке системного блока отверстие, в котором размещается интерфейсная панель периферийных устройств, закрыто заглушкой, удалите ее. Заглушки бывают двух типов: съемные - они прикреплены к фиксирующей полке винтами и повторяют своей формой профиль задней стенки системного блока, и вырубленные, то есть продавленные специальным штампующим прессом при изготовлении корпуса компьютера. Съемную заглушку необходимо отвинтить. Не забудьте, что винт, посредством которого крепится заглушка, нужно сохранить, поскольку он понадобится вам для того, чтобы зафиксировать в корпусе сетевой адаптер. Вырубленную заглушку следует аккуратно отогнуть отверткой и осторожно выломать, стараясь не повредить при этом материнскую плату. Удаляйте только ту заглушку, которая соответствует выбранному вами для установки карты слоту — определить нужное отверстие в задней стенке корпуса можно, приложив сетевой адаптер к соответствующему разъему на материнской плате.
5. Аккуратно вставьте адаптер в разъем. Внимательно следите за тем, чтобы в процессе установки платы не возникло перекосов, а контакты сетевой карты плотно прилегали к соответствующим контактам слота.

Рекомендуется предварительно уложить системный блок компьютера на бок, поскольку значительно удобнее вставлять плату, надавливая на нее сверху (рис. 4.7). С целью улучшить соединение платы с разъемом следует устанавливать ее в два этапа. Для этого поместите пальцы одной руки на верхнюю часть платы ближе к металлической лицевой пластине, а пальцы другой руки — ближе к тыльной части адаптера. Приложите адаптер к разъему и слегка надавите на ее тыльную часть до тех пор, пока контактная площадка не войдет в слот наполовину, затем надавите на лицевую часть — плата должна полностью войти в разъем. Если с первого раза установить адаптер не удалось, не следует давить на него с усилием во избежание возможной поломки других устройств, вытащите адаптер и попытайтесь вставить его снова. Поместив плату в слот, зафиксируйте ее крепежным винтом.

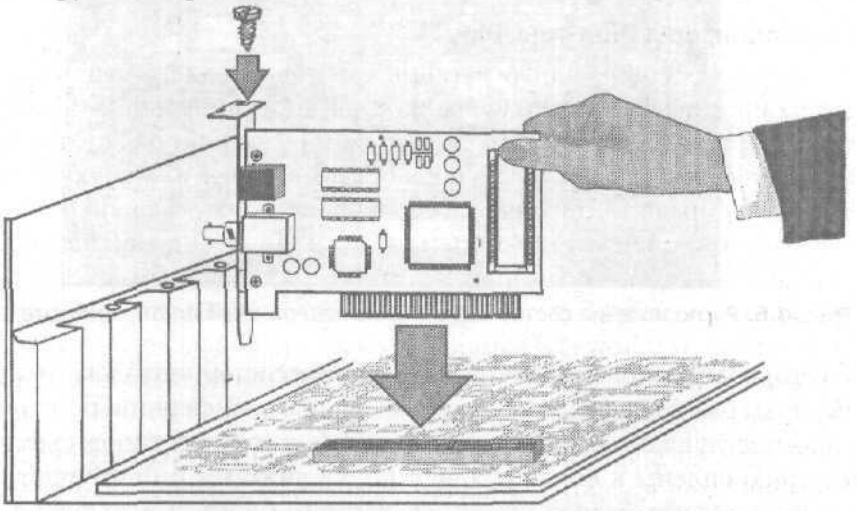


Рис. 4.7. Установка сетевого адаптера в разъем на материнской плате

6. Закройте крышку системного блока и закрепите ее соответствующими винтами.
7. Включите питание компьютера.

В случае если вы используете сетевой адаптер USB, его следует присоединить к соответствующему порту, расположенному на задней стенке системного блока компьютера, посредством специального шнура. К адаптеру, в свою очередь, подключается сетевой кабель 10BaseT/100BaseT. После выполнения этих операций можно переходить к установке драйверов.

Интегрированные сетевые адаптеры также не требуют дополнительной настройки и установки. Для того чтобы подготовить их к работе, достаточно установить соответствующие драйверы, которые входят обычно в комплект поставки программного обеспечения материнской платы.

Настройка сетевого адаптера

Порядок настройки сетевой карты зависит от ее модели и конфигурации. Большинство современных сетевых карт поддерживают стандарт Plug-And-Play, и операционная система автоматически обнаруживает эти устройства после их установки и включения питания компьютера: при этом пользователю достаточно лишь указать в соответствующем окне, откуда система должна копировать соответствующие драйверы. Более старые сетевые адаптеры (в основном, подключаемые к шине ISA) не определяются в Windows автоматически и требуют настройки вручную. В ряде случаев на самой плате сетевого адаптера имеется набор перемычек или переключателей, посредством которых можно выставить режим его настройки. Внимательно ознакомьтесь с технической документацией вашей сетевой карты прежде, чем приступить к ее конфигурированию.

Сетевые адаптеры Plug-And-Play

Практически все современные сетевые адаптеры поддерживают стандарт Plug-And-Play, позволяющий операционной системе выполнять автоматическую настройку подключаемых к компьютеру устройств. После установки таких сетевых карт, включения питания компьютера и загрузки Windows, на экране, как правило, появляется сообщение «обнаружено новое устройство» с предложением указать источник для копирования драйверов, которые поставляются обычно на дискете вместе с сетевой картой. В некоторых случаях может не потребоваться даже этого: в частности, операционная система Microsoft Windows XP самостоятельно определяет и настраивает сетевые адаптеры, совместимые с моделью NE 2000, используя для этого стандартные драйверы Microsoft.

После установки драйверов и перезагрузки компьютера сетевой адаптер фактически готов к работе. Однако в некоторых случаях автоматическая настройка Plug-And-Play-адаптеров происходит некорректно, и в результате возникают аппаратные конфликты между сетевой картой и иным оборудованием. Как правило, подобные ситуации бывают вызваны тем, что несколько различных устройств начинают несанкционированно использовать одни и те же ресурсы, например запрос на прерывание (IRQ, Interrupt Request), адреса каналов непосредственного доступа к памяти (DMA, Direct Memory Access) или диапазон ввода-вывода (I/O Range). Решить эту проблему можно одним из перечисленных ниже способов.

1. Во время перезагрузки компьютера войдите в настройки BIOS, перейдите в раздел конфигурации шины PCI или ISA, позволяющий изменить назначенные различным слотам этих шин аппаратные прерывания, и освободите одно из прерываний для соответствующей шины, которое будет впоследствии автоматически назначено сетевому адаптеру. Например, если известно, что ваш сетевой адаптер, подключенный к слоту PCI,

требует прерывание 20, назначьте для одного из слотов шины PCI значение IRQ = 20. Если это не помогло, можно поступить так, как показано в следующем пункте.

2. Переместив на плате сетевого адаптера соответствующую перемычку или переключатель либо воспользовавшись программой-конфигуратором сетевого адаптера, отключите режим Plug-And-Play для сетевой карты. Далее ее можно настроить как аппаратно-конфигурируемое или программно-конфигурируемое устройство.

Программно-конфигурируемые сетевые адаптеры

Программно-конфигурируемые сетевые адаптеры (Software configuration LAN adapters) — это, как правило, сетевые карты старых моделей, для настройки которых в комплекте поставки прилагается специальное программное обеспечение. Многие из таких программ работают только с операционной системой MS-DOS и потому они нередко запускаются с ошибками на платформах Windows 2000/XP, не поддерживающих эту систему в полной мере. Принцип работы утилит программной настройки сетевых адаптеров заключается в следующем. Программно-конфигурируемая сетевая карта содержит специальную микросхему перепрограммируемой постоянной памяти EPROM, в которой хранится информация о текущих настройках устройства и используемых им ресурсах. При запуске утилиты происходит тестирование внутренней конфигурации карты и считывание записанных в EPROM данных, после чего пользователю предлагается их изменить. Иногда программа требует указать вручную тип имеющегося в составе адаптера сетевого разъема: BNC, RJ-45 (UNC), Attachment Unit Interface (AUI) или «COMBO» для плат с комбинированным интерфейсом. Перед выходом из программы все настройки следует обязательно сохранить в EPROM.

Зачастую помимо собственно функций настройки подобные утилиты предлагают выполнить тестирование сетевого адаптера, причем подобные тесты можно условно разделить на внутренние (internal или self test) и внешние (external). В первом случае программа тестирует сетевую плату на наличие ошибок в регистрах ее встроенной памяти, во втором — отправляет информационные пакеты в локальную сеть и анализирует полученные отклики. Нередко существует возможность запустить тест на двух разных машинах одновременно, указав к настройках программы одну из них в качестве сервера (server computer), а вторую — в качестве клиента (client computer), и проверить таким образом работоспособность отдельного участка локальной сети. Однако следует учитывать тот факт, что многие тесты автоматически завершают свою работу при превышении интервала ожидания в одну минуту. Это означает, что если за указанное время вы не успеете добраться до другого компьютера и запустить на нем аналогичную утилиту, тест отрапортует о наличие в сети сбоя. На рис. 4.8 показана программа настройки сетевой карты NE 2000.

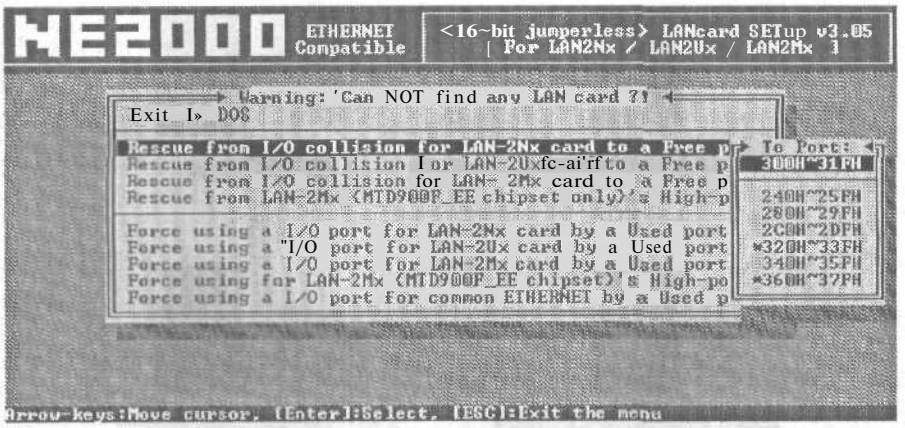


Рис. 4.8. Утилита настройки программно-конфигурируемого сетевого адаптера NE 2000

Если вы купили подержанную сетевую карту без соответствующей утилиты настройки, либо потеряли дискету с программным обеспечением, можно воспользоваться аналогичной программой от другого сетевого адаптера, имеющего в точности такой же тип чипсета (микросхемы контроллера). Также утилиту настройки сетевой карты можно бесплатно загрузить из Интернета, поискав ее на сайте производителя устройства или в коллекциях драйверов для различного оборудования ПК.

Аппаратно-конфигурируемые сетевые адаптеры

Некоторые сетевые адаптеры старых, вернее, очень старых моделей позволяют настраивать адреса и прерывания устройства при помощи расположенных непосредственно на плате перемычек, или, как их еще называют, «джамперов». Каждая из перемычек может находиться в одном из двух устойчивых состояний: On или En (Enable) — перемычка включена (рис. 4.9, *а*), либо Off — перемычка выключена (рис. 4.9, *б*). Перемычки переставляют при помощи пинцета на заранее извлеченной из компьютера сетевой плате. В выключенном положении перемычка свободно оставляется на одном из контактов — чтобы случайно ее не потерять. Правильное положение перемычек должно быть указано в документации па сетевую карту, либо напечатано краской на самом адаптере.

Иногда перемычки бывают трех- и четырехпозиционные. Это означает, что блок переключения содержит несколько контактов, один из которых должен быть обязательно помечен цифрой 1, номера остальных контактов отсчитываются от него по порядку. В этом случае для изменения настроек адаптера необходимо установить «джампер» в соответствующее положение. Например, если требуемая вам конфигурация достигается установкой перемычки в положение 2-3, то такое включение «джампера» показано на рис. 4.9 *(в)*, положение 3-4 продемонстрировано на рис. 4.9 *(г)*. Иногда настройка сетевого адаптера выполняется комбинацией из нескольких перемычек.

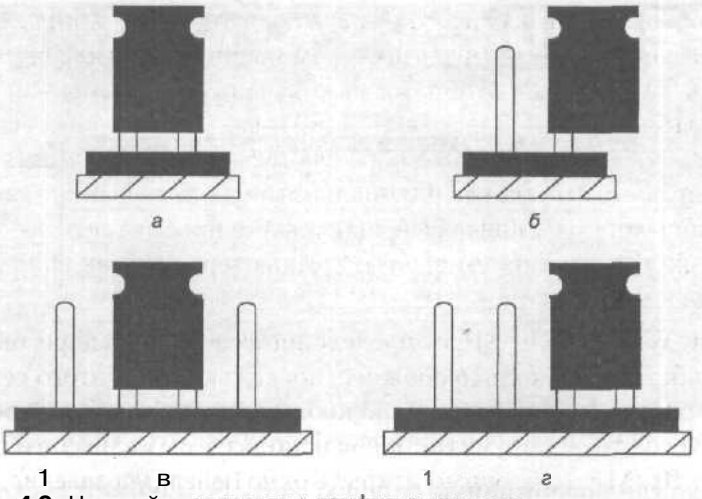


Рис. 4.9. Настройка аппаратно-конфигурируемого сетевого адаптера

Как найти свободное прерывание?

В случае, если вы являетесь «счастливым» владельцем устаревшей сетевой карты, не поддерживающей режим автоматической настройки, вам придется искать свободные ресурсы вручную для того, чтобы настроить адаптер на их использование. Легче всего эта проблема решается в операционных системах семейства Microsoft Windows NT/2000/XP, где в распоряжении пользователя имеется специальная утилита WinMsd, предназначенная для определения свободных и используемых ресурсов компьютера. Для того чтобы вызвать данную программу на исполнение, необходимо выполнить последовательность команд Пуск ▸ Выполнить и, набрав в появившемся окне Запуск программы команду winmsd, нажать на клавишу Enter (рис. 4.10).

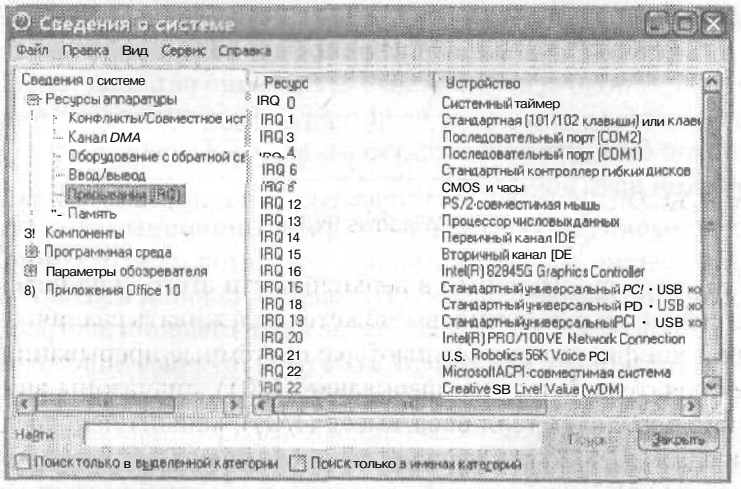


Рис. 4.10. Интерфейс утилиты WinMsd для MS Windows XP

Просматривая список ресурсов компьютера, отображающийся в левом окне программы, вы можете выбрать щелчком мыши требуемый вам компонент, при этом в правом окне отобразится перечень допустимых значений. Например, выбрав пункт Прерывания (IRQ), вы увидите список свободных и занятых аппаратных прерываний, щелкнув на пункте Ввод/Вывод, вы получите информацию о диапазонах ввода-вывода для различных устройств, обратившись к пункту Канал DMA, вы сможете просмотреть сведения об используемых оборудованием вашего компьютера адресах каналов прямого обращения к памяти.

В Microsoft Windows 9x/ME с определением свободных адресов и прерываний дело обстоит несколько сложнее, поскольку в ОС этого семейства отсутствует отдельная утилита, позволяющая отслеживать ресурсы компьютера. Для того чтобы получить список используемых адресов и прерываний в Windows 9x/ME необходимо открыть окно Панели управления, в нем дважды щелкнуть на значке Система, в окне Свойства: Система перейти ко вкладке Устройства, щелкнуть правой кнопкой мыши на устройстве Компьютер и выбрать в появившемся меню пункт Свойства. На экране появится специальное окно, содержащее перечень всех аппаратных ресурсов вашего ПК (рис. 4.11).

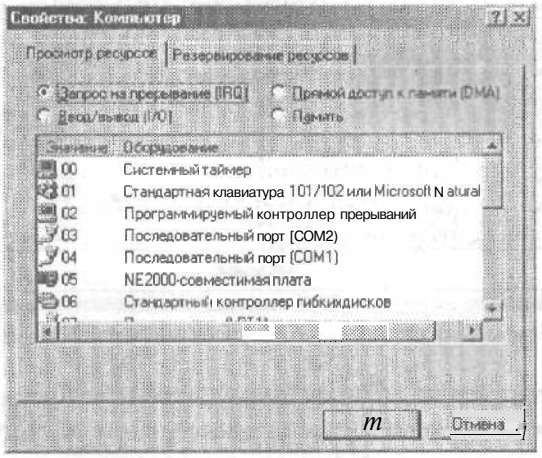


Рис. 4.11. Отслеживание аппаратных ресурсов в операционных системах Windows 9x/ME

Устанавливая расположенный в верхней части этого окна переключатель в одну из возможных позиций, вы можете отслеживать различные ресурсы аппаратной конфигурации компьютера: системные прерывания (положение переключателя Запрос на прерывание (IRQ)), диапазоны ввода-вывода (положение переключателя Ввод/вывод (I/O)), каналы непосредственного доступа к памяти (положение переключателя Прямой доступ к памяти (DMA)), или ресурсы ОЗУ, используемые различными устройствами (положение

переключателя Память). Здесь же вы можете зарезервировать какой-либо из ресурсов для его последующего использования вашим сетевым адаптером: для этого перейдите ко вкладке Резервирование ресурсов, установите переключатель в положение, соответствующее ресурсу, который вы желаете зарезервировать, нажмите на кнопку Добавить и выберите свободный ресурс из предложенного списка.

Отдельная программа для просмотра аппаратных ресурсов компьютера присутствует также в комплекте поставки операционной системы MS-DOS/ Windows 3x. Эта утилита называется msd.exe, и хранится она, как правило, в системной папке DOS. Запустить ее можно из командной строки: если в процессе загрузки программа вызывает зависание компьютера, попробуйте вызвать ее на исполнение командой msd.exe /i. После своего запуска программа msd демонстрирует список характеристик компьютера, которые она в состоянии определить: тип процессора, версию операционной системы, объем доступной памяти, модель видеоадаптера и т.д. Для того чтобы просмотреть список свободных и занятых прерываний, выберите в меню программы пункт IRQ Status или просто нажмите на клавишу 0 (рис. 4.12).

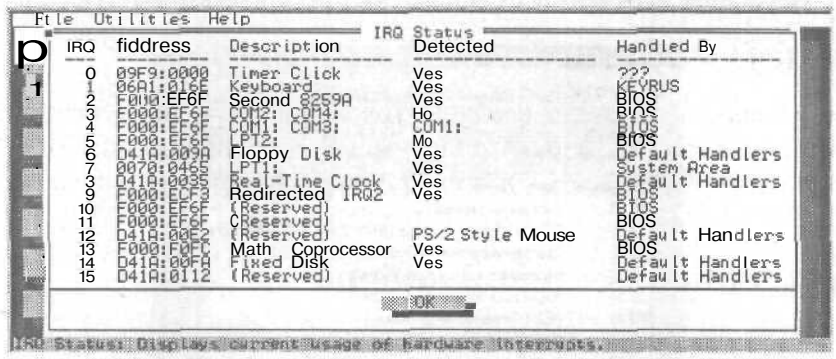


Рис. 4.12. Отслеживание аппаратных ресурсов в операционной системе MS-DOS

Выбрав в появившемся на экране списке свободное прерывание и соответствующий ему диапазон ввода-вывода, вы сможете настроить на использование этих параметров ваш сетевой адаптер.

Проблемы при подключении сетевых адаптеров USB

Порой случается так, что подключенный к USB-порту компьютера сетевой адаптер не определяется операционной системой и, соответственно, не может работать корректно. В такой ситуации можно посоветовать проделать следующее.

1. Щелкните правой кнопкой мыши на значке Мой компьютер, расположенном на Рабочем столе, и выберите в появившемся контекстном меню пункт Свойства. В ОС Windows 9x/ME перейдите к вкладке Устройства, в ОС

Windows NT/2000/XP запустите Диспетчер устройств, перейдя к вкладке Оборудование и щелкнув мышью на кнопке Диспетчер устройств.

2. Найдите в списке оборудования контроллер шины USB:
   - если контроллер шины USB отсутствует в списке, установите и настройте его при помощи Мастера настройки оборудования;
   - если контроллер шины USB присутствует в списке, но работает с ошибками или вызывает конфликт с другими устройствами, установите для него соответствующие драйверы, которые входят обычно в комплект поставки программного обеспечения материнской платы, либо попытайтесь удалить из списка устройство и настроить его заново при помощи Мастера настройки оборудования;
   - если контроллер шины USB присутствует в списке, настроен правильно и не вызывает конфликтов с другими устройствами, проверьте контакт шнура, посредством которого адаптер присоединен к порту USB и переустановите драйверы сетевого адаптера. В некоторых случаях имеет смысл попытаться принудительно обнаружить сетевой адаптер при помощи Мастера настройки оборудования.

Сетевой кабель

Одним из наиболее важных компонентов любой локальной сети является сетевой кабель, посредством которого выполняется прокладка коммуникаций. В настоящем разделе мы рассмотрим два типа сетевого кабеля, используемого в локальных сетях класса 10Base2 и 10BaseT.

Коаксиальный сетевой кабель

Коаксиальный сетевой кабель применяется в локальных сетях класса 10Base2. Он имеет четырехслойную структуру: два слоя коаксиального кабеля выполнены из проводника, два — из диэлектрика. Самый внутренний слой — это проводящая жила, по которой в локальной сети передается несущий информацию сигнал. Жила может быть представлена в виде нескольких сплетенных тонких проводников, либо в виде одной толстой медной проволоки, что является более распространенным вариантом. Жила покрыта диэлектрической пленкой, поверх которой расположен второй проводящий слой — так называемый экран, защищающий линию от посторонних помех. Экран выполнен в виде металлической проволочной оплетки, иногда помимо оплетки внутренний изолирующий слой обернут в металлическую фольгу — такие кабели называют кабелями с двойной экранизацией. Встречаются и кабели с учетверенной экранизацией: в них экран состоит из двух слоев оплетки и двух слоев фольги, либо из двух слоев фольги, оплетки и тонкой металлической сетки. Подобные кабели имеют большую толщину,

обладают высокой жесткостью при изгибах и применяются в основном в помещениях со значительным уровнем радиоэлектронных помех. В электрической схеме монтажа сетевых разъемов экран играет роль заземления. Поверх экрана расположен последний, четвертый диэлектрический слой, обеспечивающий не только электромагнитную защиту кабеля, но и его защиту от внешних физических повреждений (рис. 4.13).

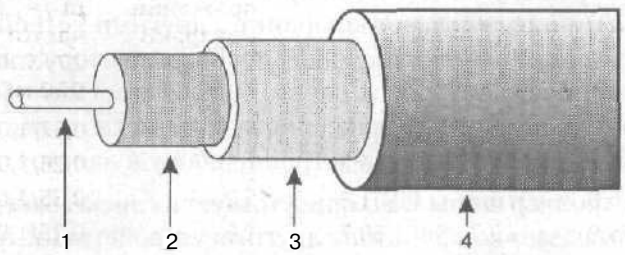


Рис. 4.13. Коаксиальный сетевой кабель:

1 — центральный провод (проводящая жила); *2*— изолирующий слой центрального провода; *3*— экранирующий слой («экран»); *4* — защитная оболочка (внешний изолятор)

Существует несколько различных типов коаксиального кабеля, применяемого в локальных сетях класса 10Base2. Их характеристики приведены в табл. 4.1.

Как это было сказано в предыдущей главе, для локальных сетей используется в основном тонкий коаксиальный кабель с волновым сопротивлением Z = 50 Ом, в табл. 4.1 этот тип кабеля представлен семействами RG-58, RG-174, RG-178, а также кабелем отечественного производства РК-50. В случае если вы располагаете коаксиальным кабелем с неизвестным волновым сопротивлением, то вы можете измерить точный диаметр внутренней проводящей жилы, диаметр экранирующего слоя, найти в справочнике значение диэлектрической постоянной для используемого в кабеле диэлектрика и рассчитать величину волнового сопротивления по следующей формуле (рис. 4.14):

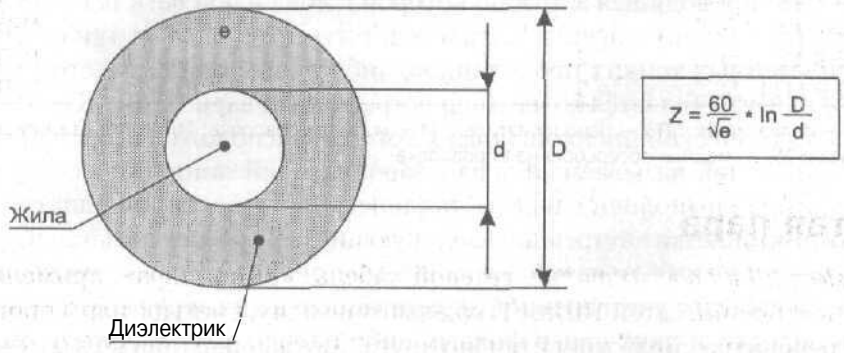


Рис. **4.14.** Расчет величины волнового сопротивления коаксиального кабеля

где e — диэлектрическая постоянная, d — диаметр центрального провода, а D — внутренний диаметр экрана.

Таблица 4.1. Характеристики различных типов коаксиального кабеля

Марка кабеля	Волновое сопротивление Z,OM	Внешний диаметр, мм	Емкость, лф/м	Максимальное эффективное напряжение Uэфф, кВ	Коэффициент затухания, дБ/м, для частот 27/300/900 МГц	Материал*
RG-8A/U	52,0	10,3	88,5	5,0	0,32/1,6/3,0	ПЭ
RG-8/U	50,0	10,3	76,2	1,5	0,26/1,0/1,7	ППЭ
RG-11A/U	75,0	10,3	61,8	5,0	0,35/1,6/3,0	ПЭ
RG-11/U	75,0	10,3	50,7	1,6	0,25/1,0/1,7	ППЭ
RG-58A/U	53,5	5,0	85,5	1,9	0,65/3,5/6,0	ПЭ
RG-58B/U	53,5	5,0	85,5	1,9	0,65/3,5/7,0	ПЭ
RG-58C/U	50,0	5,0	92,4	1,9	0,65/3,5/7,0	ПЭ
RG-58/U	53,5	5,0	85,5	1,9	0,60/2,2/3,0	ППЭ
RG-59B/U	73,0	6,2	69,0	1,9	0,60/2,2/3,0	ПЭ
RG-59/U	75,0	6,2	50,7	0,8	0,50/1,6/2,8	ППЭ
RG-71A/U	93,0	6,2	46,0	1,8	0,50/1,6/2,8	ПЭ
RG-71B/U	93,0	6,2	46,0	1,8	0,50/1,6/2,8	ПЭ
RG-174A/U	50,0	2,5	92,0	1,5	2,0/5,5/>10	ПЭ
RG-174B/U	50,0	1,5	95,0	1,2	2,2/8,0/>10	ПЭ
RG-179B/U	75,0	2,5	63,0	1,2	1,9/5,0/8,5	ПЭ
RG-213/U	50,0	10,3	92,0	5,0	0,32/1,6/3,0	ПЭ
RG-216/U	75,0	10,8	71,8	5,0	0,32/1,6/3,0	ПЭ
РК-50-2-12	50,0	3,2			2,0	МС/ПЭ/МС
РК-50-2-16	50,0	3,2			1,0	мл/пэ/мл
РК-50-3-13	50,0	4,4			0,70	м/пэ/мл
РК-50-4-11	50,0	9,6			0,50	М/ПЭ/М
РК-50-7-11	50,0	10,0			0,40	М/ПЭ/М
РК-50-7-12	50,0	11,2			0,40	М/ПЭ/М
РК-50-9-11	50,0	12,2			0,34	м/пэ/м
РК-50-9-1111	50,0	14,5			0,28	м/пэ/м

* ПЭ — полиэтилен; ППЭ — пенополиэтилен; М — медная проволока; МЛ — медная луженая проволока; МС — медная посеребренная проволока

Витая пара

Несмотря на свое название, сетевой кабель «витая пара», применяемый при построении сетей 10BaseT, содержит не одну, а четыре пары проводников, перевитых друг относительно друга. Каждая пара также закручивается относительно других пар проводников (рис. 4.15).

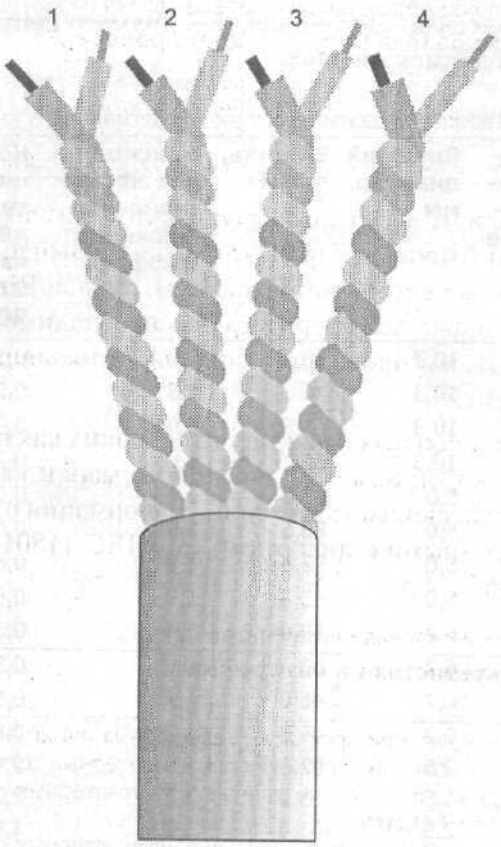


Рис. 4.15. Кабель «витая пара»

В каждой из четырех пар проводников в данном типе кабеля различается «главный» провод, который по традиции, идущей еще со времен становления телефонной связи, называют «Ring», и «дополнительный» провод, называемый «Tip». Изоляционное покрытие провода Ring имеет однотонную окраску, покрытие провода Tip — белое с полосками основного цвета. Если, например, Ring имеет зеленый цвет, то Tip в этой паре будет белым с зелеными полосами.

Для того чтобы при монтаже и прокладке компьютерных сетей было легче отличать одну пару проводников от другой, провода Ring каждой из четырех пар окрашены в собственный цвет, при этом каждой паре для простоты назначен свой порядковый номер с 1 по 4. Таким образом, среди имеющихся 8 проводов кабеля «витая пара» можно выделить проводники Ring1, Tip1, Ring2, Tip2, Ring3, Tip3 и Ring4, Tip4. Соответствия расцветок проводников номерам пар в кабеле «витая пара» приведены в табл. 4.2.

Таблица 4.2. Номера пар проводников в кабеле «витая пара»

Номер пары	Цвет провода Ring	Цвет провода Tip
1	Синий	Белый с синими полосами
2	Оранжевый	Белый с оранжевыми полосами
3	Зеленый	Белый с зелеными полосами
4	Коричневый	Белый с коричневыми полосами

Исходя из этой таблицы, легко можно понять, что если в технической документации заходит речь о проводе Tip4, то это будет белый провод с коричневыми полосами, если же упоминается, скажем, провод Ring2, то этот провод имеет оранжевую окраску. Теперь в случае необходимости мы без всякого труда отыщем нужный проводник, сняв часть изоляционного покрытия кабеля «витая пара».

Исходя из функциональных характеристик, таких как пропускная способность и устойчивость к помехам, различные марки кабеля «витая пара» принято делить на несколько категорий, информация о которых в соответствии с международными стандартами ISO/IEC 11801 и ANSI/EIA/TIA-568 приведена в табл. 4.3.

Таблица 4.3. Категории кабеля «витая пара»

Номер категории	**Характеристики и назначение**
1	Применяется при прокладке телефонных линий, не подходит для передачи данных в локальных компьютерных сетях
2	Пригоден для передачи данных в компьютерных сетях со скоростью не более 4 Мбит/с
3	Пригоден для передачи данных в компьютерных сетях со скоростью не более 10 Мбит/с, Используется при прокладке сетей класса IOBaseT
4	Пригоден для передачи данных в компьютерных сетях со скоростью не более 16 Мбит/с. Используется при прокладке сетей класса TokenRing
5	Пригоден для передачи данных в компьютерных сетях со скоростью не более 100 Мбит/с. Используется при прокладке сетей класса IOBaseT и 100BaseTX
5+	Пригоден для передачи данных в компьютерных сетях со скоростью не более 100 Мбит/с и частотой до 300 МГц включительно. Используется при прокладке сетей класса IOBaseT и 100BaseTX
6	Пригоден для передачи данных в компьютерных сетях со скоростью не более 100 Мбит/с и частотой до 600 МГц включительно. Используется при прокладке сетей класса IOBaseT и 100BaseTX

Категория, к которой относится тот или иной кабель «витая пара», обычно указана в его маркировке, которая печатается заводским способом на внешней изоляции кабеля.

Диаметр провода «витая пара» принято исчислять согласно американскому стандарту AWG (American Wide Gauge), причем чем меньше диаметр,

тем больше величина AWG. Соответствие значений AWG диаметру проводника в миллиметрах показано в табл. 4.4.

Таблица 4.4. Соответствие значений AWG диаметру проводника

AWG №	Диаметр проводника, мм	AWG №	Диаметр проводника, мм
1	7,348	21	0,723
2	6,544	22	0,644
3	5,827	23	0,573
4	5,189	24	0,511
5	4,621	25	0,455
6	4,115	26	0,405
7	3,665	27	0,361
8	3,264	28	0,321
9	2,906	29	0,286
10	2,588	30	0,255
11	2,305	31	0,227
12	2,053	32	0,202
13	1,828	33	0,180
14	1,628	34	0,160
15	1,450	35	0,143
16	1,291	36	0,127
17	1,150	37	0,113
18	1,024	38	0,101
19	0,912	39	0,090
20	0,812	40	0,080

В локальных сетях 10BaseT применяется, как правило, кабель «витая пара» категории 5 или 5+, диаметром проводника 22 или 24 AWG.

В некоторых ситуациях, например тогда, когда локальная сеть прокладывается в помещениях с высоким уровнем электромагнитных помех, либо требуется повысить точность передачи информации за счет снижения перекрестных наводок в кабеле, используется экранированная «витая пара». Как правило, экран выполняется из металлической фольги. При этом существует несколько различных вариантов экранирования: фольгой может быть обернута каждая из четырех пар, плюс все они защищены сверху дополнительным слоем фольги, расположенным под внешней изоляцией (кабель марки STP), либо внутри кабеля предусмотрен один общий для всех пар экран (кабель марки FTP).

Концентраторы

Концентраторы, или хабы, являются центральным звеном в локальных сетях классов 10BaseT и 100BaseT, имеющих топологию «звезда». Фактически хаб представляет собой мультипортовый репитер, то есть в его основную функциональную задачу входит получение данных от подключенных

к портам концентратора компьютеров или других хабов, реформирование сигнала одновременно с его усилением, и его дальнейшая ретрансляция на другие порты. Помимо разъемов RJ-45 для сетей 10BaseT многие концентраторы имеют также порты BNC, что позволяет подключать к ним сегменты 10Base2 либо использовать коаксиальный кабель в качестве магистрального, последовательно соединяя несколько хабов в цепочку.

Как правило, один из разъемов RJ-45 концентратора имеет разводку, позволяющую присоединять его к другим хабам: такое «многоэтажное» подключение концентраторов друг к другу принято называть термином *каскадирование*. Этот порт обычно обозначается надписью «In», «Uplink», «Cascading» или «Cross-Over». В некоторых случаях рядом с таким портом имеется переключатель MDI/MDI-X, позволяющий по мере необходимости включать порт либо в обычный режим, либо в режим каскадирования. В случае если порт не оснащен переключателем, но к нему требуется подключить еще один компьютер (например, если все остальные порты заняты), для этого можно использовать кабель «cross-over», применяемый обычно для соединения двух компьютеров по принципу «точка—точка». О том, как подготовить такой кабель, будет подробно рассказано в следующей главе.

Существует множество различных моделей концентраторов: все они различаются количеством портов, пропускной способностью и другими техническими характеристиками. Самые недорогие варианты для малых локальных сетей стоят всего-навсего несколько десятков долларов, в то время как более совершенные концентраторы могут обойтись вам в несколько сотен долларов США.

Глава 5

Прокладывание локальной сети

- Прокладывание сети 10Base2
- Монтаж разъемов BNC
- Установка Т-коннекторов, терминаторов и прямых переходов
- Прокладывание сети 10BaseT
- Монтаж разъемов RJ-45 и сетевых розеток
- Как быстро объединить в сеть два компьютера?

Постепенно мы подошли к одному из наиболее интересных разделов нашего «Самоучителя» — к разделу, посвященному прокладыванию и компоновке локальной сети. В настоящей главе мы рассмотрим два наиболее распространенных класса локальных сетей: 10Base2 и 10BaseT, а также обсудим ряд особенностей их монтажа.

Прокладывание локальной сети 10Base2

Сети класса 10Base2 фактически не требуют каких либо серьезных усилий для их подготовки к работе за исключением монтажа разъемов BNC на отрезках коаксиального кабеля, соединяющих между собой сегменты локальной сети. Да и с этой задачей можно справиться без особенных проблем.

Итак, прежде чем непосредственно приступить к прокладыванию локальной сети, необходимо определиться с взаимным расположением компьютеров, которые вы планируете объединить между собой. В случае если предполагается создание системы «точка—точка», то есть локальной сети, состоящей из двух компьютеров, данный вопрос автоматически становится неактуальным: вам потребуется один-единственный отрезок коаксиального кабеля, важно лишь, чтобы его общая длина не превышала 185 м. Как правило, кабель отрезается «с запасом», таким образом, чтобы в случае необходимости один из компьютеров можно было перенести в другую часть помещения, и кабель не оказался при этом натянутым поперек комнаты.

Если же создаваемая вами система будет объединять несколько ПК, следует заранее определить последовательность их подключения, поскольку в сетях 10Base2 компьютеры соединяются между собой «цепочкой». Здесь необходимо продумать длину каждого сегмента с особой тщательностью, так как вполне возможна ситуация, когда один из компьютеров придется отключить от сети — например, перенести в другое помещение или временно поставить на ремонт — и при этом в сети не должно образоваться «обрыва». Другими словами, необходимо заранее предусмотреть возможность быстрой протяжки к сетевому адаптеру кабеля от соседней машины, причем так, чтобы он при этом не путался под ногами.

Когда вопрос с конфигурацией сети будет решен, необходимо отрезать несколько частей коаксиального кабеля соответствующей длины, их количество должно совпадать с количеством сетевых сегментов. Если, например, вы планируете подключить к сети четыре компьютера, вам понадобится три отрезка кабеля. Также вам потребуется по два разъема BNC для каждого из полученных отрезков, по одному Т-коннектору для каждого из подключаемых к сети компьютеров и два терминатора. Теперь можно приступать к монтажу разъемов.

Монтаж разъемов BNC

В нашей стране наиболее распространены три типа разъемов BNC: «под пайку» отечественного производства марки «СР», предназначенные для использования в сетях с волновым сопротивлением 50 Ом и частотой до 10 ГГц, а также «под обжим» и «под накрутку» импортного производства. Существует несколько разновидностей отечественных разъемов «под пайку», отличающихся, в основном, используемыми при их изготовлении материалами, их маркировка состоит из обозначения СР-50-XX-Y, где значение 50 указывает величину волнового сопротивления, XX — число, обозначающее тип разъема, а Y — буква, определяющая материал, из которого выполнена опорная шайба: Ф — фенопласт, С — полистирол, К — керамика, П — полиэтилен, В — высокочастотный пресс-порошок. Разъемы «под пайку» обычно не обеспечивают должного качества соединения, поскольку малейшая неосторожность в припаивании контакта центральной жилы или экрана приводит к тому, что при случайном шевелении кабеля сеть перестает работать, и локализовать сбойный участок оказывается крайне сложно. Поэтому опытные специалисты рекомендуют приобретать разъемы BNC «под обжим», которые не только полностью соответствуют стандарту Ethernet 10Base2, но и крайне просты в монтаже (рис. 5.1).

Такой разъем состоит из трех элементов, продающихся в виде комплекта разделенных деталей, запаянных, как правило, в полиэтиленовую упаковку: это сам разъем с рифленой контактной площадкой заземления, контакт

центрального провода и металлическое цилиндрическое кольцо — манжета. Помимо самого разъема вам понадобится также специальный обжимной инструмент для коаксиального кабеля (рис. 5.2).

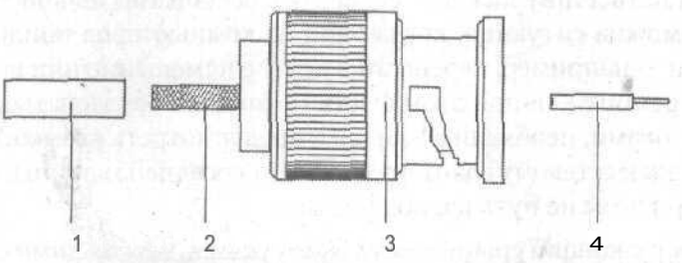


Рис. 5.1. Разъем BNC «под обжим»:
1 —манжета; *2*— контактная площадка заземления; *3* — разъем;
4 — контакт центрального провода

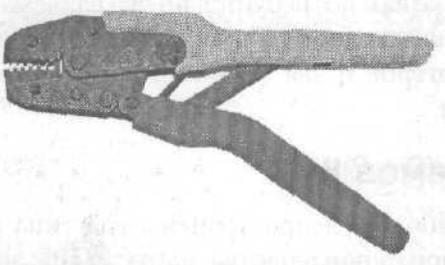


Рис. 5.2. Обжимной инструмент для коаксиального кабеля

Если обжимного инструмента нет под рукой, можно воспользоваться обыкновенными пассатижами, но в этом случае при монтаже следует проявлять особую осторожность. Итак, для того чтобы смонтировать на коаксиальном кабеле разъем BNC, необходимо выполнить такую последовательность действий (рис. 5.3).

1. Ровно обрежьте край коаксиального кабеля таким образом, чтобы на его торце не было зазубрин и скосов. Наденьте на кабель металлическую муфту разъема BNC.
2. При помощи острого ножа или скальпеля удалите верхний защитный изоляционный слой коаксиального кабеля на расстояние приблизительно 20-25 мм от края. Проделывайте эту процедуру крайне осторожно, чтобы не повредить расположенную под защитным слоем металлическую оплетку. Аккуратно расплетите оплетку экрана и разведите ее в стороны.
3. Стараясь не повредить центральный проводник, снимите острым ножом или скальпелем защитный слой проводящей жилы коаксиального кабеля на расстояние примерно 5-8 мм. Зачистите центральный проводник ножом или кусочком наждачной бумаги таким образом, чтобы на нем

не осталось следов защитного покрытия. Наденьте на проводящую жилу контакт центрального провода.

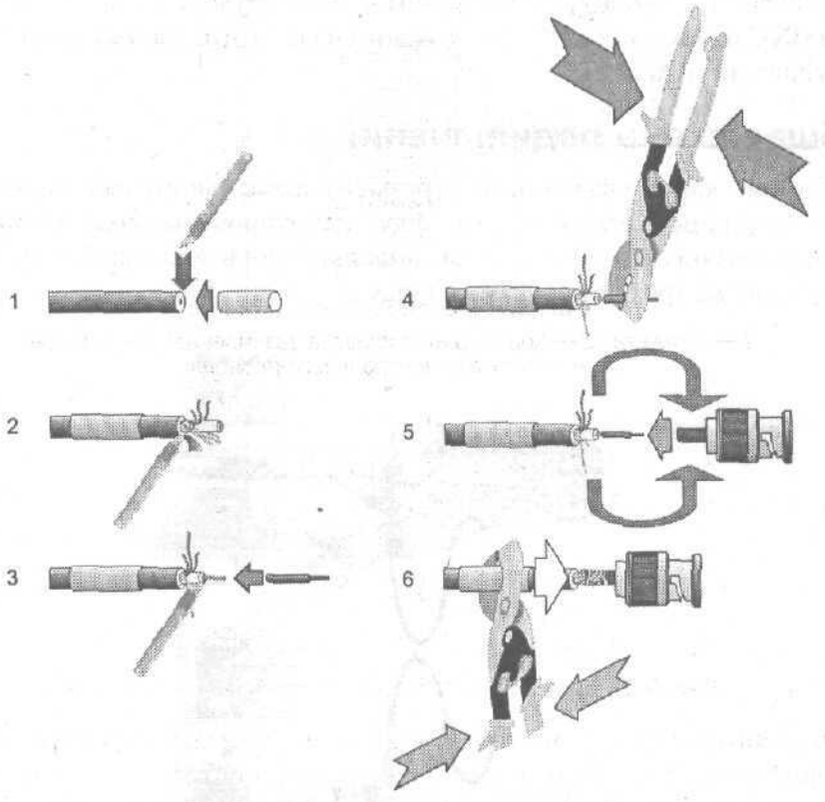


Рис. 5.3. Порядок монтажа разъема BNC

4. Посредством обжимного инструмента или тонких плоскогубцев зажмите цилиндрическую часть контакта центрального провода таким образом, чтобы он надежно зафиксировался на проводящей жиле. При отсутствии обжимного инструмента контакт центрального провода можно припаять к проводящей жиле, но при пайке следует проявлять особую аккуратность, внимательно следя за тем, чтобы соединение было надежным.
5. Наденьте на кабель разъем до щелчка таким образом, чтобы контакт центрального провода показался из соответствующего отверстия во внутренней части разъема. Равномерно обмотайте ранее расплетенные вами проводники экранирующей оплетки вокруг рифленой контактной площадки заземления. Если волокна экранирующей оплетки окажутся слишком длинными, их можно обрезать на требуемое расстояние.
6. Надвиньте на контактную площадку заземления с обмотанным вокруг нее экранирующим проводником металлическую муфту разъема

и надежно зафиксируйте ее при помощи обжимного инструмента или плоскогубцев. Разъем готов к работе.

Повторите эту процедуру необходимое количество раз, смонтировав разъемы BNC на обоих окончаниях каждого из подготовленных вами отрезков коаксиального кабеля.

Общая схема подключений

После того как все разъемы на отрезках коаксиального кабеля, соединяющего отдельные сегменты сети, будут смонтированы, можно приступать к сборке самой сети. Общая схема подключений в локальной сети 10Base2, состоящей из трех компьютеров, показана на рис. 5.4.

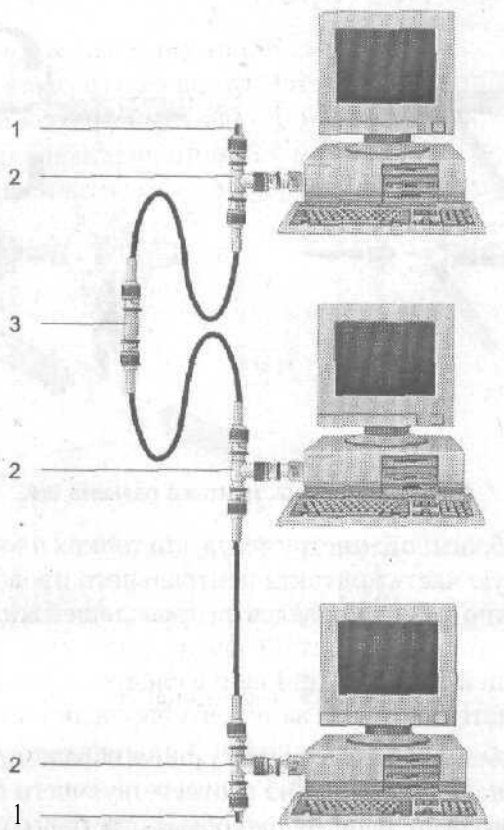


Рис. 5.4. Общая схема подключений в сети 10Base2:
1 — терминатор; *2*— Т-коннектор; *3*— I-коннектор (прямой переход)

К оконечным разъемам Т-коннекторов, к которым не присоединяется более никаких устройств, подключаются терминаторы — специальные заглушки, которые создают в локальной сети требуемое сопротивление нагрузки.

На участках сети, где требуется соединить два отрезка коаксиального кабеля без подключения промежуточного устройства, используются так называемые I-коннекторы или прямые переходы.

При такой конфигурации допустимо выключать питание любого из входящих в сеть компьютеров без потери соединения для всех остальных узлов сети. Локальная сеть перестает работать только в том случае, если на одном из участков линии (в разъеме, Т-коннекторе или прямом переходе) потерян контакт, либо если один из отрезков коаксиального кабеля неплотно подключен к соответствующему разъему. В некоторых случаях отказ сети бывает вызван потерей сопротивления нагрузки в одном из терминаторов.

Установка Т-коннекторов

Т-коннекторы предназначены для организации надежного соединения коаксиального кабеля с разъемом сетевого адаптера в сетях 10Basc2. Внешне Т-коннектор представляет собой Т-образный трехсекционный разъем, к двум противоположным секциям которого подключаются разъемы BNC коаксиального кабеля, а третий фиксируется в соответствующем гнезде сетевого адаптера (рис. 5.5).

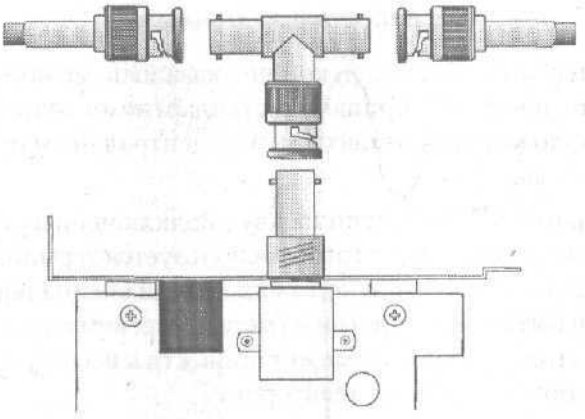


Рис. 5.5. Т-коннектор

Обычная последовательность установки Т-коннекторов и подключения к ним сетевого кабеля выглядит следующим образом;

1. Установите Т-коннектор в ответный разъем BNC сетевого адаптера таким образом, чтобы штырьки замка разъема вошли в соответствующие пазы на вращающейся шайбе Т-коннектора. Проверните шайбу до полной фиксации Т-коннектора в разъеме.
2. Аналогичным образом наденьте на боковые секции Т-коннектора разъемы сетевого кабеля и зафиксируйте их поворотом вращающейся шайбы.

Установка терминаторов

Терминаторы, либо, как их еще называют, колпачки или заглушки — это специальные металлические насадки, подключающиеся к разъемам Т-коннекторов на крайних сегментах локальной сети 10Base2 и создающие в сети требуемое сопротивление нагрузки (рис. *5.6).*

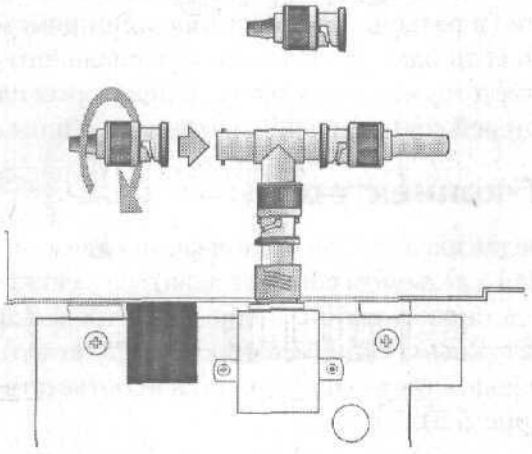


Рис. 5.6. Установка терминатора

В случае если терминатора под рукой не оказалось, можно изготовить его самостоятельно, аккуратно припаяв к стандартному разъему BNC резистор 51 Ом, расположив его контакты между центральным проводом кабеля и корпусом разъема.

Согласно стандарту 10Base2, один из двух подключенных к сети терминаторов должен быть заземлен. Для этого используется терминатор с припаянной к нему металлической цепочкой, оснащенной специальным контактом, который должен быть зафиксирован на металлическом корпусе компьютера. Несоблюдение этого требования может привести к выходу из строя локальной сети или одного из сетевых адаптеров.

Переходы прямые

Переходы прямые, или I-коннекторы, применяются в тех случаях, когда возникает необходимость соединить между собой несколько отрезков коаксиального кабеля (сегментов сети) без подключения между ними промежуточного устройства. Например, в случае, если один из компьютеров пришлось физически отключить от локальной сети, и в данном ее сегменте образуется «разрыв». Существует два типа разъемов, пригодных для организации прямых переходов: так называемый I-коннектор (barrel-connector, рис. 5.7, *а)* и стационарный прямой переход (bulk-head connector, рис. 5.7, б).

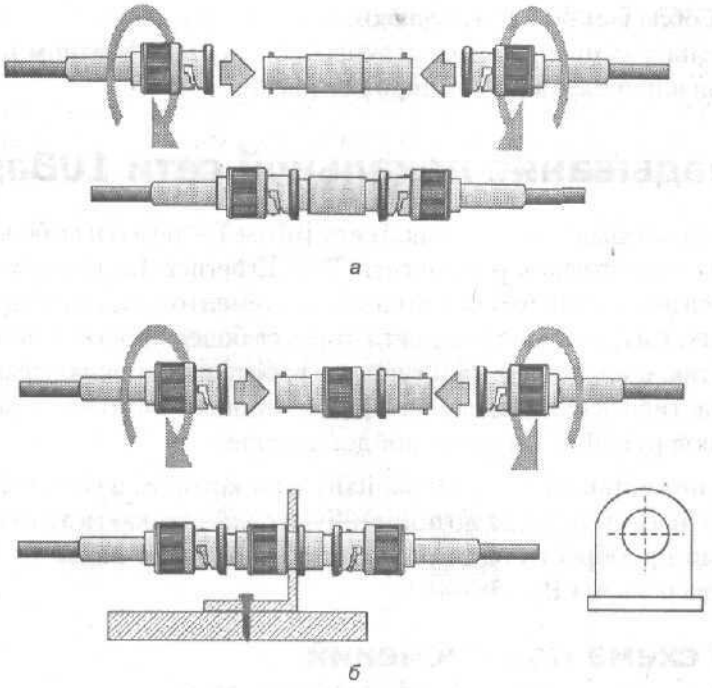


Рис. 5.7. I-коннекторы (переходы прямые)

Обычные I-коннекторы представляют собой двухсекционный разъем, позволяющий подключать к каждой из своих секций по одному разъему BNC, установленному на соответствующем отрезке коаксиального кабеля, выполняя таким образом непосредственное соединение между собой двух сегментов сети. I-коннекторы не крепятся к каким-либо внешним предметам, а свободно присоединяются к кабелю.

В отличие от обычных I-коннекторов стационарные прямые переходы имеют специальную упорную шайбу и вращающуюся гайку, между которыми помещается металлический уголок с отверстием или вырезом под диаметр разъема. Этот уголок, в свою очередь, жестко крепится винтом к стене, боковой стенке стола или к полу. Такое соединение более надежно, поскольку исключает возможность потери контакта в прямом переходе при случайном шевелении кабеля, но требует больше усилий при монтаже.

В принципе, прямые переходы — необязательный компонент локальной сети 10Base2, особенно в случае, когда все отрезки кабеля можно непосредственно соединить между собой. Например, если при физическом отключении какого-либо компьютера от сети существует возможность напрямую протянуть к Т-коннектору следующего в цепочке компьютера коаксиальный кабель от предыдущей машины, прямой переход становится попросту не нужен. К тому же локальная сеть, построенная без использования прямых

переходов, обладает большим запасом надежности, поскольку в ней имеется значительно меньше промежуточных сочленений, в одном из которых может произойти случайная потеря контакта.

Прокладывание локальной сети lOBaseT

Монтаж и прокладывание локальной сети lOBaseT — несколько более сложная задача, чем подготовка к работе сети Thin Ethernet. Во-первых, для этого потребуется значительно больше базовых элементов, чем в случае 10Base2, а во-вторых, сам монтаж такой сети требует более кропотливой и тонкой работы. Итак, прежде, чем приступить к работе над прокладыванием сети, нужно запастись необходимым набором компонентов, которые должны находиться под рукой. О них речь пойдет дальше.

Исключение составляет только вариант, при котором в сеть lOBaseT объединяются два компьютера по принципу «точка—точка»: в этом случае вам необходимо приобрести один отрезок кабеля «витая пара» необходимой длины и два разъема RJ-45.

Общая схема подключений

Если перед прокладыванием локальной сети класса 10Base2 приходится продумывать взаимное расположение компьютеров, то в случае lOBaseT к этому вопросу следует подойти еще более тщательно.

В конфигурации lOBaseT компьютеры подключаются к концентратору не напрямую, а через специальные сетевые розетки RJ-45 (рис. 5.8).

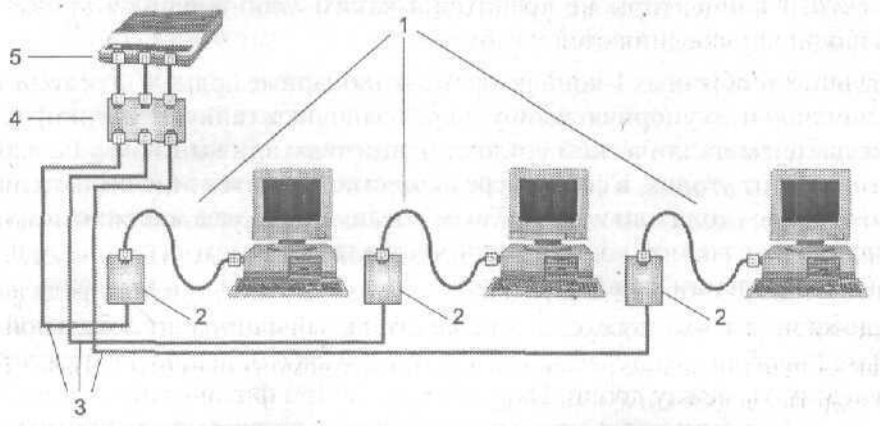


Рис. 5.8. Общая схема подключений устройств в сети lOBaseT:
1— Path Cord; *2*— сетевые розетки RJ-45; *3*— кабель «витая пара»;
4— path panel; *5*— концентратор

Сетевые розетки монтируются на стену в непосредственной близости от подключаемого к локальной сети компьютера. Каждая розетка соединяется с разъемом RJ-45, расположенным на сетевом адаптере ПК, при помощи небольшого отрезка кабеля «витая пара», который принято называть Path cord или «поводок». Длина этого кабеля не должна превышать 10 м, на концах провода Path cord крепится два разъема RJ-45. Такая конфигурация подключений крайне удобна, потому что, во-первых, позволяет быстро присоединять и отсоединять компьютеры от локальной сети, а также менять их местами — для этого достаточно вытащить Path cord из розетки, а во-вторых, сетевой кабель не натягивается при прокладывании и не путается под ногами.

От каждой сетевой розетки отходит еще один отрезок кабеля «витая пара», с одной стороны смонтированный непосредственно в розетке, с другой стороны — оснащенный разъемом RJ-45. Длина каждого отрезка такого кабеля не может превышать 90 м. Оконечные разъемы всех идущих от сетевых розеток отрезков кабеля присоединяются к комбинированной многопортовой сетевой розетке Path panel, либо к равному количеству обычных сетевых розеток RJ-45. В свою очередь, маленькие отрезки кабеля «витая пара», смонтированные в Path panel (длиной не более 1 м) и оснащенные на концах собственными разъемами RJ-45, вставляются в соответствующие гнезда концентратора. Path panel или дополнительный набор сетевых розеток применяются только исходя из удобства администрирования локальной сети: во-первых, каждую из таких розеток или каждое из гнезд Path panel можно промаркировать — если концентратор расположен на значительном удалении от рабочих мест, порой бывает трудно определить, какой из проводов ведет к нужному компьютеру. Во-вторых, используя Path panel, можно без труда переместить любой из проводов между имеющимися в наличии разъемами, быстро подключив его таким образом к другому порту концентратора.

На практике дополнительный набор сетевых розеток или Path panel обычно не монтируются — участки кабеля, идущие от розеток RJ-45 па рабочих местах, как правило, подключаются к концентратору напрямую. Во избежание путаницы их просто фиксируют прикрученной к степе поблизости от концентратора металлической пластиной и па каждый провод приклеивают при помощи скотча бумажку с указанием, от какой именно розетки он идет. Такой монтаж гораздо более удобен и надежен, хотя и может вызвать определенные неудобства в случае необходимости изменения конфигурации локальной сети.

Итак, общая последовательность действий при монтаже сети 10BaseT будет выглядеть следующим образом.

1. Составьте точный план помещения, в котором вы планируете проложить сеть, и определите, где именно будут располагаться рабочие места пользователей и где будет смонтирован концентратор. Учтите, что

большинство моделей концентраторов требуют подключения питания от электрической сети. Точно измерьте расстояния между точкой подключения концентратора и рабочими местами, определите, где именно будет пролегать сетевой кабель.

2. Смонтируйте концентратор — обычно он привинчивается к стене при помощи специальных фиксирующих винтов.
3. Изготовьте необходимое количество проводов Patch cord, их число должно соответствовать числу рабочих мест в локальной сети. Для этого вам придется отрезать требуемое количество частей кабеля «витая пара» и смонтировать на концах каждого отрезка разъем RJ-45. Помните, что длина Path cord не должна превышать 10 м (рекомендуемая длина — 2-3 м).
4. Смонтируйте вблизи каждого рабочего места сетевую розетку RJ-45, закрепив ее при помощи фиксирующих винтов на стене. Смонтируйте внутри каждой розетки отрезок кабеля «витая пара». Длина этого отрезка должна соответствовать расстоянию от розетки до концентратора, но она не может превышать установленное стандартное значение 90 м.
5. Проложите каждый отрезок кабеля «витая пара» от розетки до концентратора, укрепив его вдоль плинтуса или на стене помещения специальными фиксирующими скобами.
6. Смонтируйте на противоположном от розетки конце каждого отрезка сетевого кабеля разъем RJ-45.
7. Подключите оконечные разъемы RJ-45 в соответствующие гнезда концентратора и включите его питание.

Существует еще несколько технических требований, которые обязательно следует учитывать при прокладывании сетевого кабеля 10BaseT. Несоблюдение этих требований в конечном итоге может привести к выходу из строя локальной сети. Вот они:

- во избежание образования разрывов изоляции и заломов проводника минимальный радиус изгиба кабеля «витая пара» должен составлять 1 дюйм (2,5 см) или величину, равной четырем диаметрам кабеля; рекомендуемый радиус изгиба — 2 дюйма (5 см);
- во избежание возникновения посторонних электромагнитных помех и наводок минимальное расстояние от кабеля «витая пара» до близлежащего силового электрического кабеля с напряжением до 2 кВ должно быть более 5 дюймов (12,5 см), от кабеля с напряжением более 2 кВ — не менее 10 дюймов (25 см);
- участок сети от концентратора до сетевого адаптера не должен включать более трех отдельных отрезков кабеля (соединенных, например, посредством розеток или устройств Path-panel);

а все отрезки кабеля локальной сети (включая Path cord) должны быть одной категории. Рекомендуемый к использованию кабель — восьмижильная «витая пара» категории 5 или 5+ диаметром AWG=22 или 24.

Теперь давайте рассмотрим каждый из перечисленных выше этапов прокладывания локальной сети более подробно.

Монтаж разъемов RJ-45 на кабеле Path cord

Кабель Path cord — это небольшой отрезок кабеля «витая пара» длиной от 1 до 10 м, на обоих концах которого смонтирован разъем RJ-45. Этот кабель образует участок локальной сети от гнезда сетевого адаптера на компьютере до ближайшей сетевой розетки. Для изготовления одного провода Path cord вам потребуется, помимо отрезка кабеля, два защитных колпачка, два разъема RJ-45 и обжимной инструмент для этих разъемов.

Обжимной инструмент

Обжимной инструмент для разъемов RJ-45 несколько отличается от инструмента, используемого при прокладывании сетей 10Base2 (рис. 5.9).

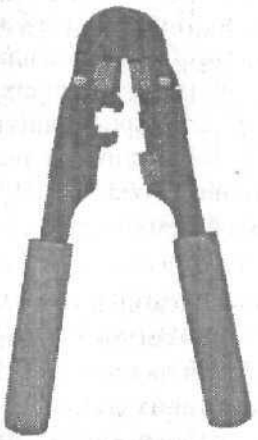


Рис. 5.9. Обжимной инструмент для разъемов RJ-45

Обжимной инструмент данного типа отличает, прежде всего, наличие специального выреза в форме разъема RJ-45 (в некоторых случаях рабочая часть инструмента имеет дополнительный вырез под разъем RJ-11, используемый в телефонии), помимо этого многие модели оснащены режущей кромкой для ровной обрезки кабеля «витая пара».

Защитные колпачки

Защитные колпачки внешне напоминают небольшие полые изнутри чехлы, повторяющие своей формой очертания разъема RJ-45, выполнены они из мягкого пластика или резины различных цветов. Многообразие расцветок

защитных колпачков имеет свой «философский смысл»: при подключении к концентратору нескольких кабелей они позволяют без труда определить, к какому именно компьютеру ведет тот или иной шнур. В этом случае достаточно лишь запомнить цвет, который вы заранее назначили для каждой из работающих в сети машин.

Защитные колпачки призваны предохранять место соединения кабеля «витая пара» с разъемом RJ-45 от изгибов и заломов. В принципе, ваша локальная сеть вполне сможет обойтись и без них: функциональные характеристики всей системы в целом от отсутствия защитных колпачков не изменятся.

Существует два типа защитных колпачков: литые — они надеваются на кабель до монтажа разъема RJ-45 и позже сдвигаются по направлению к разъему до нужной позиции, и разборные — они состоят из двух половинок, оснащенных замком, и могут надеваться на разъем уже после окончания его монтажа.

Разъем RJ-45

Разъемы RJ-45 представляют собой полый прозрачный пластиковый корпус с фиксирующим замком, внутри которого расположено восемь подвижных металлических контактов. В новом, необжатом разъеме контакты выходят за пределы корпуса, после обжима они вдавливаются внутрь, прорезая наружный изолирующий слой на проводниках, расположенных внутри кабеля «витая пара», и замыкаясь на проводящую жилу. Исходя из незначительных отличий в конструкции различают два типа разъемов RJ-45: с контактной вставкой и без таковой (разъем RJ-45 без контактной вставки показан на рис. 5.10). В дальнейшем мы будем рассматривать разъемы RJ-45 без контактной вставки.

Разъем с контактной вставкой несколько отличается по своему устройству от стандартного разъема RJ-45: он состоит из двух независимых элементов — вставки и собственно корпуса разъема (рис, 5.11, *а).*
Последовательность монтажа таких разъемов иная по сравнению с обычными: сначала проводники кабеля «витая пара» до упора вставляются в контактную вставку, затем вставка заводится до щелчка в корпус разъема, после чего разъем обжимается.

Верхняя кромка подвижных контактов разъема RJ-45 — острая, она имеет, как правило, два или три зубца (рис. 5.11, *б).* При обжиме разъема контакты утапливаются внутрь его корпуса, при этом верхняя кромка прорезает изолирующий слой проводника и впивается в проводящую жилу. Практика показывает, что контакты с тремя зубцами обеспечивают более высокую надежность соединения, но при этом двузубые контакты лучше режут изоляцию проводника. Обобщая можно сказать, что глобальных различий в качестве соединения при использовании этих двух типов разъемов нет, то есть можно смело покупать любой тип разъема RJ-45...

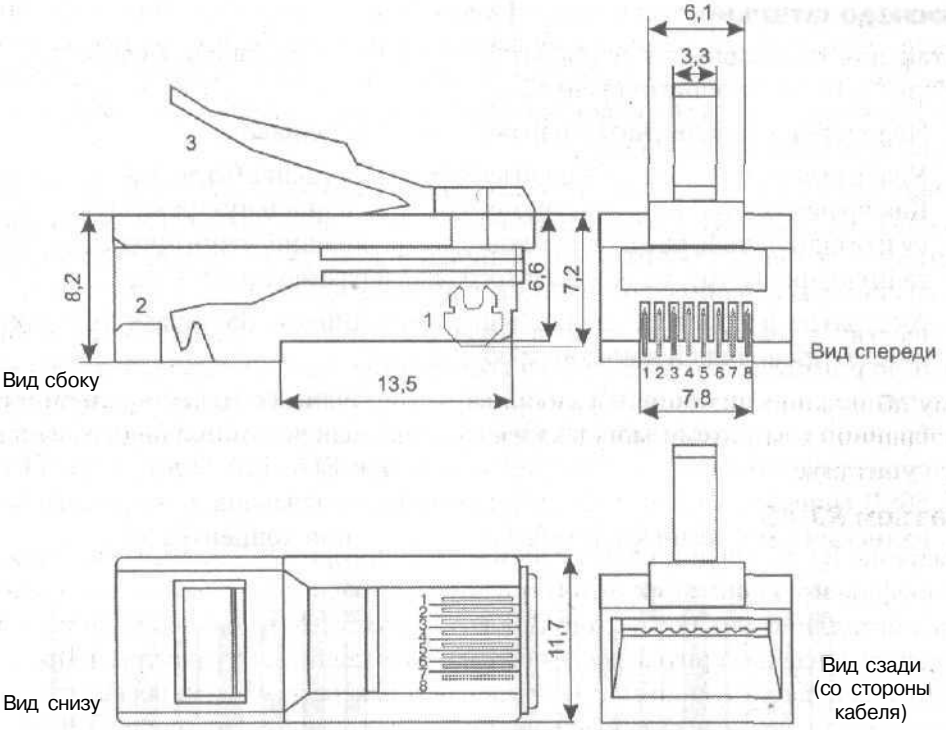


Рис. 5.10. Разъем RJ-45:
1 — контакты; *2*— держатель кабеля; *3*— замок разъема

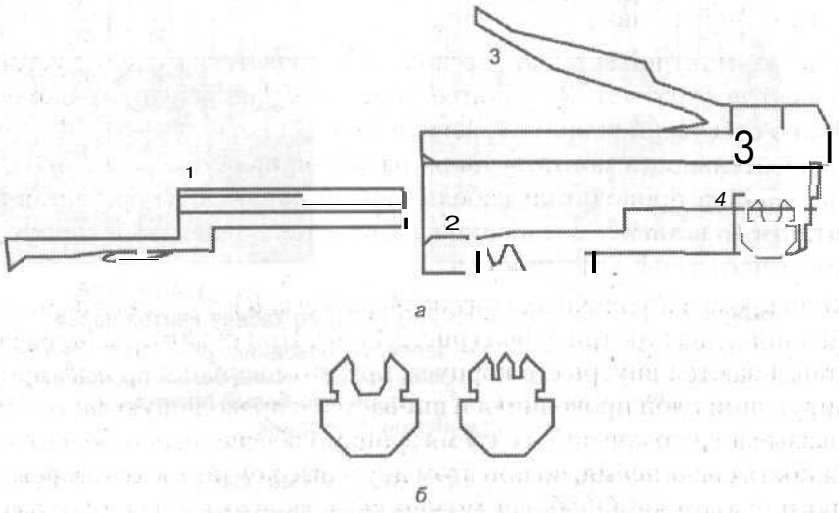


Рис. 5.11. Разъем RJ-45 с контактной вставкой:
1 — контактная вставка; *2*— держатель контактной вставки;
3 — замок разъема; *4*— контакты

Последовательность монтажа разъема

Итак, для того чтобы смонтировать разъем RJ-45 на кабель «витая пара», проделайте следующие операции.

1. Наденьте на кабель «витая пара» защитный колпачок.
2. Удалите верхний защитный слой кабеля на расстояние 0,5 дюйма (12,5 мм). Как правило, обжимной инструмент имеет специальную режущую кромку и ограничитель на это расстояние, позволяющий точно проделать указанную процедуру, не выверяя требуемый размер по линейке.
3. Аккуратно расплетите свитые пары проводников. Зачищать их изоляцию до проводящей жилы не требуется.
4. Расположите проводники витой пары в порядке, соответствующем выбранной вами схеме заделки кабеля. Всего для восьмижильного кабеля существует три возможные схемы заделки: EIA/TIA-568A, EIA/TIA-568B (рис. 5.12) и Cross-Over, которая предназначена для прямого соединения двух компьютеров без использования концентратора.

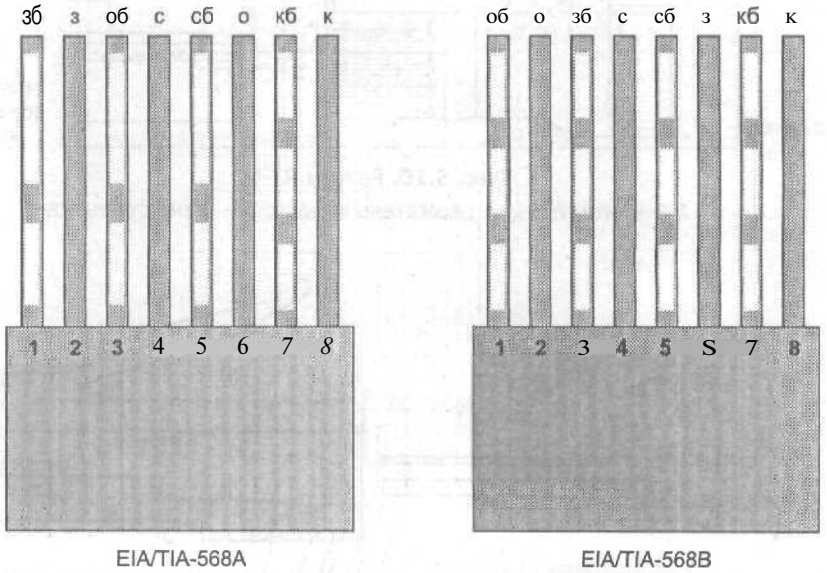


Рис. 5.12. Схемы заделки восьмижильного кабеля «витая пара»:
зб— зелено-белый проводник; *з* — зеленый проводник; *об*— оранжево-белый проводник; *о* — оранжевый проводник; *сб*— сине-белый проводник; *с* — синий проводник; *кб* — коричнево-белый проводник; *к*— коричневый проводник

Указанные схемы в целом идентичны, однако следует понимать, что на обоих концах кабеля схема должна быть одинаковой, за исключением случая, когда посредством кабеля «витая пара» напрямую соединяется два компьютера (речь о таком соединении пойдет дальше). Выбор

конкретного порядка следования проводников зависит от уже используемой в вашей локальной сети схемы заделки. Если вы создаете сеть заново, выберите любую из этих двух схем и в дальнейшем придерживайтесь именно ее.

5. В случае если вы используете четырехжильный кабель «витая пара», схема его заделки и расположение в разъеме будут несколько отличаться от описанного выше (рис. 5.13). Проводники располагаются в следующем порядке: оранжево-белый, оранжевый, сине-белый, синий, причем первые три подключаются к контактам разъема с 1 по 3, а последний – к контакту 6.

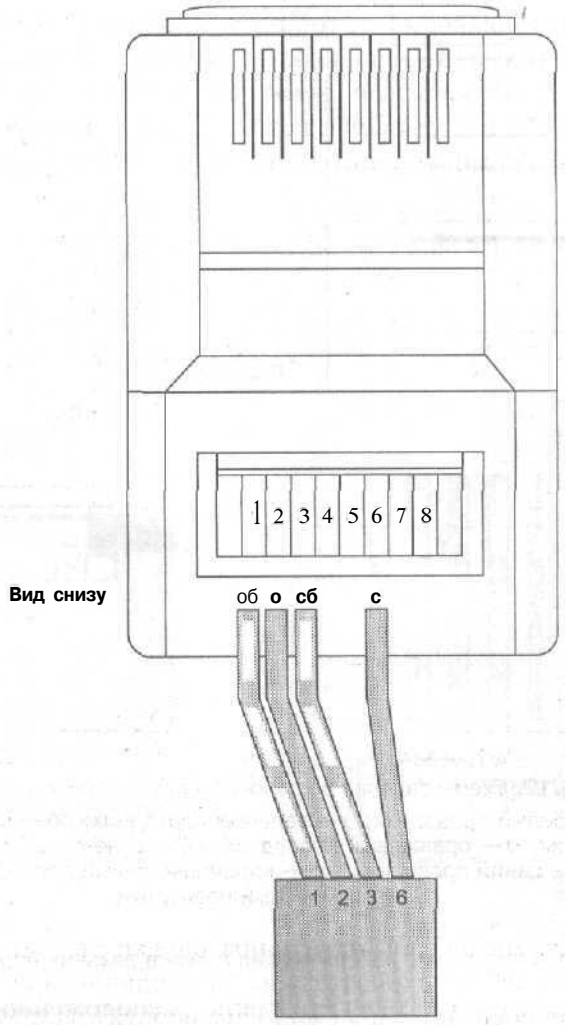


Рис. 5.13. Схема заделки четырехжильного кабеля «витая пара»

6. Расположив проводники соответствующим образом, возьмите в руки разъем RJ-45, переверните его контактами к себе, разместив тыльной стороной к кабелю — так, чтобы крепление замка оказалось на противоположной от кабеля стороне разъема, и до предела надвиньте его на выступающие из кабеля проводники (рис. 5.14).

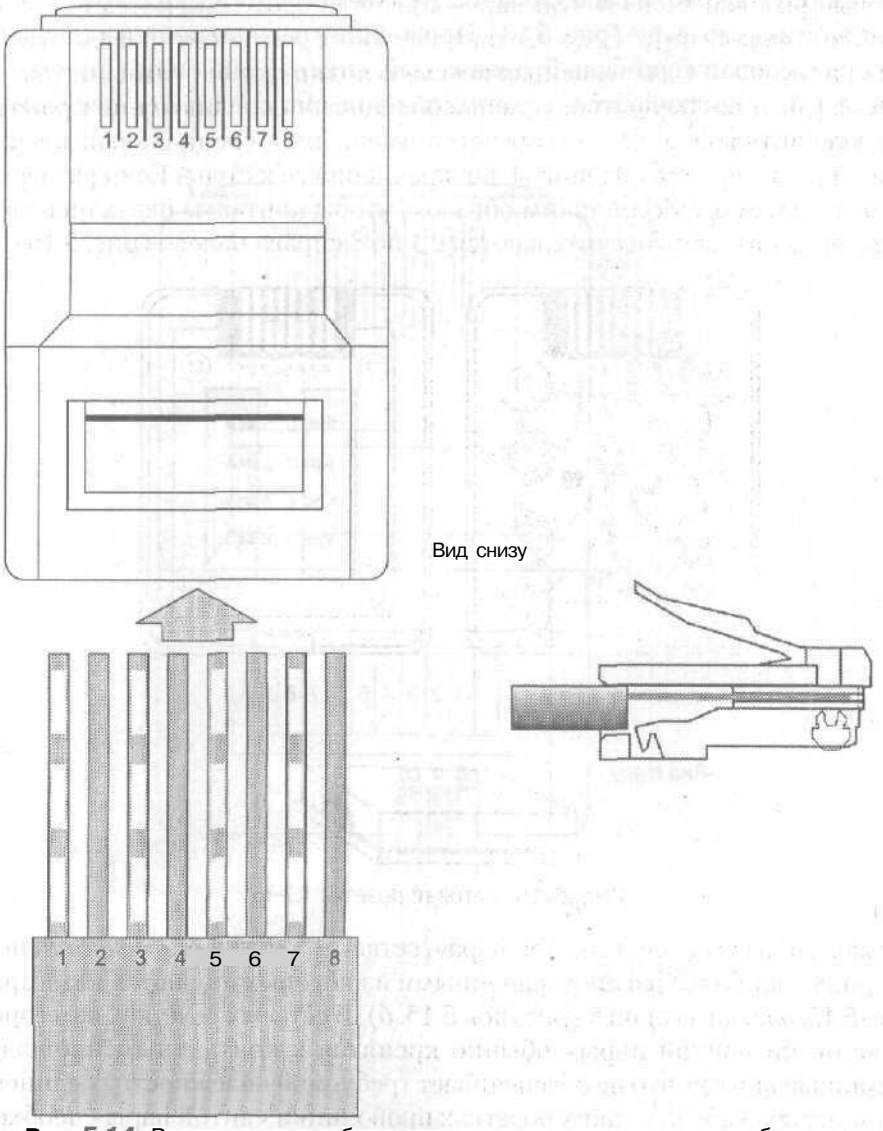


Рис. 5.14. Расположение кабеля «витая пара» в разъеме перед обжимом

7. Вставьте разъем с кабелем в углубление, расположенное на рабочей поверхности обжимного инструмента, и сильным быстрым нажатием на

ручки обожмите кабель. При этом выступающие из корпуса разъема контакты и держатель кабеля должны полностью утопиться внутрь разъема.

8. Смонтируйте аналогичным образом все требуемые разъемы RJ-45.

Монтаж сетевых розеток

Сетевые розетки под «витую пару» представляют собой пластмассовый короб со съемной крышкой, в верхней части которого смонтирована ответная часть разъема RJ-45, оснащенная восемью подпружиненными контактами, а также имеется то или иное приспособление для подключения проводников сетевого кабеля. Обычно розетка имеет либо специальный клеящий слой, либо отверстия под винты для крепления ее к стене. Если развернуть розетку разъемом к себе таким образом, чтобы контакты оказались внизу, то номера контактов отсчитываются с 1 по 8 справа налево (рис. 5.15).

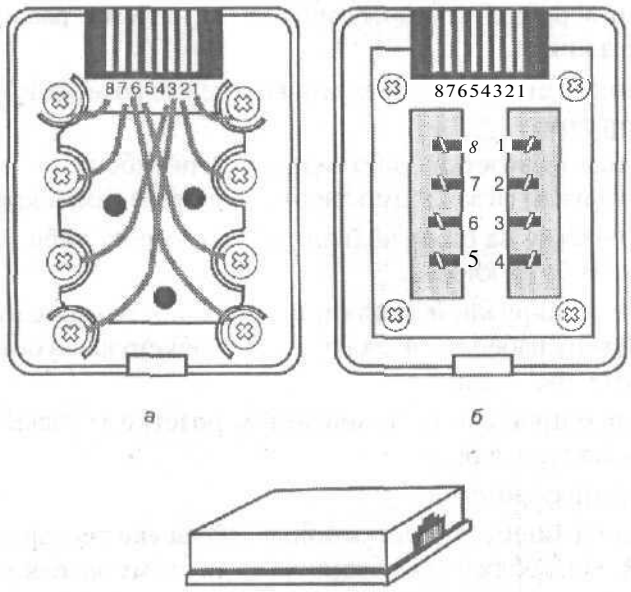


Рис. 5.15. Сетевая розетка RJ-45

Так же, как и сам кабель «витая пара», сетевые розетки различаются по категориям, наиболее распространенными из которых являются категория 3 (рис. 5.15, *а)* и категория 5 (рисунок 5.15, *б).* В сетевых розетках категории 3 проводники «витой пары» обычно крепятся к контактным площадкам с помощью винтов, что не обеспечивает требуемой надежности соединения. Для монтажа кабеля в таких розетках проводники «витой пары» необходимо расплести на необходимую длину, освободить от изоляции и, вставив в соответствующие контакты, зафиксировать прижимными винтами. При этом необходимо следить за тем, чтобы длина расплетенных проводников

была не слишком большой, в противном случае между ними могут возникнуть паразитные наводки. Определить, какой провод «витой пары» должен идти к каждому из прижимных винтов, можно по номерам контактов разъема розетки: в целом схема подключения проводников должна соответствовать выбранной вами схеме заделки кабеля (рис. 5.12).

В более современных розетках категории 5 проводники витой пары просто вставляются в щели специальных контактных площадок, расположенных под углом в 90° к плоскости разъема RJ-45 (рис. 5.15, *б*). При этом удаления защитного слоя с проводников не требуется: щели оснащены специальной режущей кромкой, которая сама прекрасно снимает с них изоляцию. Для надежной фиксации проводников в контактах розетки существует специальный инструмент, позволяющий поместить провод на максимальную глубину, однако в большинстве случаев можно прекрасно обойтись обыкновенным пинцетом и отверткой. Все контакты в розетках категории 5, как правило, пронумерованы, поэтому никаких проблем с разводкой кабеля возникнуть не должно.

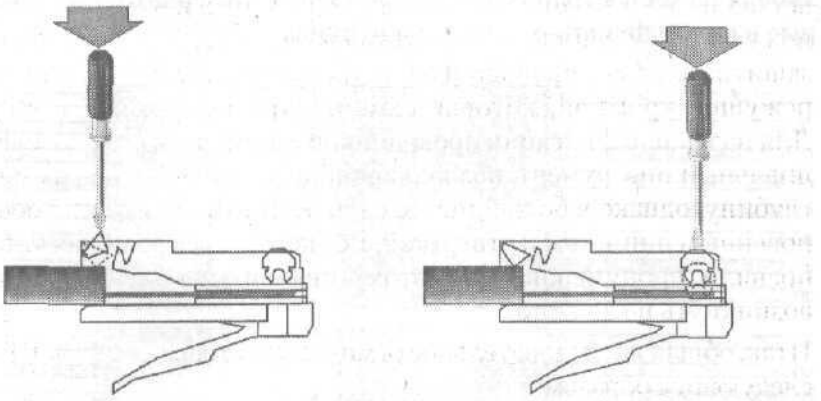
Итак, общая последовательность монтажа сетевых розеток RJ-45 выглядит следующим образом.

1. Снимите крышку розетки, либо надавив на нее сбоку, либо поддев края крышки отверткой (в зависимости от устройства замка крышки).
2. Закрепите розетку на стене вблизи рабочего места либо на фиксирующих винтах, либо на клею.
3. Освободите от наружной изоляции оконечность идущего от розетки к концентратору кабеля «витая пара» на требуемую глубину и аккуратно расплетите проводники.
4. Присоедините проводники к контактам розетки согласно выбранной вами схеме заделки кабеля.
5. Закройте крышку розетки.
6. На противоположном от розетки конце кабеля «витая пара» смонтируйте разъем RJ-45, соблюдая выбранную вами схему заделки.
7. Проложите кабель до места крепления концентратора, фиксируя его через равные промежутки на плинтусе или на стене специальными крепежными скобами (их можно приобрести в любом магазине строительных товаров).
8. Подключите разъем RJ-45 в соответствующий порт концентратора.

Если нет обжимного инструмента

Если под рукой не оказалось обжимного инструмента, разъем RJ-45 можно смонтировать при помощи обыкновенной отвертки. В процессе проведения подобной операции следует проявлять крайнюю осторожность, поскольку,

во-первых, обжим разъема «вручную» далеко не всегда обеспечивает требуемую надежность соединения, а во-вторых, многократно увеличивает опасность испортить разъем. Вместе с тем, такой способ монтажа вполне имеет право на жизнь, и более того, нередко применяется на практике. Итак, последовательность операций при монтаже разъема RJ-45 без обжимного инструмента такова (рис. 5.16).



а б

Рис. **5.16.** Монтаж разъема RJ-45 без обжимного инструмента

1. Вставьте в разъем кабель «витая пара», предварительно распределив проводники согласно выбранной вами схеме заделки.
2. Переверните разъем замком вниз, контактами к себе. Уложите его на ровную поверхность таким образом, чтобы края разъема имели надежную опору, а замок находился в свободном положении во избежание его случайных повреждений — например, между двух дощечек или двух книг.
3. Взяв в руки твердую отвертку, осторожным нажатием утопите вниз фиксатор кабеля до тех пор, пока он не перестанет выступать из корпуса разъема. Кабель будет надежно закреплен в корпусе (рис. 5.16, *а*).
4. Осторожными нажатиями на отвертку утопите в корпус разъема до упора все восемь выступающих наружу контактов — они должны проткнуть изоляционный слой проводников и «впиться» в проводящую жилу. Внимательно следите за тем, чтобы не погнуть и не повредить иным способом тонкие пластины контактов (рис. 5.16, *а).*

Прямое соединение двух компьютеров по схеме «точка—точка»

Для соединения двух компьютеров в сеть по технологии Ethernet lOBaseT без использования каких-либо дополнительных устройств, таких как концентраторы или сетевые розетки, вам потребуется специальным образом

смонтированный кабель «витая пара», который подключается непосредственно к разъемам RJ-45 присоединенных к сети компьютеров. Такой монтаж кабеля принято называть cross-over, MDI-X или null-hub cable. Длина cross-over-кабеля не должна превышать 100 м. Порядок следования проводников в разъемах для восьмижильного и четырехжильного кабеля при заделке по стандарту cross-over показан на рис. 5.17. Для восьмижильного кабеля на иллюстрации предлагается два альтернативных варианта, которые в целом функционально идентичны.

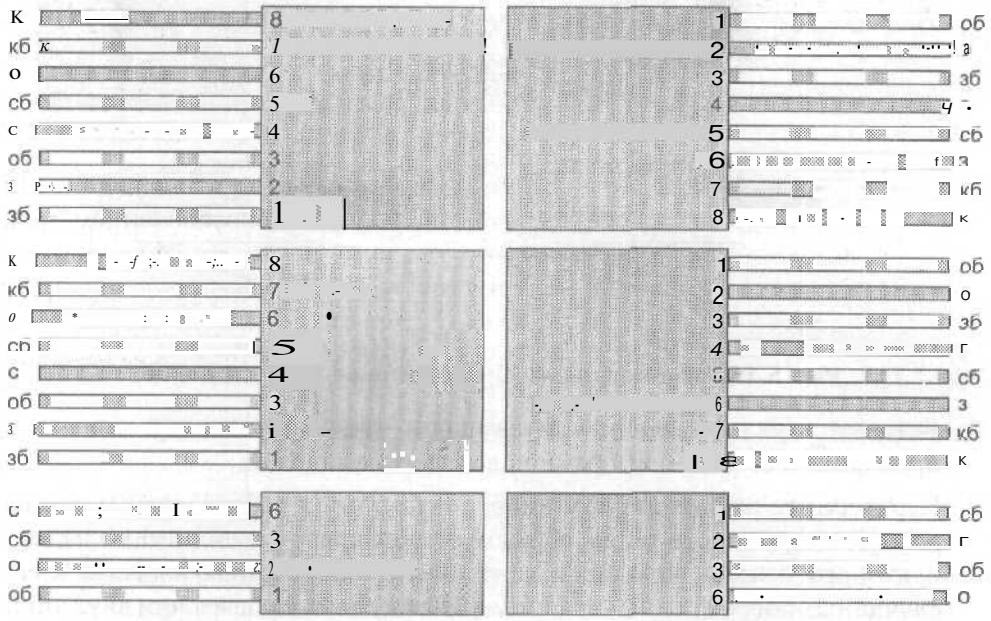


Рис. 5.17. Схема заделки кабеля «витая пара» при cross-over подключении:
зб — зелено-белый проводник; *з* — зеленый проводник; *об* — оранжево-белый проводник; *о*— оранжевый проводник; *сб* — сине-белый проводник; *с*— синий проводник; *кб* — коричнево-белый проводник; *к*— коричневый проводник

Обратите внимание на тот факт, что при использовании четырехжильного кабеля монтаж первых трех проводников в разъем осуществляется подключением к контактам 1, 2 и 3, а последнего — к контакту 6.

Глава 6

Настройка локальной сети

- Настройка локальной сети для Microsoft Windows XP
- Настройка локальной сети для Microsoft Windows 9x/ME
- Настройка локальной сети для Microsoft Windows 2000
- Управление общим доступом к сетевым ресурсам
- Принципы работы в локальной сети

Поскольку домашние локальные сети создаются обычно на основе двух компьютеров, один из которых, как правило, имеет более старую, а другой - более современную конфигурацию, необходимо рассмотреть принципы настройки локальной сети для нескольких различных операционных систем. И если одна из подключенных к локальной сети машин будет более совершенна по отношению к другой, вполне вероятно, что на ней будет установлена ОС Microsoft Windows XP. С изучения принципов настройки локальной сети в этой ОС мы и начнем настоящую главу.

Настройка локальной сети в Microsoft Windows XP

Прежде чем приступить к настройке локальной сети, необходимо задать сетевое имя вашего компьютера для идентификации его в сети, а также указать название рабочей группы. Щелкните правой кнопкой мыши на значке Мой компьютер, расположенном на Рабочем столе Windows, выберите в появившемся меню пункт Свойства и перейдите ко вкладке Имя компьютера открывшегося окна Система: Свойства.

Щелкните мышью на кнопке Изменить, чтобы создать или изменить сетевое имя компьютера и название рабочей группы.

В поле Имя компьютера диалогового окна Изменение имени компьютера введите сетевое имя своего компьютера. Если вы подключаетесь к сети, используя удаленный домен, установите переключатель Является членом в положение

Домена и введите в соответствующее поле название домена; если ваш компьютер входит в сетевую рабочую группу, выберите режим Рабочей группы и наберите ее название в расположенном рядом поле.

Компьютеры, работающие в больших корпоративных сетях, нередко используют DNS-сервер для определения своего сетевого адреса. Если вы хотите изменить конфигурацию DNS, щелкните мышью на кнопке Дополнительно и введите в поле Основной DNS-суффикс этого компьютера DNS-суффикс своего компьютера.

Если вы хотите, чтобы при подключении к другому домену DNS-суффикс вашего компьютера автоматически менялся, установите флажок рядом с функцией Сменить основной DNS-суффикс при смене членства в домене. Щелкните на кнопке OK, чтобы вернуться в окно Изменение имени компьютера.

Настало время настроить компьютер для работы в локальной сети. Вернитесь на вкладку Имя компьютера окна Свойства:Система и нажмите кнопку Идентификация. На экране появится окно Мастера сетевой идентификации (рис. 6.1).

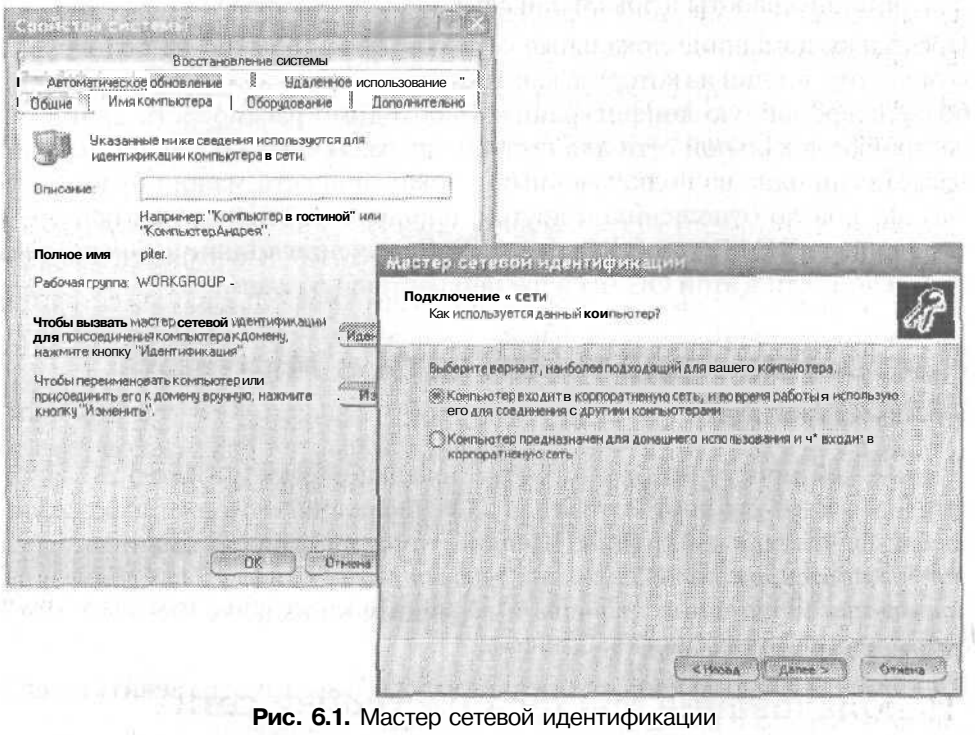


Рис. 6.1. Мастер сетевой идентификации

Щелкните на кнопке Далее. В следующем окне вам будет предложено выбрать вариант подключения к локальной сети: если ваш компьютер является частью большой корпоративной сети и вы намерены установить соединение с другими

сетевыми компьютерами, вам следует выбрать режим Компьютер входит в корпоративную сеть и во время работы я использую его для соединения с другими компьютерами. Если же ваш компьютер подключен к небольшой домашней сети, установите переключатель в положение Компьютер предназначен для домашнего использования и не входит в корпоративную сеть.

Щелкните на кнопке Далее. В случае подключения к домашней сети конфигурация компьютера на этом будет закончена: вам останется только нажать на кнопку Готово, чтобы покинуть окно Мастера сетевой идентификации. При подключении к корпоративной сети вам потребуется указать метод входа в сеть: если в ней используется домен, установите переключатель в режим Моя организация использует сеть с доменами, а если вы подключаетесь к рабочей группе, выберите режим Моя организация использует сеть без доменов, введите в следующем окне название рабочей группы, в которую входит ваш компьютер, и щелкните на кнопке Готово.

При подключении к сети, использующей сетевой домен, вам потребуется следующая информация:

- ваше имя пользователя для подключения к домену;
- пароль;
- ваша учетная запись для подключения к домену;
- сетевое имя вашего компьютера;
- имя домена.

В случае затруднений с определением одного из этих параметров обратитесь за разъяснениями к администратору вашей сети. Щелкните на кнопке Далее.

В следующем окне вам предстоит ввести ваше имя пользователя сети в поле Пользователь, набрать в поле Пароль свой сетевой пароль и указать в поле Домен имя вашего домена.

Снова нажмите Далее и в следующем окне наберите сетевое имя своего компьютера (поле Имя компьютера) и сетевое имя домена, если оно отличается от домена, через который вы входите в локальную сеть.

Нажмите Далее. Ваш компьютер идентифицирован в локальной сети. Щелкните на кнопке Готово, чтобы покинуть окно Мастера сетевой идентификации.

Перезагрузите компьютер, чтобы все изменения, внесенные вами в настройку сети, вступили в силу.

Использование Мастера настройки сети

Откройте системную папку Сетевое окружение и щелкните на расположенной в меню Сетевые задачи функции Установить домашнюю или малую сеть. На экране появится окно Мастера настройки сети.

Щелкните на кнопке Далее. В следующем окне Мастер сообщит вам о возможных вариантах сетевых настроек и необходимости установить на компьютере соответствующее оборудование до того, как вы начнете процедуру подключения к локальной сети. Снова нажмите Далее. В новом окне, позволяющем выбрать метод подключения к сети, установите переключатель в режим Другое и еще раз щелкните на кнопке Далее. Теперь необходимо указать системе тип сетевого подключения.

В большинстве случаев оптимальный режим подключения к домашней или корпоративной локальной сети, не имеющей соединения с высокоскоростной магистралью Интернета, — Этот компьютер принадлежит к сети, не имеющей подключения к Интернету. Установите переключатель в соответствующее положение и снова нажмите Далее.

В следующем окне укажите сетевое имя и дайте описание своего компьютера.

Введите произвольное описание компьютера в поле Описание, например, «Computer of Marketing Department», «Piter-Press Network Computer» или «Компьютер отдела продаж». Сетевое имя компьютера будет отображаться в папке Сетевое окружение других пользователей локальной сети. Оно и предназначено для идентификации компьютера в сетевой структуре. Введите его в поле Имя компьютера и нажмите на кнопку Далее.

В следующем окне укажите название сетевой рабочей группы, к которой принадлежит ваш компьютер.

Если вы не знаете, к какой рабочей группе подключается ваш компьютер, выясните это у администратора локальной сети либо (если сеть создается заново) используйте произвольное имя, однако помните, что оно должно быть одинаково для всех работающих в сети компьютеров. Введите название рабочей группы в поле Рабочая группа и щелкните на кнопке Далее. В следующем окне Мастер настройки сети продемонстрирует все указанные вами сведения. Если что-либо введено неправильно, воспользуйтесь кнопкой Назад, чтобы отредактировать соответствующие настройки. Когда все будет готово, нажмите на кнопку Далее.

Теперь Windows XP автоматически протестирует конфигурацию локальной сети и настроит сетевое подключение на вашем компьютере.

Чтобы настроить подключение к локальной сети на других компьютерах, входящих в сеть, вы должны выбрать один из режимов в следующем окне Мастера настройки сети (рис. 6.2).

Для того чтобы настроить подключение к локальной сети на компьютерах, не использующих Microsoft Windows XP, можно воспользоваться компакт-диском с дистрибутивом Windows XP, либо диском, содержащим информацию о сетевых настройках и Мастер установки сети. Чтобы создать подобный диск, поместите в дисковод чистую отформатированную дискету,

установите переключатель в режим Создать диск настройки сети и щелкните на кнопке Далее. Если вы уже располагаете такой дискетой, в текущем окне Мастера настройки сети выберите режим Использовать уже имеющийся диск настройки сети. Для того чтобы использовать дистрибутивный компакт-диск Windows XP, выберите пункт Использовать компакт-диск Windows XP. Если вы не хотите менять конфигурацию локальной сети на других сетевых компьютерах, на которых конфигурация сети уже полностью настроена, установите переключатель в положение Просто завершить работу Мастера; нет нужды запускать его на других компьютерах.

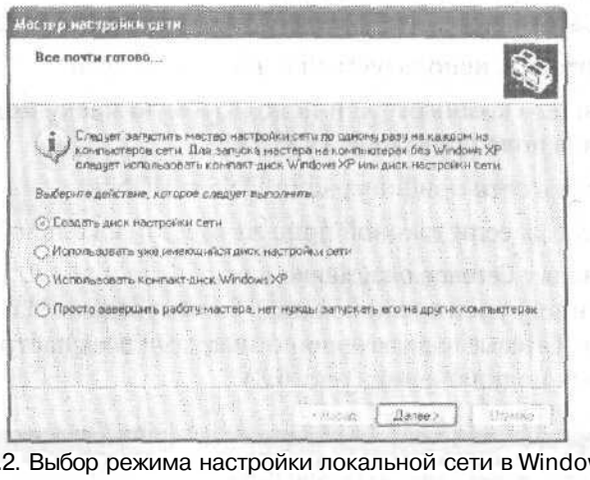


Рис. 6.2. Выбор режима настройки локальной сети в Windows XP

Сетевая дискета даст вам возможность автоматически настроить локальную сеть на подключенных к сети компьютерах, не использующих Windows XP. Чтобы применить Мастер конфигурации сети на таком компьютере, вставьте созданную вами дискету в дисковод, запустите программу Netsetup и укажите Мастеру информацию о сетевом имени компьютера и рабочей группе, к которой он принадлежит. Локальная сеть будет настроена на данном компьютере автоматически.

ПРИМЕЧАНИЕ

Программа Netsetup запускается только на компьютерах, работающих под управлением Windows 98, Windows 98 SE, Windows Millennium Edition и Windows 2000. Если на сетевом компьютере используется другая операционная система, например, Windows 95 или Windows 3.X, настраивать конфигурацию локальной сети вам придется вручную.

Настройка локальной сети завершена. Щелкните на кнопке Готово, чтобы покинуть окно Мастера настройки сети.

Чтобы все указанные вами настройки вступили в силу, перезагрузите компьютер.

Настройка конфигурации и протоколов

Если вы создаете свою локальную сеть заново, обычно каких-либо дополнительных настроек после проведения описанных выше процедур не требуется — такая сеть будет вполне работоспособна. Однако автоматически создаваемые Мастером настройки сети настройки режимов доступа в сеть и сетевых протоколов могут не соответствовать действующей конфигурации локальной сети, вследствие чего работа в сети будет невозможна. Если, открыв папку Сетевое окружение, вы не увидите в ней значков подключенных к локальной сети компьютеров, придется изменить настройки сетевых протоколов вручную. Для этого выясните у сетевого администратора следующее:

- сетевой протокол, используемый в локальной сети;
- IP-адрес вашего компьютера и используемую маску подсети, если сеть работает на основе протокола TCP/IP;
- применяемая в сети конфигурация DNS и WINS;
- IP-адрес шлюза, если таковой присутствует в локальной сети.

Перейдите в папку Сетевое окружение и выберите пункт Отобразить сетевые подключения в инструментальной панели Сетевые задачи. На экране появится системное окно Сетевые подключения со значками всех настроенных в вашей системе сетевых подключений (рис. 6.3).

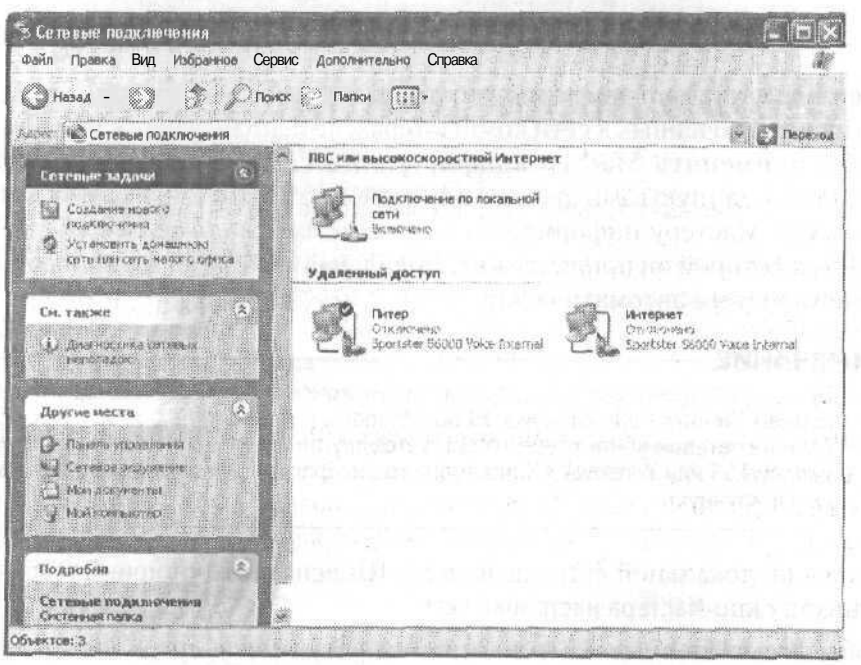


Рис. 6.3. Диалоговое окно Сетевые подключения

Дважды щелкните мышью на значке соответствующего сетевого подключения, чтобы вызвать на экран окно статуса локальной сети.

Для того чтобы внести какие-либо изменения в конфигурацию локальной сети, щелкните на кнопке Изменение настроек подключения. На экране появится диалоговое окно свойств сетевого подключения.

Если вы хотите изменить аппаратные настройки своего сетевого адаптера, щелкните на кнопке Настроить, а для того чтобы при подключении к локальной сети в Области уведомлений Windows XP отображался графический индикатор, установите флажок рядом с функцией При подключении вывести значок в Области уведомлений.

Если локальная сеть работает с использованием протоколов NetBEUI/NetBIOS или IPX/SPX, вам следует установить поддержку этих протоколов в своей системе. Щелкните на кнопке Установить, в появившемся меню выберите пункт Протокол и в открывшемся окне дважды щелкните на пункте NWLink IPX/SPX/NetBIOS-совместимый транспортный протокол (рис. 6.4).

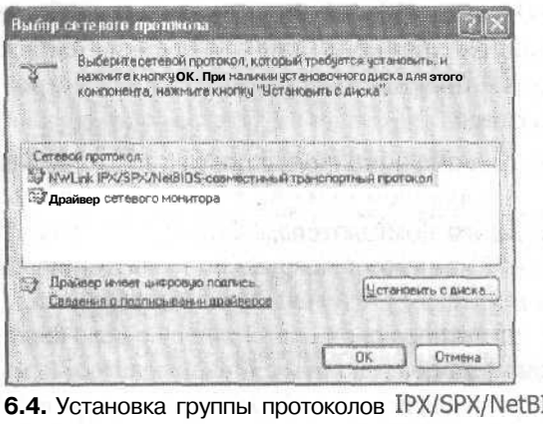


Рис. 6.4. Установка группы протоколов IPX/SPX/NetBIOS

Если ваша локальная сеть работает с использованием протокола TCP/IP, необходимо настроить его параметры в соответствии с действующей сетевой конфигурацией. Для этого выделите пункт Протокол Интернета (TCP/IP) в окне Подключение по локальной сети — свойства и нажмите на кнопку Свойства. На экране появится окно настройки протокола TCP/IP.

Введите IP-адрес своего компьютера в поле Использовать следующий IP-адрес, а в поле Маска подсети — маску подсети. Если в локальной сети используется шлюз, укажите его IP-адрес в поле Основной шлюз. В том случае, если в сети предусмотрено использование DNS-серверов, укажите IP-адреса первичного и вторичного DNS-серверов в полях Предпочитаемый DNS-сервер и Альтернативный DNS-сервер.

Если в сети используется более одного шлюза, вы можете настроить их параметры, воспользовавшись вкладкой Параметры IP диалогового окна

Дополнительные параметры TCP/IP. Оно открывается нажатием на кнопку Дополнительно. Перейдите ко вкладке DNS и введите DNS-суффикс в поле DNS суффикс для подключения, если этого требует конфигурация вашего DNS-сервера. И, наконец, настроить конфигурацию WINS можно при помощи одноименной вкладки окна Дополнительные параметры TCP/IP. По умолчанию поддержка WINS для протокола TCP/IP отключена.

Щелкните на кнопке OK, чтобы сохранить изменения, внесенные в настройки сетевой конфигурации. Для того чтобы эти изменения вступили в силу, потребуется перезагрузка компьютера.

Настройка локальной сети в Microsoft Windows 9x/ME

Первоначальная настройка локальной сети в операционной системе Microsoft Windows Millennium Edition может быть выполнена при помощи Мастера домашней сети, который можно вызвать двойным щелчком мыши на соответствующем значке в окне Мое сетевое окружение. Так же как и в MS Windows XP, этот Мастер призван помочь настроить локальную сеть на вашем компьютере.

После того как на экране появится окно Мастера домашней сети, нажмите на кнопку Далее. В следующем окне вам будет предложено определить тип подключения данного компьютера к Интернету. Всего предлагается три варианта: Да, данный компьютер использует подключение к другому компьютеру домашней сети, который обеспечивает прямой доступ к поставщику услуг Интернета, Да, данный компьютер использует прямое подключение к поставщику услуг Интернета с помощью устройства: [ваш сетевой адаптер] и, наконец, Нет, данный компьютер не настроен для использования Интернета (рис. 6.5). Если вы хотите просто настроить локальную сеть на ваших компьютерах, выберите третий вариант и щелкните мышью на кнопке Далее,

В поле Имя компьютера введите уникальное имя вашего компьютера, которое будет идентифицировать его в локальной сети. В поле Имя рабочей группы наберите название рабочей группы, узлом которой является данный компьютер. Снова нажмите Далее.

В следующем окне вам будет предложено выбрать папки и принтеры, которые могут быть доступны другим пользователям из локальной сети. Установите соответствующие флажки, при необходимости разрешить удаленный доступ к выбранным папкам по паролю щелкните мышью на кнопке Пароль и дважды введите его в соответствующие поля. Впоследствии этот пароль будет запрашиваться при попытке других пользователей обратиться к вашему компьютеру. Щелкните мышью на кнопке Далее.

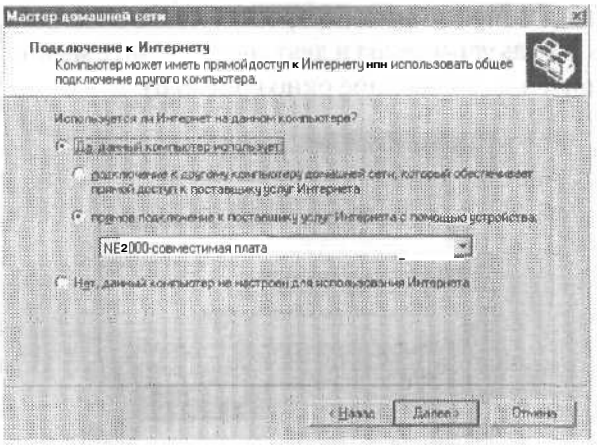


Рис. 6.5. Мастер домашней сети

На следующем этапе вам будет предложено создать диск настройки сети, который позволит установить локальную сеть с текущими настройками на других компьютерах. Если у вас уже имеется аналогичный диск, созданный при помощи операционной системы Microsoft Windows XP, вы можете пропустить этот шаг, установив переключатель в положение Нет, сейчас создавать дискету не требуется. В противном случае, чтобы создать подобный диск, поместите в дисковод чистую отформатированную дискету, установите переключатель в режим Да, создать установочную дискету домашней сети и щелкните на кнопке Далее. Чтобы применить Мастер конфигурации сети на таком компьютере, вставьте созданную вами дискету в дисковод, запустите программу Netsetup и укажите Мастеру информацию о сетевом имени компьютера и рабочей группе, к которой он принадлежит. Локальная сеть будет настроена на данном компьютере автоматически.

Для завершения работы Мастера щелкните мышью на кнопке Готово и перезапустите операционную систему. Чтобы запустить Мастер настройки домашней сети на других компьютерах, работающих под управлением Microsoft Windows ME, выполните последовательность команд Пуск ▸ Программы ▸ Стандартные ▸ Связь ▸ Мастер домашней сети. На компьютерах, работающих под управлением Windows 95 или Windows 98 можно воспользоваться созданной вами дискетой настройки сети.

Настройка конфигурации и протоколов в Windows 9x

В некоторых случаях, например когда вы не пользуетесь подготовленной ранее дискетой настройки сети или если вы настраиваете локальную сеть на компьютерах, работающих под управлением ОС семейства Windows 9x, в составе которых отсутствует Мастер настройки домашней сети, вам

потребуется указать некоторые настройки локальной сети вручную. Для этого откройте Панель управления и дважды щелкните мышью на значке Сеть. На экране появится одноименное окно (рис. 6.6).

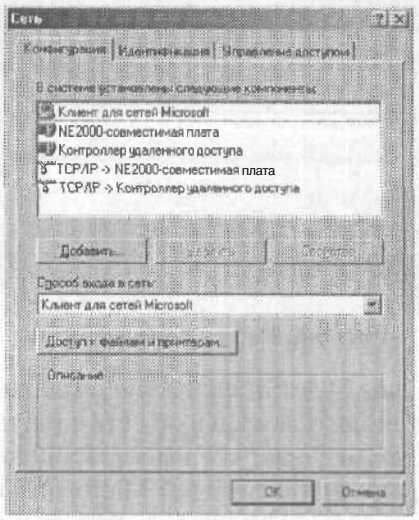


Рис. 6.6. Диалоговое окно Сеть

Перейдите ко вкладке Идентификация и проверьте правильность указанных там имени компьютера и названия рабочей группы. Вводить произвольное описание компьютера не обязательно. На вкладке Управление доступом вы можете задать режим управления удаленными подключениями к данному компьютеру. Всего существует два режима управления доступом: *на уровне ресурсов,* — в этом режиме администратор компьютера может открывать или закрывать сетевой доступ к отдельным ресурсам компьютера, таким как: папки, файлы, дисковые разделы или принтеры; и на уровне пользователей — в этом режиме доступ выборочно открывается или закрывается для отдельных пользователей локальной сети или групп пользователей. Первый из этих двух режимов является используемым по умолчанию.

Перейдите ко вкладе Конфигурация. Конфигурация сети включает, как правило, набор клиентов, адаптеров, протоколов и служб. *Клиент* (в терминологии ОС Windows) — это набор программного обеспечения, поддерживающий двусторонний обмен данными между локальной сетью и данным компьютером. *Адаптеры* — это устройства, посредством которых реализуется непосредственное подключение компьютеров к сети. В ОС Microsoft Windows 9x/ME различается два типа адаптеров — физические, то есть те сетевые карты, которые непосредственно входят в аппаратную конфигурацию компьютера, и «виртуальные адаптеры», в частности, так называемый Контроллер удаленного доступа — программный эмулятор сетевого адаптера,

используемый операционной системой. В свою очередь, *службы* — это подсистемы сетевого программного обеспечения, созданные для выполнения какой-либо одной конкретной задачи, например для организации общего доступа к ресурсам компьютера, удаленного обращения к реестру и т. д. По умолчанию в ОС Windows 9x/ME устанавливаются, как правило, следующие компоненты конфигурации локальной сети.

1. Клиент для сетей Microsoft — комплект клиентского программного обеспечения, поддерживающего работу в сетях Microsoft Windows;
2. Сетевой адаптер — сетевой адаптер, входящий в аппаратную конфигурацию вашего компьютера;
3. Контроллер удаленного доступа — программный модуль для обеспечения удаленных подключений по локальной сети;
4. Протокол TCP/IP для сетевого адаптера;
5. Протокол TCP/IP для Контроллера удаленного доступа.

Чтобы настроить ваш компьютер для работы в локальной сети, щелкните на кнопке Доступ к файлам и принтерам в окне Сеть и установите флажки Файлы этого компьютера можно сделать общими и Принтеры этого компьютера можно сделать общими. Нажмите на кнопку OK. В списке конфигурации сети появится новый пункт — Служба доступа к файлам и принтерам сетей Microsoft.

Если конфигурация вашей локальной сети требует использования доменов Windows NT/2000, вы можете настроить режим подключения к этим доменам при входе в сеть, выбрав в списке пункт Клиент для сетей Microsoft и нажав на кнопку Свойства. В открывшемся окне также существует возможность изменить настройки подключения к сети: режим Быстрый вход в сеть подразумевает, что при загрузке операционной системы компьютер регистрируется в сети, но сетевые диски подключаются только по мере обращения к ним; в режиме Вход с восстановлением сетевых подключений операционная система проверяет в процессе своей загрузки готовность всех зарегистрированных в Windows удаленных устройств, таких как сетевые диски и сетевые принтеры. Если вы работаете в стандартной конфигурации локальной сети, где не требуется обязательного подключения всех сетевых устройств, выберите первый режим, если вы используете какие-либо программы, требующие обращения к удаленным ресурсам сети (например, некоторые версии «1С» или приложения, работающие с распределенными базами данных), второй режим предпочтительнее.

Для того чтобы настроить протокол TCP/IP, выделите в списке конфигурации сети пункт TCP/IP для сетевого адаптера и щелкните мышью на кнопке Свойства. На экране появится диалоговое окно Свойства: TCP/IP, открытое на вкладке IP-адрес (рис. 6.7).

1. Установите переключатель в положение Указать IP-адрес явным образом и введите в поля IP-адрес и Маска подсети требуемые значения. Установите флажок Обнаружение подключения к сетевой плате.
2. Перейдите ко вкладке Привязка. На ней должны быть установлены флажки Клиент для сетей Microsoft и Служба доступа к файлам и принтерам.

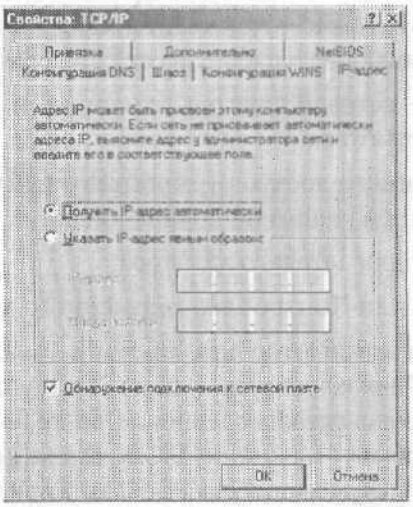


Рис. 6.7. Окно настройки протокола TCP/IP

3. Перейдите ко вкладке Дополнительно и установите флажок Использовать данный протокол по умолчанию.
4. Щелкните мышью на кнопке OK, закрывая окно Свойства: TCP/IP, еще раз нажмите OK в окне Сеть и перезагрузите компьютер.

При следующей загрузке Windows на экране появится диалоговое окно Ввод сетевого пароля (рис. 6.8), в котором вам будет предложено ввести имя пользователя и пароль для подключения к локальной сети. Введите соответствующие значения в поля Имя пользователя и Пароль (поле Пароль можно оставить пустым) и запомните их, поскольку в последствии вам придется правильно указывать эти значения при каждом входе в Windows. Если вы укажете неправильный пароль или нажмете на кнопку Отмена, вполне вероятно, что локальная сеть перестанет быть доступной на данном компьютере.

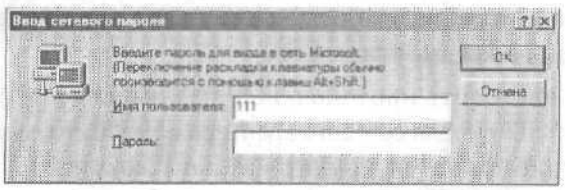


Рис. 6.8. Окно Ввод сетевого пароля

СОВЕТ

Если вы неправильно ввели пароль или хотите повторить подключение к сети без перезагрузки компьютера, выполните команды Пуск ▸ Завершение сеанса, щелкните в открывшемся окне на кнопке Да и снова введите ваши учетные данные для входа в сеть в окне Ввод сетевого пароля.

ВНИМАНИЕ

Для того чтобы настраиваемый вами компьютер был «виден» в сетевом окружении других удаленных узлов локальной сети, вы должны открыть на нем общий доступ как минимум к одному ресурсу. О том, как это сделать, будет рассказано далее в этой главе.

Настройка протоколов NetBEUI/NetBIOS

Б отличие от протокола TCP/IP настройка протоколов семейства NetBEUI/NetBIOS для операционных систем Microsoft Windows 9x/ME производится достаточно просто, к тому же эти протоколы менее чувствительны к изменениям параметров их конфигурации. Однако следует учитывать, что если вы хотите обеспечить общий доступ к Интернету на всех компьютерах локальной сети, они должны поддерживать протокол TCP/IP.

Для настройки протоколов NetBEUI/NetBIOS на компьютере, работающем под управлением Microsoft Windows 9x/ME, откройте Панель управления и дважды щелкните мышью на значке Сеть. На экране появится одноименное окно. Щелкните мышью на кнопке Добавить, в окне Выбор типа компонента дважды щелкните мышью на пункте Протокол и выберите в появившемся списке пункт NetBEUI. В списке компонентов конфигурации локальной сети появится две новых позиции: NetBEUI -> Ваш сетевой адаптер и NetBEUI -> Контроллер удален ного доступа. Выделите щелчком мыши первый из них и нажмите на кнопку Свойства. На экране появится диалоговое окно Свойства: NetBEUI (рис. 6.9).

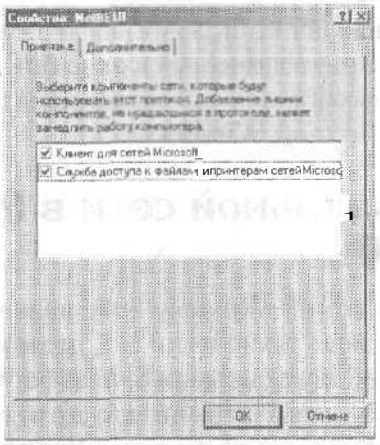


Рис. 6.9. Окно настройки протокола NetBEUI

Проследите за тем, чтобы на вкладке Привязка были установлены флажки Клиент для сетей Microsoft и Служба доступа к файлам и принтерам сетей Microsoft. Если в вашей локальной сети используется только протокол NetBEUI, а также не требуется обеспечить совместный доступ к Интернету, перейдите ко вкладке Дополнительно и установите флажок Использовать этот протокол по умолчанию, во всех прочих случаях делать это не рекомендуется. Щелкните мышью на кнопке OK, закрывая окно Свойства: NetBEUI, еще раз нажмите OK в окне Сеть и перезагрузите компьютер. В процессе перезагрузки вам может понадобиться диск, содержащий дистрибутив Microsoft Windows.

Настройка протоколов семейства IPX/SPX

Если в вашей локальной сети требуется использование протоколов **IPX/SPX**, для их установки и настройки проделайте описанные ниже действия.

1. Откройте окно Панели управления и дважды щелкните мышью на значке Сеть. На экране появится одноименное окно.
2. Щелкните мышью на кнопке Добавить, в окне Выбор типа компонента дважды щелкните мышью на пункте Протокол и выберите в появившемся списке пункт IPX/SPX-совместимый протокол.
3. В списке компонентов конфигурации локальной сети появятся две новые позиции: IPX/SPX-совместимый протокол -> Ваш сетевой адаптер и IPX/SPX-совместимый протокол -> Контроллер удаленного доступа. Выделите щелчком мыши первый из них и нажмите на кнопку Свойства. На экране появится диалоговое окно Свойства: IPX/SPX-совместимый протокол.
4. Перейдите ко вкладке NetBIOS и установите флажок Запустить поддержку NetBIOS протоколом IPX/SPX.
5. Перейдите ко вкладке Дополнительно и установите в поле Макс. число каналов значение 5, а в поле Макс. число подключений значение 10.
6. Щелкните мышью на кнопке OK, закрывая окно Свойства: IPX/SPX-совместимый протокол, еще раз нажмите OK в окне Сеть и перезагрузите компьютер. В процессе перезагрузки вам может понадобиться диск, содержащий дистрибутив Microsoft Windows.

Настройка локальной сети в Microsoft Windows 2000

Как и Windows XP, Microsoft Windows 2000 является операционной системой, созданной на основе технологии NT, поэтому методики настройки локальной сети на этих двух системных платформах весьма схожи. Для определения уникальности имени работающего в сети компьютера, а также для указания имени рабочей группы служит Мастер сетевой идентификации,

который можно вызвать на исполнение, щелкнув правой кнопкой мыши на значке Мой компьютер, расположенном на Рабочем столе Windows, выбрав в появившемся меню пункт Свойства, перейдя ко вкладке Сетевая идентификация открывшегося окна Свойства системы и нажав на кнопку Идентификация.

Щелкните на кнопке Далее. В следующем окне вам будет предложено выбрать вариант подключения к локальной сети: если ваш компьютер является частью большой корпоративной сети, и вы намерены установить соединение с другими сетевыми компьютерами, вам следует выбрать режим Компьютер входит в корпоративную сеть и во время работы я использую его для соединения с другими компьютерами. Если же ваш компьютер подключен к небольшой домашней сети, установите переключатель в положение Компьютер предназначен для домашнего использования и не входит в корпоративную сеть.

Щелкните на кнопке Далее. В случае подключения к домашней сети конфигурация компьютера на этом будет закончена: вам останется только нажать на кнопку Готово, чтобы покинуть окно Мастера сетевой идентификации. При подключении к корпоративной сети вам потребуется указать метод входа в сеть: если в ней используется домен, установите переключатель в режим Моя организация использует сеть с доменами, а если вы подключаетесь к рабочей группе, выберите режим Моя организация использует сеть без доменов, введите в следующем окне название рабочей группы, в которую входит ваш компьютер, и щелкните на кнопке Готово.

При подключении к сети, использующей сетевой домен, вам потребуется следующая информация:

- ваше имя пользователя для подключения к домену;
- пароль;
- ваша учетная запись для подключения к домену;
- сетевое имя вашего компьютера;
- имя домена.

В случае затруднений с определением одного из этих параметров обратитесь за разъяснениями к администратору вашей сети. Щелкните на кнопке Далее.

В следующем окне вам предстоит ввести ваше имя пользователя сети в поле Пользователь, набрать в поле Пароль свой сетевой пароль и указать в поле Домен имя вашего домена.

Снова нажмите Домен и в следующем окне наберите сетевое имя своего компьютера (поле Имя компьютера) и сетевое имя домена, если оно отличается от домена, через который вы входите в локальную сеть.

Снова нажмите Далее. Ваш компьютер идентифицирован в локальной сети. Щелкните на кнопке Готово, чтобы покинуть окно Мастера сетевой идентификации.

Перезагрузите компьютер, чтобы все внесенные вами изменения в настройку сети вступили в силу.

Для последующего изменения идентификационных данных можно воспользоваться кнопкой Свойства, расположенной на вкладке Сетевая идентификация окна Свойства системы. На экране появится диалоговое окно Изменение идентификации, в котором вы сможете указать новое сетевое имя компьютера, название рабочей группы или имя домена (рис. 6.10).

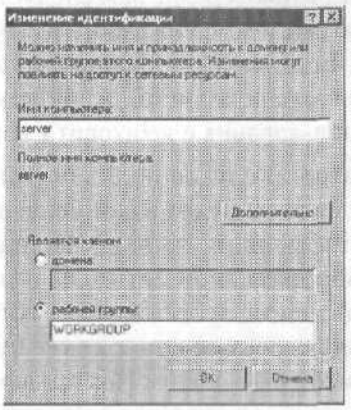


Рис. 6.10. Диалоговое окно Изменение идентификации

Настройка конфигурации и протоколов в Windows 2000

Настройка конфигурации и протоколов локальной сети в Microsoft Windows 2000 осуществляется следующим образом: откройте Панель управления, дважды щелкните мышью на значке Сеть и удаленный доступ к сети, в открывшемся окне, содержащем значки всех настроенных в вашей системе сетевых подключений, выделите значок подключения к локальной сети, щелкните на нем правой кнопкой мыши и в появившемся меню выберите пункт Свойства. На экране появится диалоговое окно Подключение по локальной сети - свойства (рис. 6.11).

Выделите в списке компонент пункт Протокол Интернета (TCP/IP) и щелкните мышью на кнопке Свойства. В открывшемся окне Свойства: Протокол Интернета (TCP/IP) установите переключатель в положение Использовать следующий IP-адрес, после чего введите соответствующие значения в поля IP-адрес и Маска подсети. Для настройки дополнительных параметров протокола, таких как адреса DNS-серверов или конфигурации WINS, можно воспользоваться кнопкой Дополнительно. Щелкните на кнопке OK, чтобы сохранить изменения, внесенные в настройки сетевой конфигурации. Для того чтобы эти изменения вступили в силу, потребуется перезагрузка компьютера.

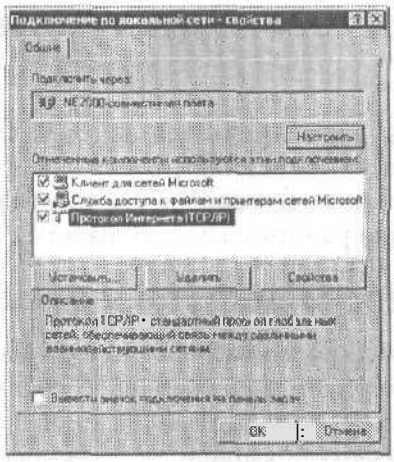


Рис. 6.11. Диалоговое окно Подключение по локальной сети — свойства

Настройка протоколов NetBEUI/IPX/SPX в Windows 2000

Чтобы настроить поддержку протоколов NetBEUI/NetBIOS или IPX/SPX под управлением операционной системы Microsoft Windows 2000, необходимо проделать предложенную далее последовательность шагов.

1. Откройте Панель управления, дважды щелкните мышью на значке Сеть и удаленный доступ к сети.
2. В открывшемся окне, содержащем значки всех настроенных в вашей системе сетевых подключений, выделите значок подключения к локальной сети, щелкните на нем правой кнопкой мыши и в появившемся меню выберите пункт Свойства.
3. В окне Подключение по локальной сети - свойства щелкните мышью на кнопке Установить, в открывшемся окне Выбор типа сетевого компонента дважды щелкните мышью на пункте Протокол и выберите в предложенном списке позицию NWLink IPX/SPX/NetBIOS - совместимый транспортный протокол или Протокол NetBEUI.

Как быстро настроить домашнюю локальную сеть?

Проще всего настраивать локальную сеть, состоящую из двух компьютеров, один из которых работает под управлением операционной системы Microsoft Windows XP или Millennium Edition, а на другом установлена ОС Window 9x. В данном случае достаточно создать на одном из компьютеров дискету автоматического конфигурирования сети и запустить Мастер настройки сети на другом компьютере, после чего перезагрузить обе машины.

Управление сетевым доступом к ресурсам компьютера

Если вы хотите, чтобы другие пользователи локальной сети могли обращаться к ресурсам вашего компьютера, таким как принтеры, диски, файлы и папки, вы должны открыть сетевой доступ к этим ресурсам и установить права пользователей для работы с каждым из них.

Настройка сетевого доступа к дискам

Вы можете открыть пользователям локальной сети доступ к дискам вашего компьютера, что позволит им просматривать, редактировать и сохранять файлы на этих дисках, создавать и удалять папки, прослушивать хранящиеся на вашем компьютере аудиозаписи, устанавливать с вашего винчестера различные программы. Совместное использование дисковых ресурсов может быть необходимо, например, в случае, если только ваш компьютер во всей сети оснащен приводом CD-ROM или DVD.

Чтобы открыть пользователям локальной сети доступ к дисковым ресурсам вашего компьютера, необходимо проделать следующее:

- откройте системное окно Мой компьютер;
- щелкните правой кнопкой мыши на изображении диска, к которому вы хотите открыть доступ по сети, и выберите в появившемся меню пункт Свойства;
- в открывшемся окне Свойства: локальный диск перейдите ко вкладке Доступ и выберите пункт Если вы хотите открыть доступ к корневой папке диска, щелкните здесь (для MS Windows XP), в другой операционной системе семейства Windows достаточно установить переключатель в положение Общий ресурс;
- в разделе Сетевой совместный доступ и безопасность установите флажок рядом с пунктом Открыть общий доступ к этой папке и введите в поле Общий ресурс сетевое имя своего диска — оно будет отображаться в папке Сетевое окружение других пользователей локальной сети (рис. 6.12);
- если вы хотите открыть пользователям сети полный доступ к своему диску, то есть разрешить им создавать, удалять, перемещать и переименовывать файловые объекты на вашем винчестере, установите флажок рядом с пунктом Разрешить изменение файлов по сети. Если флажок сброшен, пользователи смогут обращаться к диску в режиме «только чтение»;
- щелкните на кнопке OK, чтобы сохранить внесенные вами изменения. Диск, к которому открыт доступ из локальной сети, будет показан в папке Мой компьютер с помощью специальной метки в виде изображения открытой ладони.

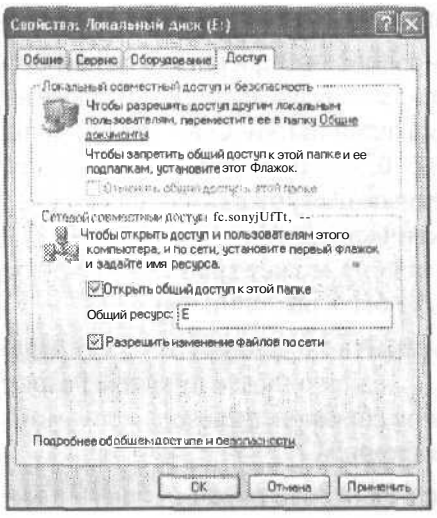


Рис. 6.12. Настройка общего доступа к локальному ресурсу

ПРИМЕЧАНИЕ

В целях безопасности не рекомендуется открывать доступ к диску или логическому дисковому разделу, на котором установлена Microsoft Windows. Кто-либо из пользователей локальной сети может случайно или намеренно внести изменения в системные файлы, в результате чего Windows придет в неработоспособное состояние.

Управление сетевым доступом к папкам

Открытие сетевого доступа к дискам и дисковым разделам является потенциально опасным для хранящихся на винчестере данных, поскольку пользователь локальной сети может случайно или намерено уничтожить, переименовать или изменить файлы, предназначенные только для вашего личного пользования. С точки зрения безопасности лучше открыть доступ не к диску в целом, а к одной дисковой директории, предназначенной для совместного использования в локальной сети. Вы можете назначить такой папке произвольное сетевое имя, например, аналогичное системному имени дискового раздела, благодаря чему пользователям будет казаться, что они работают непосредственно с диском вашего компьютера, в то время как доступ к каким-либо ресурсам за пределами данной директории будет для них закрыт.

Чтобы настроить сетевой доступ к какой-либо папке на жестком диске компьютера, необходимо проделать описанные ниже шаги.

- Перейдите на один из дисков своего компьютера и создайте папку с произвольным именем, которую вы хотите сделать доступной из локальной сети.
- Щелкните на значке папки правой кнопкой мыши и в появившемся меню выберите пункт Свойства.

а В открывшемся окне Свойства папки перейдите к вкладке Доступ.

❑ В разделе Сетевой совместный доступ и безопасность установите флажок рядом с пунктом Открыть общий доступ к этой папке и введите в поле Сетевой ресурс сетевое имя вашей папки. Оно может совпадать с именем вашего диска, например C, D, E или F, либо быть произвольным, например, Netfolder. Папка, сетевое имя которой совпадает с именем одного из дисковых разделов, фактически может находится на любом диске. Например, папка с сетевым именем C может храниться на диске D. Локальное и сетевое имя папки могут быть различными.

а Если вы хотите открыть пользователям сети полный доступ к данной папке, установите флажок рядом с пунктом Разрешить изменение файлов по сети. Если флажок сброшен, пользователи смогут обращаться к папке в режиме «только чтение».

а Щелкните на кнопке OK, чтобы сохранить внесенные вами изменения. Папка, к которой открыт сетевой доступ, будет отображаться в окне Проводника с помощью специальной метки в виде изображения открытой ладони.

Управление доступом к локальному принтеру

Вы можете открыть пользователям локальной сети доступ к принтеру, подключенному к вашему компьютеру, чтобы они могли печатать свои документы по сети. Для этого:

а перейдите в системную папку Принтеры и факсы, выполнив команды Пуск ▸ Панель управления ▸ Принтеры и другое оборудование ▸ Принтеры и факсы;

а щелкните на значке установленного в вашей системе принтера правой кнопкой мыши и выберите в появившемся меню пункт Свойства;

а перейдите к вкладке Доступ диалогового окна Свойства: Принтер, установите переключатель в положение Общий доступ к данному принтеру и введите в поле Сетевое имя произвольное сетевое имя принтера;

а щелкните на кнопке OK, чтобы сохранить внесенные изменения. Принтер, к которому открыт сетевой доступ, будет отображаться в окне Принтеры и факсы с помощью специальной метки в виде изображения открытой ладони.

Подключение сетевого принтера

Если принтер подключен не к вашему, а к другому компьютеру локальной сети, вы можете использовать его для распечатки своих документов. Для этого:

а перейдите в системную папку Принтеры и факсы, выполнив команды Пуск ▸ Панель управления ▸ Принтеры и другое оборудование ▸ Принтеры и факсы;

- щелкните на пункте Установка принтера в командном меню Задачи печати;
- в появившемся окне Мастера установки принтеров нажмите на кнопку Далее;
- в следующем окне Мастера установки принтеров выберите пункт Сетевой принтер, подключенный к другому компьютеру и снова нажмите Далее;
- в следующем окне установите переключатель в положение Обзор принтеров и щелкните на кнопке Далее;
- в предложенном списке принтеров, доступных в локальной сети, выберите нужный и снова нажмите Далее (рис. 6.13);

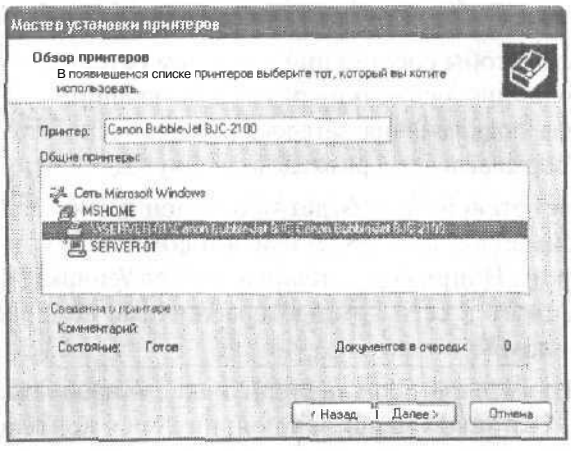


Рис. 6.13. Выбор сетевого принтера из списка

- если вы хотите сделать этот принтер используемым в вашей системе по умолчанию, установите в следующем окне переключатель в положение Да и щелкните на кнопке Далее;
- настройка сетевого принтера завершена. Нажмите на кнопку Готово, чтобы покинуть окно Мастера установки принтеров. Теперь все документы, распечатываемые вами из приложений Windows, будут направляться на этот принтер.

Подключение сетевого диска

Некоторые программы MS Windows, работающие с файловыми ресурсами других сетевых компьютеров (например, сетевая версия бухгалтерского пакета «1С») требуют, чтобы физический диск или дисковый раздел удаленного компьютера был подключен к вашей системе как сетевой диск. Сетевые диски отображаются в системном окне Мой компьютер наравне с вашими локальными дисками, вы можете обращаться к ним и работать с их содержимым так же, как с содержимым собственного винчестера. Для того чтобы подключить к системе сетевой диск, необходимо выполнить следующие операции:

- щелкните правой кнопкой мыши на расположенном на Рабочем столе Windows значке Мой компьютер и выберите в появившемся меню пункт Подключить сетевой диск. На экране появится окно одноименного Мастера подключения сетевого диска;
- выберите в меню Диск символ, которым будет обозначаться подключаемый к вашей системе сетевой диск, затем щелкните на расположенной рядом кнопке Обзор;
- в открывшемся окне Обзор папки выберите из списка доступный для совместного использования диск удаленного компьютера и нажмите кнопку OK.
- если вы хотите, чтобы соединение с данным сетевым диском автоматически восстанавливалось всякий раз при включении вашего компьютера, в окне Мастера подключения сетевого диска установите флажок рядом с функцией Восстанавливать при входе в систему. Щелкните на кнопке Готово.

Созданный вами сетевой диск будет обозначен в окне Мой компьютер выбранным вами символом и сетевым именем компьютера, которому фактически принадлежит. Например, сетевой диск E on Veronika (K:) является диском E подключенного к сети компьютера Veronika, но в вашей системе он обозначен символом K.

Чтобы отключить сетевой диск, щелкните на его изображении в окне Мой компьютер правой кнопкой мыши и в появившемся контекстном меню выберите пункт Отключить.

Работа в локальной сети

Для работы в локальной сети служит системная папка Сетевое окружение, в которой отображаются все доступные на текущий момент ресурсы локальной сети (рис. 6.14).

Вы можете работать с этими сетевыми ресурсами так же, как с файловыми объектами своего локального диска в программе Проводник, но с учетом ограничений, наложенных на использование данных сетевых ресурсов владельцами компьютеров или администратором локальной сети. Например, если какому-либо диску или папке удаленного компьютера присвоен режим доступа «только чтение», вы не сможете редактировать, перемещать, переименовывать, удалять и создавать расположенные на этом диске или в этой папке файлы и папки.

Если вы хотите увидеть список всех компьютеров, входящих в вашу рабочую группу, щелкните мышью на пункте Отобразить компьютеры рабочей группы в командной панели Сетевые задачи системного окна Сетевое окружение (рис. 6.15).

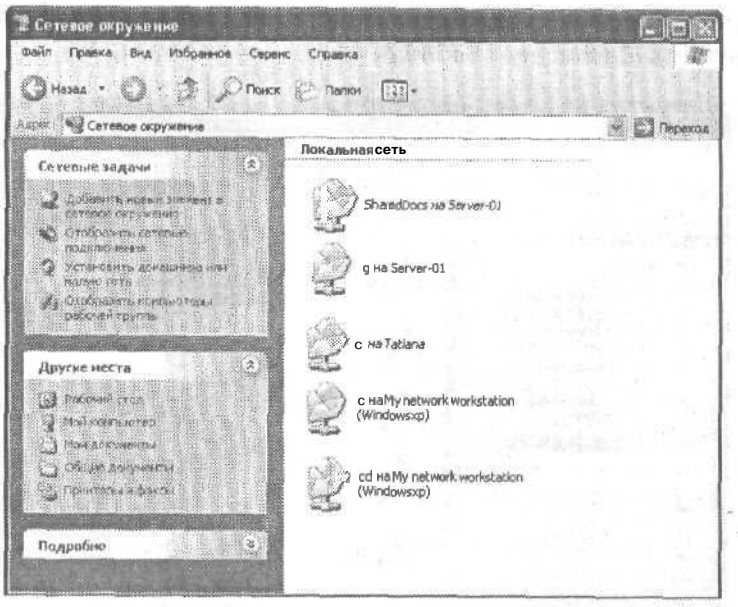


Рис. 6.14. Системная папка Сетевое окружение

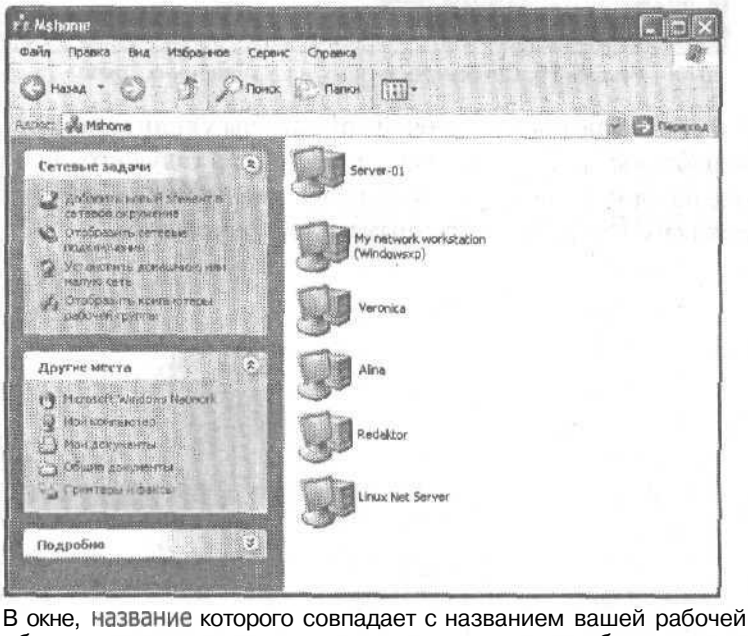


Рис. 6.15. В окне, название которого совпадает с названием вашей рабочей группы, отображаются все компьютеры, входящие в данную рабочую группу

Дважды щелкнув мышью на значке любого из удаленных компьютеров в данном окне, вы можете увидеть, какие его ресурсы доступны для использования в локальной сети.

Нажав в инструментальной панели данного окна кнопку UP («вверх»), можно просмотреть список всех рабочих групп в сети (рис. 6.16).

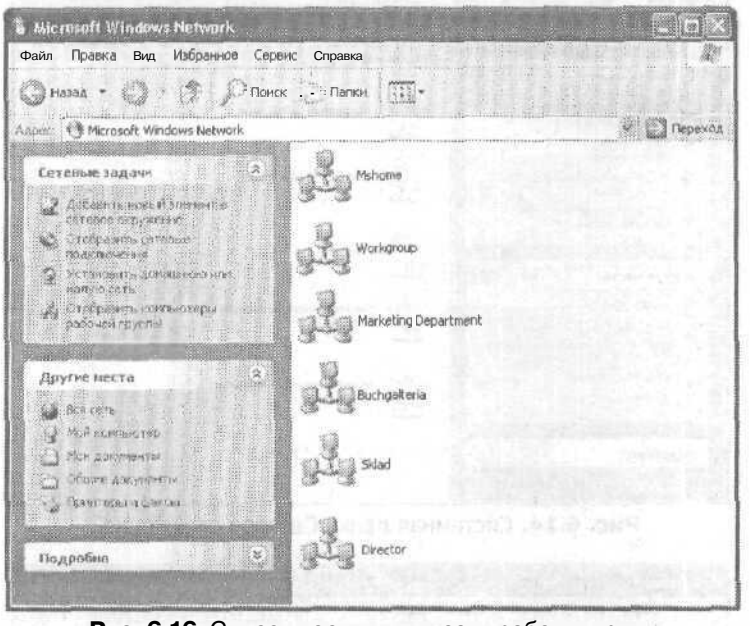


Рис. 6.16. Список доступных в сети рабочих групп

Дважды щелкнув на значке рабочей группы, вы увидите список входящих в данную рабочую группу компьютеров. Если из текущего окна вы поднимете сь еще на один уровень вверх, в окне Entire Network вам будет представлен список всех сервисов, доступных из локальной сети.

Глава 7

Совместное использование Интернета

- Настройка локальной сети для совместного использования Интернета
- Установка и настройка программы WinGate
- Установка и настройка программы WinRoute
- Настройка общего использования электронной почты в локальной сети

Одно из основных преимуществ локальной сети — это возможность совместного использования на всех сетевых компьютерах доступа в Интернет через один из узлов, который оснащен модемом либо подключен ко Всемирной Сети через высокоскоростное соединение, например, соединение ADSL или ISDN. Для этих целей используется специальное программное обеспечение, позволяющее после предварительной настройки обращаться к ресурсам Интернета через единственное подключение. Такие программы принято называть локальными прокси-серверами. В настоящее время существует достаточно широкий ассортимент таких программ, но мы рассмотрим только две наиболее распространенных из них: а именно, пакеты WinGate и WinRoute.

Программа WinGate

Программа Deerfield WinGate распространяется с сайта разработчика этого приложения (http://www.deerfield.com/products/wingate) в виде trial-версии, доступной для использования в течение тридцати дней с частичным ограничением ее функциональных возможностей. Возможна установка WinGate в двух вариантах: в серверной конфигурации — на компьютере, через который осуществляется подключение к Интернету (такой компьютер далее будет называться Gateway), и в клиентской — на всех остальных компьютерах локальной сети. Давайте подробно рассмотрим все этапы установки и настройки этого приложения.

Настройка локальной сети перед установкой WinGate

Корректная работа прокси-сервера Deerfield WinGate требует специальной настройки локальной сети и операционной системы на всех компьютерах, на которых планируется установить эту программу. Прежде всего, если вы используете на сетевых компьютерах операционную систему Microsoft Windows XP, перед началом инсталляции WinGate рекомендуется отключить в настройках соединения функции Общий доступ к Интернету и Брандмауэр подключения к Интернету. Для отключения брандмауэра перейдите в Главное меню Windows XP и откройте системную папку Сетевые подключения, выполнив последовательность команд Пуск ▸ Подключение ▸ Отобразить все подключения либо через Панель управления при помощи команд Пуск ▸ Панель управления ▸ Сеть и подключения к Интернету ▸ Сетевые подключения. Щелкните правой кнопкой мыши на значке используемого вами подключения к Интернету и выберите в открывшемся контекстном меню пункт Свойства. В открывшемся окне Подключение: Свойства перейдите ко вкладке Дополнительно и сбросьте флажок Защитить мое подключение к Интернету.

Механизм общего доступа к Интернету (Internet Connection Sharing, ICS) доступен во всех версиях Microsoft Windows XP Professional, но отсутствует в Microsoft Windows XP Home и 64-bit Edition. Чтобы отключить режим общего доступа к Интернету, перейдите в системное окно Сетевые подключения, воспользовавшись командами Пуск ▸ Панель управления ▸ Сеть и подключения к Интернету ▸ Сетевые подключения, щелкните правой кнопкой мыши на значке созданного соединения и в появившемся меню выберите пункт Свойства либо просто выберите пункт Изменение настроек подключения в меню Сетевые задачи. В открывшемся диалоговом окне Подключение: Свойства перейдите ко вкладке Дополнительно и обратитесь к разделу Общий доступ подключения к Интернету. Сбросьте флажок Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера, также сбросьте флажки Устанавливать вызов по требованию и Разрешить другим пользователям сети управление общим доступом подключения к Интернету.

Для нормальной работы программы WinGate необходимо, чтобы всем работающим в локальной сети компьютерам были назначены фиксированные IP-адреса определенного формата. Для того чтобы назначить IP-адреса вашим сетевым компьютерам, необходимо выполнить следующие действия.

1. Для Microsoft Windows XP:
   1) перейдите в папку Сетевые подключения, выполнив команды Пуск ▸ Подключение ▸ Отобразить все подключения или Пуск ▸ Панель управления ▸ Сеть и подключения к Интернету ▸ Сетевые подключения;

2) щелкните правой кнопкой мыши на значке вашего подключения к локальной сети и в появившемся контекстном меню выберите пункт Свойства;
3) в открывшемся окне Подключение по локальной сети: Свойства перейдите ко вкладке Общие;
4) выделите в списке пункт Протокол Интернета (TCP/IP) и нажмите на кнопку Свойства;
5) установите переключатель в положение Использовать следующий IP-адрес и введите в соответствующие поля требуемый IP-адрес и маску подсети.

2. Для Microsoft Windows 9x/ME:
1) откройте Панель управления и дважды щелкните мышью на значке Сеть;
2) в открывшемся окне Сеть перейдите ко вкладе Конфигурация;
3) в списке конфигурации сети выделите пункт TCP/IP для сетевого адаптера (не для Контроллера удаленного доступа) и щелкните мышью на кнопке Свойства;
4) на вкладке IP-адрес установите переключатель в положение Указать IP-адрес явным образом и введите в поля IP-адрес и Маска подсети требуемые значения.

Компьютер, имеющий непосредственное подключение к Интернету по модему или высокоскоростному каналу (Gateway), должен иметь статический IP-адрес 192.168.0.1 и маску подсети 255.255.255.0. Этот адрес не используется в современном Интернете и потому вы можете назначить его любому компьютеру вашей локальной сети, не опасаясь того, что он совпадет с IP-адресом какой-либо другой работающей во Всемирной Сети машины: даже если это случится, ничего страшного не произойдет. Все остальные компьютеры локальной сети должны иметь IP-адреса вида 192.168.0.*, где «*» — номера хостов начиная с 2, например, 192.168.0.2, 192.168.0.3, 192.168.0.4 и т. д. Все эти компьютеры должны использовать маску подсети 255.255.255.0, IP-адреса в пределах одной локальной сети не должны совпадать.

Функция Конфигурация WINS на всех компьютерах локальной сети, использующих WinGate, должна быть выключена, поле Шлюз должно быть пустым, в разделе Привязка следует оставить режим Клиент для сетей Microsoft.

Отдельной настройки требует раздел конфигурации DNS как на компьютере Gateway, так и на клиентских компьютерах. В операционных системах семейства Windows 9x/ME эти настройки доступны на вкладке Конфигурация DNS диалогового окна Свойства TCP/IP, чтобы открыть это окно, зайдите в Панель управления и дважды щелкните мышью на значке Сеть, затем в списке конфигурации сети выделите пункт TCP/IP для сетевого адаптера (не для Контроллера удаленного доступа) и щелкните мышью на кнопке Свойства.

В Windows XP добраться до этих настроек можно, щелкнув правой кнопкой мыши на значке вашего подключения к локальной сети в окне Сетевые подключения, в появившемся контекстном меню выбрав пункт Свойства и перейдя ко вкладке Общие. Доступ к настройкам WINS и дополнительным параметрам DNS открывается по щелчку на кнопке Дополнительно.

На компьютере Gateway требуется указать следующие настройки DNS.

1. Установите переключатель в положение Использовать следующие адреса DNS-серверов (для Windows XP) или Включить DNS (для Windows 9x/ME).
2. Введите в соответствующие поля IP-адреса DNS-серверов вашего провайдера — обычно они указаны в документации, поставляемой вместе с другими параметрами подключения к Интернету (в Windows 9x/ME эти адреса вводятся в поле Порядок просмотра серверов DNS, для указания нескольких адресов следует нажать кнопку Добавить).
3. Если в качестве Gateway используется компьютер, работающий под управлением Windows 9x/ME, в поле Имя компьютера следует ввести значение gateway, а в поле Домен — домен вашего провайдера, например, provider.net или provider.ru.

На клиентских компьютерах настройка DNS выглядит еще проще: в поле Предпочитаемый DNS-сервер (для Windows XP) или в поле Порядок просмотра серверов DNS (для Windows 9x/ME) должен стоять IP-адрес вашей Gateway-машины, то есть 192.168.0.1. Все остальные поля можно оставить пустыми. Перезагрузите компьютеры после внесения изменений в настройки протоколов.

Теперь необходимо проделать еще несколько дополнительных действий для обеспечения работоспособности системы. Откройте текстовый редактор Блокнот и введите в нем одну-единственную строку, не забыв нажать в конце этой строки клавишу Enter:

```
192.168.0.1 wingate
```

Сохраните этот файл на диск под именем hosts без расширения, затем скопируйте его в папку Windows на компьютерах, работающих под управлением Windows 9x/ME, или в папку %SYSTEMROOT%\sysyem32\drivers\etc\, где %SYSTEMROOT% — папка, в которой установлена ваша система (обычно — C:\Windows или C:\WINNT) в ОС семейства Windows XP/2000. Если файл с таким именем уже существует, замените его.

Финальный шаг. На всех клиентских компьютерах откройте окно настройки Microsoft Internet Explorer, для чего необходимо щелкнуть правой кнопкой мыши на значке этого браузера, расположенном на Рабочем столе, либо двойным щелчком мыши на значке Свойства обозревателя в Панели управления и выбрать в появившемся контекстном меню пункт Свойства. Перейдите ко вкладке Подключения и щелкните на кнопку Настройка LAN или Настройка

сети (в зависимости от версии браузера). Установите флажок Использовать прокси-сервер, введите в поле Адрес значение 192.168.0.1, а в поле Порт - значение 80. Если после установки WinGate доступ к Интернету на этих компьютерах будет невозможен, попробуйте указать порты 8080 или 3128.

Можно приступать к установке WinGate.

Установка WinGate

Программа WinGate устанавливается аналогично всем прочим приложениям Microsoft Windows. Следует помнить, что при установке WinGate на компьютерах, работающих под управлением операционной системы Windows NT 4, на ней должен быть предварительно установлен Service Pack 4, в Windows 95 требуется наличие WinSocks 2.

Если до установки WinGate на вашем компьютере работал другой прокси-сервер, например WinRoute или Microsoft Proxy, эти программы лучше предварительно удалить, воспользовавшись функцией Установка и удаление программ в Панели управления Windows.

После запуска программы установки WinGate проверит конфигурации сети и предложит вам выбрать режим инсталляции (рис. 7.1). На компьютере Gateway необходимо установить переключатель в положение Configure this computer as a WinGate server, на всех клиентских компьютерах программу следует устанавливать в режиме Configure this computer as a WinGate Internet Client.

Рис. 7.1. выбор режима установки программы WinGate

В следующем окне вам будет предложено ввести ключ для использования полнофункциональной версии WinGate. Если вы не имеете такого ключа, установите переключатель в позицию Evaluation version — на вашем компьютере будет установлена trial-версия программы с ограничением на срок ее

использования в 30 дней. Щелкните мышью на кнопке Next. Далее вы сможете выбрать папку для размещения файлов WinGate, а также указать режим установки — рекомендуемым режимом является Express Setup.

Если на Gateway-компьютере вы используете операционную систему Microsoft Windows NT4/2000/XP Professional, в следующем окне, появляющемся по нажатию на кнопку Next, вы сможете активизировать функцию доступа к настройкам WinGate с помощью используемых вами по умолчанию для входа в систему логина и пароля. Для этого следует установить флажок Use NT for Users Authentication. Данная функция, к сожалению, не работает в Windows XP Home Edition. Снова нажмите Next.

Программа WinGate начиная с версии 5 имеет встроенный почтовый сервер, позволяющий пересылать сообщения электронной почты по локальной сети без использования других программ. Для включения этой функции установите флажок Use WinGate mail server и введите в поле Default Domain название домена почтового сервера, при помощи которого WinGate будет идентифицировать себя при обмене сообщениями с другими почтовыми серверами сети Интернет. Снова нажмите Next.

Помимо встроенного почтового сервера WinGate версии 5 и выше содержит специальную утилиту Extended Network Support (ENS), которая дополняет протокол NAT (Network Address Translation), что дает возможность использовать в локальной сети клиентские компьютеры, работающие под управлением отличных от Windows операционных систем и позволяет пользователям взаимодействовать с устройствами на компьютерах, работающих в разных подсетях. Если вы настраиваете WinGate в малой корпоративной или домашней локальной сети, на всех машинах которой установлены любые версии Windows, и желаете использовать стандартный протокол NAT производства Microsoft (который не требует отдельной настройки), сбросьте флажок Install ENS и нажмите на кнопку Next. Если вы не планируете устанавливать ENS, вам также не удастся установить необязательный компонент VPN (Virtual Private Network), позволяющий соединять через Интернет несколько удаленных друг от друга подсетей в одну локальную сеть. Следует учесть, что в ОС Windows XP Professional уже имеется полнофункциональная поддержка VPN.

После нажатия на кнопку Next вам будет предложено установить компонент AutoUpdate, который через определенные промежутки времени будет автоматически соединяться с сервером разработчика программы и загружать на ваш компьютер обновления для WinGate. Если вы не планируете использовать эту функцию, сбросьте флажок Enable AutoUpdate и щелкните мышью на кнопке Begin. Программа установки начнет процедуру инсталляции WinGate на вашем компьютере. По завершении этого процесса перезагрузите операционную систему.

На всех клиентских компьютерах WinGate должен быть установлен в конфигурации Configure this computer as a WinGate Internet Client, которую следует выбрать на начальном этапе процедуры установки программы.

Настройка WinGate

После своего запуска программа WinGate начинает работать в фоновом режиме: о том, что она загружена, свидетельствует значок приложения, отображающийся рядом с системными часами в Области уведомлений Windows. Для того чтобы изменить настройки программы, вам необходимо перейти в режим администрирования WinGate, дважды щелкнув мышью на этом значке. На экране появится окно Online Options (рис. 7.2).

Рис. 7.2. Окно Online Options программы WinGate

Щелкните мышью на кнопке OK. Поскольку вы запустили программу без пароля, в следующем окне вам будет предложено указать пароль администратора. Дважды введите его в поля New Password и Confirm New Password. На экране появится окно программы GateKeeper, с помощью которой вы сможете выполнять мониторинг и администрирование вашего прокси-сервера (рис. 7.3).

Окно программы GateKeeper вертикально разделено на две независимые области; в левой отображаются поддерживаемые программой сервисы, в правой — их компоненты. Помимо этого в левой области окна приложения имеется три вкладки: System — здесь демонстрируются все службы, поддерживаемые WinGate, Services — список всех сетевых сервисов, и Users — список пользователей и групп пользователей, которые могут работать с программой. Правая область окна программы также имеет четыре вкладки: Activity — список всех активных сессий при подключении к WinGate, Network — текущий мониторинг локальной сети, History — история обращений к прокси-серверу и наконец, Firewall — текущее состояние встроенного в WinGate брандмауэра.

По умолчанию сервисы WinGate имеют следующие базовые настройки:

- сервер POP3 — порт 110;
- сервер SMTP - порт 25;

- сервер FTP Proxy — порт 21;
- сервер POP3 Proxy — порт 8110;
- сервер Telnet Proxy — порт 23;
- сервер HTTP Proxy — порт 80.

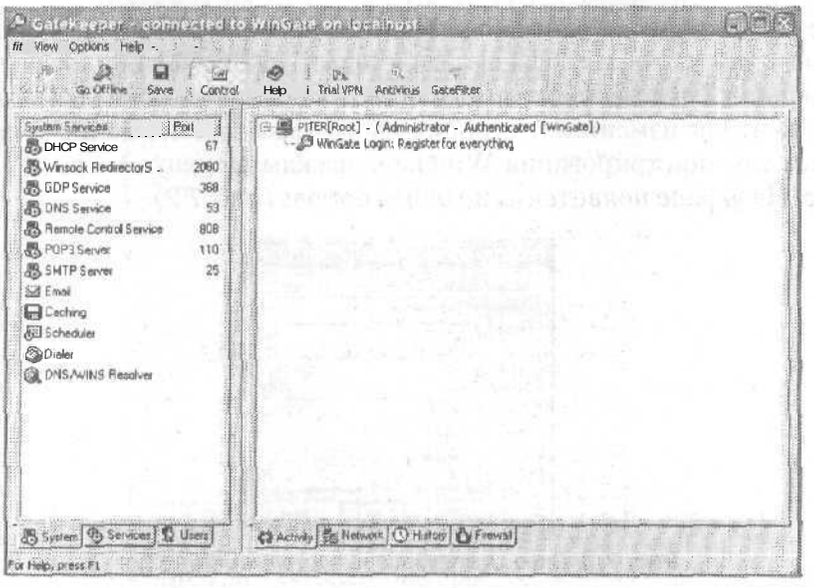


Рис. 7.3. Интерфейс программы GateKeeper

Перемещаясь между вкладками и выбирая двойным щелчком мыши любой из сервисов WinGate, вы можете изменять произвольным образом его настройки.

Как настроить общий доступ к электронной почте в сети WinGate

В составе программы WinGate начиная с версии 5 имеется встроенный почтовый сервер, который позволяет пользователям принимать и отправлять сообщения **электронной** почты на своих компьютерах, подключенных к локальной сети, используя единственное подключение к Интернету. В данном случае вся система работает следующим образом: каждый пользователь локальной сети имеет собственную учетную запись электронной почты в Интернете (электронный почтовый ящик), обращение к которому осуществляется через Gateway-компьютер, использующий непосредственное подключение к сети Интернет. Сообщения из почтовых ящиков пользователей загружаются на этот компьютер и впоследствии автоматически пересылаются пользователям сети при помощи программы WinGate. Для отправки исходящей почты в настройках WinGate можно указать любой доступный сервер SMTP.

Для того чтобы изменить настройки локального почтового сервера на Gateway-машине откройте GateKeeper и дважды щелкните мышью на значке Email в левой части рабочего окна программы, открытого на вкладке System. На экране появится диалоговое окно Mail Server (рис. 7.4).

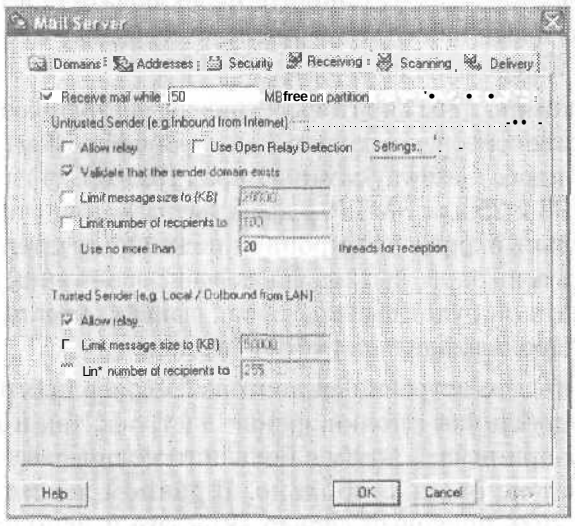


Рис. 7.4. Настройка локального почтового сервера

Прежде всего следует обратить внимание на обозначение домена почтового сервера по умолчанию, которое демонстрируется в списке на вкладке Domains. Домен, указанный в этом списке, служит для идентификации почтового сервера, с которым будет работать WinGate. Если, например, все почтовые ящики пользователей расположены в одном корпоративном домене и выглядят, скажем, следующим образом: boss@mycompany.ru, alexander@mycompany.ru,maria@mycompany.ruит.д,товспискедолженбыть указан домен mycompany.ru. Если почтовые ящики пользователей расположены в нескольких доменах, их следует указать в данном списке по порядку, нажав на кнопку Add. В меню Default Domain выберите домен, который будет использоваться в настройках программы по умолчанию. Перейдите ко вкладке Addresses и укажите адреса электронной почты всех пользователей вашей локальной сети: для этого следует ввести название учетной записи в поле Address, выбрать в списке Domain домен почтового сервера, с которого будет приниматься почта, а в меню Local user mailbox — локальный почтовый ящик программы WinGate, на который будут перенаправляться все входящие почтовые сообщения, поступившие на указанный вами адрес.

Для того чтобы указать настройки почтового сервера для исходящих сообщений, через который WinGate будет отправлять почту, перейдите ко вкладке Delivery. В меню How to deliver выберите пункт Use gateway, в поле Server

укажите адрес SMTP-сервера, в поле Port введите номер порта (по умолчанию — 25). Для настройки обращений к серверам POP3 необходимо перейти ко вкладке Services в рабочем окне GateKeeper и выбрать двойным щелчком мыши в предложенном списке пункт POP3 Proxy Server. Перейдите ко вкладке Non-Proxy Requests, установите переключатель в положение Pipe requests trough to predetermined server, после чего введите в соответствующие поля адрес POP3-сервера и номер порта.

На клиентских компьютерах почтовые клиенты настраиваются следующим образом: в качестве серверов исходящей и входящей почты (POP3 и SMTP) указывается IP-адрес Gateway-компьютера (192.168.0.1) с номерами портов 110 для POP3 и 25 для SMTP, в качестве названия учетной записи записывается реальный адрес электронной почты получателя с символом # вместо @, то есть если адрес выглядит как mail@myserver.ru, то в настройках почтового клиента он будет выглядеть как mail#myserver.ru. В качестве пароля вводится пароль владельца учетной записи.

Следует отметить, что встроенный почтовый сервер программы WinGate объективно неудобен как с точки зрения настроек, так и использования: он не позволяет принимать почту с большого количества удаленных серверов и работает не очень стабильно. В данном аспекте можно посоветовать отключить почтовый сервер WinGate и использовать отдельный локальный почтовый сервер, например, очень простую и надежную программу MDaemon (http://www.mdaemon.ru) или VisNetic MailServer (http://www.deerfield.com/products/visnetic_mailserver/).Альтернативным вариантом может служить встроенный почтовый сервер программы WinRoute, речь о которой пойдет далее в этой главе.

Блокировка доступа пользователей к определенным URL

В некоторых случаях возникает необходимость запретить пользователям локальной сети доступ к некоторым веб-сайтам, например, страницам непристойного содержания. В корпоративных локальных сетях это позволяет заметно увеличить антивирусную защиту сетевых компьютеров, в домашней сети нередко требуется оградить ребенка от получения ненужной информации. С этой задачей прекрасно справляется прокси-сервер WinGate. Итак, для того чтобы заблокировать доступ сетевых компьютеров к сайтам с заданными адресами, проделайте следующие действия:

1. Войдите в программу GateKeeper.
2. Перейдите ко вкладке Services.
3. Двойным щелчком мыши выберите пункт WWW proxy services.
4. В открывшемся диалоговом окне WWW proxy services properties перейдите ко вкладке Policies.

5. В меню Default rights (System policies) выберите пункт Are ignored
6. Щелкните мышью на кнопке Add, в открывшемся окне перейдите ко вкладке Ban List.
7. Установите флажок Enable ban list и щелкните мышью на кнопке Add.
8. Если вы хотите ограничить доступ к строго определенным адресам, установите переключатель в положение This criterion is met if выберите в левом меню пункт HTTP URL, в среднем — contains, а в расположенном справа поле введите требуемый URL, после чего щелкните мышью на кнопке OK. Повторите процедуру для всех требуемых адресов.
9. Если вы хотите запретить доступ к ресурсам, в URL которых присутствуют заданные слова или словосочетания, перейдите ко вкладке Advanced, установите переключатель в положение Specify which requests this recipient has rights for и щелкните мышью на кнопке Add filter. Выделите в появившемся списке пункт Filter1 и щелкните мышью на кнопке Add Criterion. В открывшемся диалоговом окне установите переключатель в позицию This criterion is NOT met if, выберите в левом меню пункт HTTP URL, в среднем — contains, а в расположенном справа поле введите слова и словосочетания, при наличие которых в URL сайта доступ к такому сайту будет заблокирован, например, xxx, porn, sex и т. д.
10. Указанные выше изменения необходимо продублировать в настройках SOCKS Proxy server. Для этого на вкладке Services программы GateKeeper выберите пункт SOCKS Proxy server и перейдите ко вкладке SOCKS Advanced.
11. Установите переключатель в положение Use following policy и в расположенном ниже меню выберите пункт WWW Proxy server.
12. Щелкните мышью на кнопке OK.

Блокировка возможности загрузки файлов из Интернета

При подключении к Интернету провайдер нередко накладывает жесткие ограничения на входящий трафик, нарушение которых приводит к необходимости производить отдельную доплату за каждый загруженный через провайдерский узел мегабайт. К тому же, передача загружаемых из Интернета по локальной сети больших файловых массивов заметно снижает скорость соединения для пользователей и замедляет работу сети в целом. С целью избежать подобных неприятностей многие системные администраторы блокируют для своих пользователей возможность загрузки файлов из Всемирной сети. Для этого проделайте следующее.

1. Войдите в программу GateKeeper.
2. Перейдите ко вкладке Services.
3. Двойным щелчком мыши выберите пункт WWW proxy services.

4. В открывшемся диалоговом окне WWW proxy services properties перейдите ко вкладке Policies.
5. В меню Default rights (System policies) выберите пункт Are ignored.
6. Установите переключатель в позицию Specify Users or group.
7. Щелкните мышью на кнопке Add, в открывшемся окне перейдите ко вкладке Ban List.
8. Установите флажок Enable ban list и щелкните мышью на кнопке Add.
9. Если вы хотите ограничить доступ к строго определенным адресам, установите переключатель в положение This criterion is met if выберите в левом меню пункт HTTP URL, в среднем — contains, а в расположенном справа поле введите требуемое значение FTP. При таких настройках будет запрещена загрузка файлов из браузера.
10. Если вы хотите запретить передачу на клиентские компьютеры файлов по протоколу FTP, перейдите ко вкладке Advanced, установите переключатель в положение Specify which requests this recipient has rights for и щелкните мышью на кнопке Add filter. Выделите в появившемся списке пункт Filter1 и щелкните мышью на кнопке Add Criterion. В открывшемся диалоговом окне установите переключатель в позицию This criterion is NOT met if, выберите в левом меню пункт HTTP Protocol, в среднем - equals, а в расположенном справа поле введите значение FTP.
11. Щелкните мышью на кнопке OK.

Программа WinRoute

Многим администраторам локальных сетей, особенно тем, кто только начинает осваивать принципы построения и использования подобных систем, программа WinGate вполне обоснованно кажется достаточно громоздкой и сложной в настройках. Именно поэтому начинающим системным администраторам можно посоветовать использовать в небольших локальных сетях более простой и удобный прокси-сервер WinRoute (http://www.kerio.com). Так же, как и программа WinGate, WinRoute имеет встроенный почтовый сервер и позволяет ограничивать доступ пользователей к ресурсам Интернета. Однако эта утилита, во-первых, имеет русскую локализацию с русской же справкой (версия 4.2), которую можно скачать с сайта http://www.kerio.com/wrp_download.html, и во-вторых, она занимает значительно меньше места на диске.

Настройка локальной сети перед установкой WinRoute

Как и в случае с WinGate, перед установкой WinRoute необходимо специальным образом изменить конфигурацию локальной сети и операционной

системы на всех компьютерах, на которых планируется установить эту программу. Прежде всего, если вы используете на сетевых компьютерах операционную систему Microsoft Windows XP, перед началом инсталляции WinRoute рекомендуется отключить в настройках соединения функции Общий доступ к Интернету и Брандмауэр подключения к Интернегу. Для этого перейдите в Главное меню Windows XP и откройте системную папку Сетевые подключения, выполнив последовательность команд Пуск ▸ Подключение ▸ Отобразить все подключения либо через Панель управления при помощи команд Пуск ▸ Панель управления ▸ Сеть и подключения к Интернету ▸ Сетевые подключения. Щелкните правой кнопкой мыши на значке используемого вами подключения к Интернету и выберите в открывшемся контекстном меню пункт Свойства. В открывшемся окне Подключение: Свойства перейдите ко вкладке Дополнительно и сбросьте флажок Защитить мое подключение к Интернету.

Механизм общего доступа к Интернету (Internet Connection Sharing, ICS), есть во всех версиях Microsoft Windows XP Professional, по отсутствует в Microsoft Windows XP Home и 64-bit Edition. Чтобы отключить режим общего доступа к Интернету, перейдите в системное окно Сетевые подключения, воспользовавшись командами Пуск ▸ Панель управления > Сеть и подключения к Интернету V Сетевые подключения, щелкните правой кнопкой мыши на значке созданного соединения и в появившемся меню выберите пункт Свойства либо просто выберите пункт Изменение настроек подключения в меню Сетевые задачи. В открывшемся диалоговом окне Подключение: Свойства перейдите ко вкладке Дополнительно и обратитесь к разделу Общий доступ подключения к Интернету. Сбросьте флажок Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера, также сбросьте флажки Устанавливать вызов по требованию и Разрешить другим пользователям сети управление общим доступом подключения к Интернету.

Для нормальной работы программы WinRoute необходимо, чтобы всем работающим в локальной сети компьютерам были назначены фиксированные IP-адреса определенного формата. Для того чтобы назначить IP-адреса вашим сетевым компьютерам, необходимо выполнить следующие действия.

1. Для Microsoft Windows XP:
   1) перейдите в папку Сетевые подключения, выполнив команды Пуск ▸ Подключение ▸ Отобразить все подключения или Пуск ▸ Панель управления ▸ Сеть и подключения к Интернету ▸ Сетевые подключения;
   2) щелкните правой кнопкой мыши на значке вашего подключения к локальной сети и в появившемся контекстном меню выберите пункт Свойства;
   3) в открывшемся окне Подключение по локальной сети: Свойства перейдите ко вкладке Общие;
   4) выделите в списке пункт Протокол Интернета (TCP/IP) и нажмите на кнопку Свойства;

5) установите переключатель в положение Использовать следующий IP-адрес и введите в соответствующие поля требуемый IP-адрес и маску подсети.

2. Для Microsoft Windows 9x/ME:
   1) откройте Панель управления и дважды щелкните мышью на значке Сеть;
   2) в открывшемся окне Сеть перейдите ко вкладе Конфигурация;
   3) в списке конфигурации сети выделите пункт TCP/IP для сетевого адаптера (не для Контроллера удаленного доступа) и щелкните мышью на кнопке Свойства;
   4) на вкладке IP-адрес установите переключатель в положение Указать IP-адрес явным образом и введите в поля IP-адрес и Маска подсети требуемые значения.

Компьютер, имеющий непосредственное подключение к Интернету по модему или высокоскоростному каналу (Gateway), должен иметь статический IP-адрес 192.168.11.1 и маску подсети 255.255.255.0. Все остальные компьютеры локальной сети должны иметь IP-адреса вида 192.168.11.*, где «*» — номера хостов начиная с 2, например, 192.168.11.2, 192.168.11.3, 192.168.11.4 и т. д. Все эти компьютеры должны использовать маску подсети 255.255.255.0, IP-адреса в пределах одной локальной сети не должны совпадать.

Другие настройки протокола TCP/IP для локальной сети на серверном компьютере (Gateway) должны иметь следующую конфигурацию.

1. WINS — отключено.
2. IP-адрес шлюза — отсутствует.
3. Привязка — Клиент для сетей Microsoft.

В Windows XP добраться до этих настроек можно, щелкнув правой кнопкой мыши на значке вашего подключения к локальной сети в окне Сетевые подключения, в появившемся контекстном меню выбрав пункт Свойства и перейдя ко вкладке Общие. Доступ к настройкам WINS и дополнительным параметрам DNS открывается по щелчку на кнопке Дополнительно.

На компьютере Gateway для настройки DNS выполните следующие действия.

1. Установите переключатель в положение Использовать следующие адреса DNS-серверов (для Windows XP) или Включить DNS (для Windows 9x/ME).
2. Введите в соответствующие поля IP-адреса DNS-серверов вашего провайдера — обычно они указаны в документации, поставляемой вместе с другими параметрами подключения к Интернету (в Windows 9x/ME эти адреса вводятся в поле Порядок просмотра серверов DNS, для указания нескольких адресов следует нажать кнопку Добавить).
3. Если в качестве Gateway используется компьютер, работающий под управлением Windows 9x/ME, в поле Имя компьютера следует ввести значение gateway, а в поле Домен — домен вашего провайдера, например, provider.net или provider.ru.

На клиентских компьютерах настройка DNS выглядит еще проще: в поле Предпочитаемый DNS-сервер (для Windows XP) или в поле Порядок просмотра серверов DNS (для Windows 9x/ME) должен стоять IP-адрес вашей Gateway-машины, то есть 192.168.11.1. Все остальные поля можно оставить пустыми. Другие настройки протокола TCP/IP на клиентских машинах выглядят следующим образом,

1. WINS — отключено.
2. IP-адрес шлюза — 192.168.11.1.
3. Привязка — Клиент для сетей Microsoft.

Перезагрузите компьютеры после внесения изменений в настройки протоколов.

Последнее, что еще следует сделать, это на всех клиентских компьютерах открыть окно настройки Microsoft Internet Explorer, для чего необходимо щелкнуть правой кнопкой мыши на значке этого браузера, расположенном на Рабочем столе, и выбрать в появившемся контекстном меню пункт Свойства, либо дважды щелкнуть мышью на значке Свойства обозревателя в Панели управления. Перейдите ко вкладке Подключения и щелкните на кнопке Настройка LAN или Настройка сети (в зависимости от версии браузера). Установите флажок Использовать прокси-сервер, введите в поле Адрес значение 192.168.11.1, а в поле Порт — значение 3128. Если после установки WinRoute доступ к Интернету на этих компьютерах будет невозможен, попробуйте указать порты 8080 или 80.

Можно приступать к установке WinRoute.

Установка WinRoute

Запустите на исполнение файл программы установки прокси-сервера WinRoute. В первом окне выберите папку, в которую вы планируете установить программу, и щелкните мышью на кнопке Install. В процессе установки вам будет продемонстрировано окно Initial Configuration, в котором вам следует установить переключатель в положение, соответствующее способу подключения вашего компьютера к Интернету: Dial-Up connection для соединения по модему или каналу ISDN либо Network adapter для подключения по ASDL или через кабельный модем. Щелкните мышью на кнопке OK и согласитесь с предложением перезагрузить компьютер. Установки программы WinRoute на клиентских компьютерах локальной сети не требуется.

Настройка WinRoute

После своего запуска программа WinRoute начинает работать в фоновом режиме: о том, что она загружена, свидетельствует значок приложения, отображающийся рядом с системными часами в Области уведомлений Windows.

Для того чтобы изменить настройки программы, вам необходимо дважды щелкнуть мышью на этом значке. Сразу вслед за этим на экране появится окно Открыть конфигурацию (рис. 7.5). Введите в поле Имя пользователя произвольное название учетной записи, поле Пароль оставьте пустым, после чего щелкните мышью на кнопке OK.

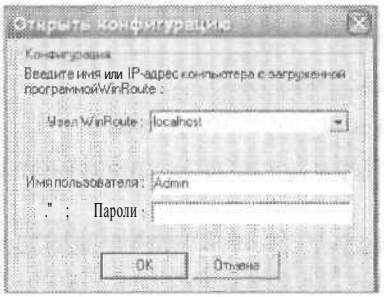


Рис. 7.5. Диалоговое окно Открыть конфигурацию

На экране откроется окно программы WinRoute. Назначение кнопок инструментальной панели этого приложения показано на рис. 7.6.

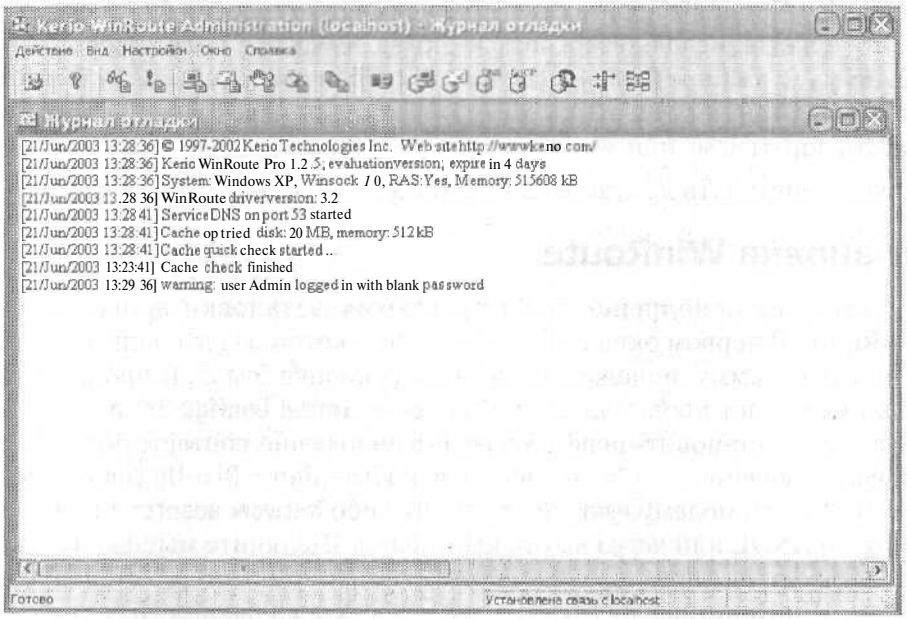


Рис. 7.6. Назначение кнопок инструментальной панели программы WinRoute

- Вывести на экран диалоговое окно Открыть конфигурацию.
- Вывести на экран справку.
- Отобразить журнал отладки.

 - Отобразить журнал ошибок.

 — Отобразить журнал HTTP.

 — Отобразить почтовый журнал.

 — Отобразить журнал протокола безопасности.

 — Отобразить журнал звонков.

 — Показать архив журналов.

 — Продемонстрировать таблицу интерфейсов.

 — Открыть окно настроек прокси-сервера.

dp — Открыть окно настроек почтового сервера.

 _ Открыть окно настроек транслятора DNS.

 - Открыть окно настроек сервера DHSP.

 -- Продемонстрировать список учетных записей всех пользователей программы.

 - Отобразить окно настроек пакетного фильтра.

 - Открыть окно настройки распределения портов.

Для того чтобы приступить к работе с программой WinRoute, достаточно внести в ее конфигурацию минимальные настройки: щелкните мышью на кнопке  и установите флажок Включить прокси-сервер на вкладке Общие настройки. Программа готова к работе.

Настройка доступа к электронной почте в сети WinRoute

Локальный почтовый сервер WinRoute фактически работает аналогично серверу WinGate, однако он заметно проще в настройках и не требует лишних усилий для изменения своей конфигурации. Итак, чтобы настроить почтовый сервер WinRoute, следуйте приведенным ниже инструкциям.

1. Щелкните мышью на кнопке  .
2. На вкладке Общие настройки диалогового окна Настройки почтового сервера (рис. 7.7) установите флажок Включить почтовый сервер.
3. В поле Сервер-ретранслятор SMTP введите адрес SMTP-сервера, через который вы будете отправлять сообщения электронной почты.
4. Если вы используете единственный почтовый ящик для приема всех входящих сообщений электронной почты, вы можете указать домен

вашего почтового сервера в настройках WinRoute. Для этого установите флажок У меня есть Интернет-домен, и введите соответствующие значения через точку с запятой в поле Локальный(е) домен(ы). В этом случае письма будут рассортировываться пользователям локальной сети согласно значению поля Кому (To:) электронного письма. Флажок Использовать ETRN-команду при такой конфигурации должен быть сброшен.

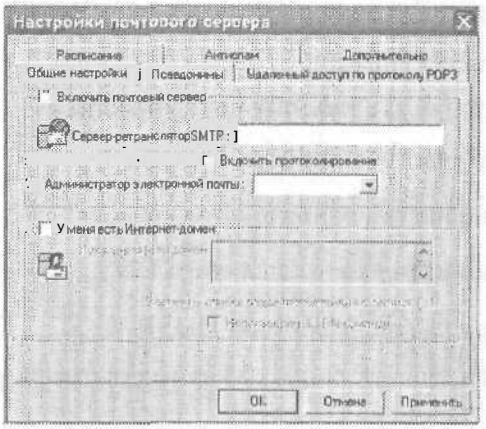


Рис. 7.7. Диалоговое окно Настройки почтового сервера

5. Для каждого пользователя локальной сети, подключаемого к Интернету при помощи программы WinRoute, должна быть создана собственная учетная запись. Для того чтобы создать учетные записи пользователей, откройте окно программы WinRoute Administration и выполните в нем последовательность команд Настройки ▸ Учетные записи. В появившемся окне Учетные записи пользователей нажмите на кнопку Добавить. На экране появится окно Ввод (рис. 7.8). Введите соответствующие значения в поля Имя пользователя, Пароль и Подтвердить, после чего, установив переключатель в положение Нет доступа к средствам администрирования, щелкните мышью на кнопке OK. Повторите эту процедуру для каждой учетной записи пользователей локальной сети. В этом случае конфигурация почтовых клиентов на других машинах будет такой:
   - адрес POP3 сервера - 192.168.11.1, порт НО;
   - адрес SMTP сервера — 192.168.11.1, порт 25;
   - учетная запись — соответствует указанной вами в поле Имя пользователя окна Ввод;
   - пароль — соответствует указанному вами в поле Пароль окна Ввод.
6. Для настройки доступа пользователей сети к своим почтовым ящикам в Интернете по протоколу POP3, перейдите на вкладку Удаленный доступ по протоколу POP3 окна Настройки почтового сервера и нажмите на кнопку Добавить. На экране появится диалоговое окно Ввод (рис. 7.9).

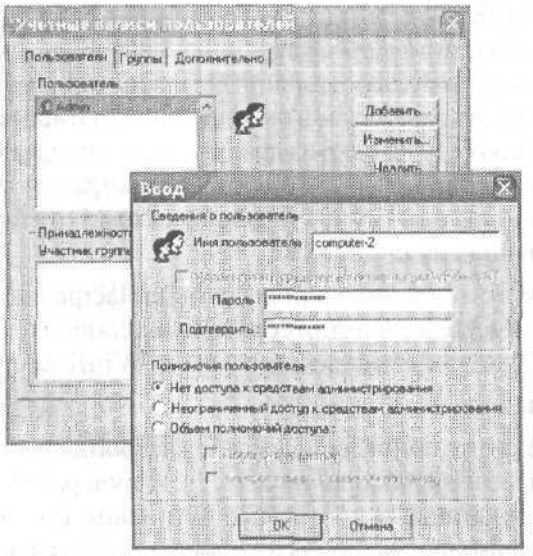


Рис. 7.8. Настройка учетных записей пользователей

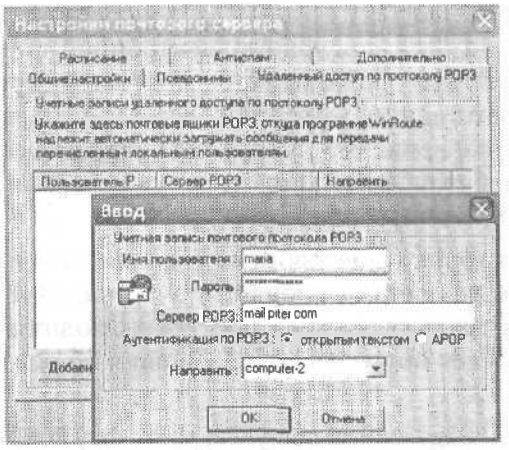


Рис. 7.9. Настройка доступа к серверу POP3

7. Введите в поле Имя пользователя учетную запись, соответствующую учетной записи пользователя на почтовом сервере (так, как она указывается в настройках почтового клиента). В поле Пароль введите пароль для доступа к почтовому серверу. В поле Сервер POP3 укажите адрес сервера входящей почты, установите переключатель в положение Аутентификация по POP3 и выберите в меню Направить наименование учетной записи пользователя WinRoute, которому адресована почта.
8. Можно включить режим сортировки входящих сообщений согласно значению поля Кому (To:) письма. Для этого щелкните мышью на кнопке Правила сортировки, затем на кнопке Добавить, в открывшемся окне Ввод

наберите в поле Если поле заголовка сообщения Кому содержит требуемое значение поля, например user@mail.ru, а в меню Направить выберите учетную запись пользователя локальной сети. Повторите эту процедуру требуемое количество раз. Затем в окне Правила сортировки сообщений POP3 выберите в меню Если ни одно из правил не подходит, направить сообщение название учетной записи, на которую будут направляться все сообщения, не отвечающие ни одному из указанных вами критериев сортировки. Щелкните мышью на кнопке OK.

9. Перейдите на вкладку Дополнительно окна Настройки почтового сервера и проверьте номера портов для серверов входящей и исходящей почты, с которыми будет соединяться программа WinRoute.
10. Щелкните мышью на кнопке OK.

Давайте рассмотрим все приведенные выше настройки на простых примерах. Предположим, мы имеем локальную сеть, в которой работают три пользователя, зарегистрированные в программе WinRoute с учетными записями valentin, maria и administrator. Каждый из этих пользователей имеет собственный почтовый ящик у провайдера: у пользователя valentin — valentin_1@server.ru, у пользователя maria — marta@free-e-mail.com, у пользователя administrator — postmaster@server.ru. Для получения электронной почты пользователей valentin и administrator используется почтовый сервер mail.server.ru с логинами, соответственно, valentin_1 и postmaster, пользователь maria получает почту с сервера POP3.free-e-mail.com, подключаясь к серверу с использованием логина marta. Для отправки исходящих сообщений применяется сервер SMTP.server.ru.

Откроем окно Настройки почтового сервера на вкладке Общие настройки и введем в поле Сервер-ретранслятор SMTP значение SMTP.server.ru, в меню Администратор электронной почты выберем любого пользователя, например — administrator, он будет получать все сообщения об ошибках при доставке сообщений.

Перейдем ко вкладке Удаленный доступ по протоколу POP3 окна Настройки почтового сервера и нажмем на кнопку Добавить. Введем следующие настройки для пользователя valentin:

- Имя пользователя: valentin_1 (это имя должно соответствовать учетной записи, требуемой для входа на сервер mail.server.ru);
- Пароль: пароль пользователя valentin для доступа к почтовому ящику valentin_1@server.ru;
- установим переключатель в положение Аутентификация по POP3;
- в поле Сервер POP3 введем mail.server.ru;
- в меню Направить выберем пользователя valentin;
- щелкнем мышью на кнопке OK.

Снова нажмем кнопку Добавить в окне Настройки почтового сервера и настроим учетную запись для пользователя administrator:

- Имя пользователя: postmaster (это имя должно соответствовать учетной записи, требуемой для входа на сервер mail.server.ru);
- Пароль: пароль пользователя administrator для доступа к почтовому ящику postmaster@server.ru;
- установим переключатель в положение Аутентификация по POP3;
- в поле Сервер POP3 введем mail.server.ru;
- в меню Направить выберем пользователя administrator;
- щелкнем мышью па кнопке OK.

Еще раз нажмем кнопку Добавить и настроим учетную запись для пользователя maria:

- Имя пользователя: marta (это имя должно соответствовать учетной записи, требуемой для входа на сервер POP3.free-e-mail.com);
- Пароль: пароль пользователя maria для доступа к почтовому ящику marta@free-e-mail.com;
- установим переключатель в положение Аутентификация по POP3;
- в поле Сервер POP3 введем POP3.free-e-mail.com;
- в меню Направить выберем пользователя maria;
- щелкнем мышью на кнопке OK.

После проведения данных процедур вкладка Удаленный доступ по протоколу POP3 окна Настройки почтового сервера будет выглядеть так, как показано на рис. 7.10.

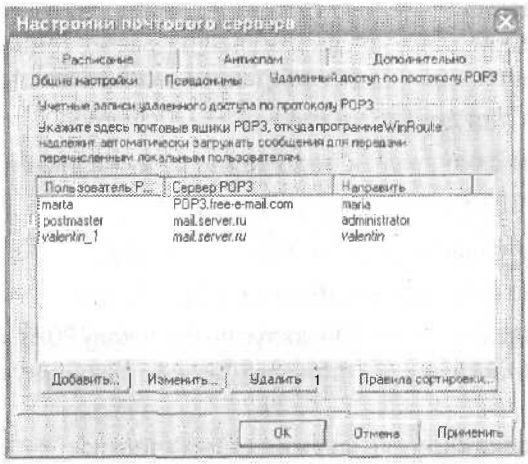


Рис. 7.10. Пример настроек почтового сервера в программе WinRoute

Теперь давайте рассмотрим другое решение, немного изменив начальные условия. У нас по-прежнему имеется три пользователя локальной сети,

зарегистрированные в WinRoute: valentin, maria и administrator. Для получения электронной почты мы используем единый для всех пользователей сервер mail.server.ru, для отправки — сервер smtp.server.ru, оба эти сервера работают в зоне нашего собственного корпоративного домена server.ru. Пользователь valentin имеет почтовый ящик valentin@server.ru, пользователь maria — maria@server.ru и, наконец, пользователь administrator - administrator@server.ru. В дополнение к этому у нас имеется два почтовых ящика: info@server.ru, почту с которого должен получать valentin, и webmaster@server.ru, сообщения с которого перенаправляются пользователю maria. Сообщения для всех этих учетных записей хранятся на сервере в общей папке mail, для доступа к ней используется логин mail.server. Наличие общей серверной папки для временного хранения всех сообщений, поступающих на почтовые адреса нашего домена, здесь — обязательное условие. Рассмотрим процедуру настройки WinRoute для такой ситуации.

Откроем окно Настройки почтового сервера на вкладке Общие настройки и введем в поле Сервер-ретранслятор SMTP значение smtp.server.ru, в меню Администратор электронной почты выберем любого пользователя, например — administrator, он будет получать все сообщения об ошибках при доставке сообщений. Установим флажок У меня есть Интернет-домен и введем в расположенное ниже поле значение server.ru. Сбросим флажок Использовать ETRN-команду.

Перейдем ко вкладке Удаленный доступ по протоколу POP3 окна Настройки почтового сервера и нажмем на кнопку Добавить. Введем следующие настройки учетной записи электронной почты:

- Имя пользователя: mail.server (это имя должно соответствовать учетной записи, требуемой для доступа к общей папке mail на почтовом сервере, в которой хранится вся почта для наших пользователей);
- Пароль: пароль для доступа к почтовому серверу;
- установим переключатель в положение Аутентификация по POP3;
- вполе Сервер POP3 введем mail.server.ru;
- в меню Направить выберем пункт {Sorting Rule};
- Щелкнем мышью на кнопке OK.

Вернувшись во вкладку Удаленный доступ по протоколу POP3, нажмем на кнопку Правила сортировки, затем — на кнопку Добавить. Введем следующие правила сортировки:

- Если поле заголовка «Кому» содержит: valentin@server.ru Направить: valentIn
- Если поле заголовка «Кому» содержит: administrator@server.ru Направить: administrator
- Если поле заголовка «Кому» содержит: maria@server.ru Направить: maria

а Если поле заголовка **«Кому» содержит:** info@server.ru Направить: valentin

а **Если поле заголовка «Кому» содержит:** webmaster@server.ru **Направить:** maria

Конфигурация окна настройки почтового сервера WinRoute в этом примере показана на рис. 7.11.

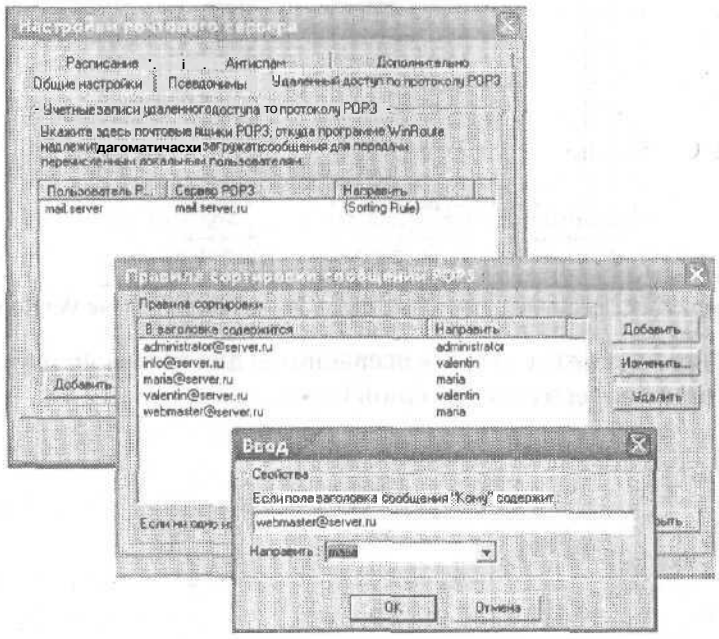


Рис. 7.11. Пример настроек сортировки почтовых сообщений в программе WinRoute

В окне Правила сортировки сообщений POP3 выберите в меню Если ни одно из правил не подходит, направить сообщение: учетную запись пользователя, на который будут направляться все прочие письма, например administrator. Это означает, что если, например, в папку mail на сервере попадет письмо, направленное на адрес company@server.ru, оно попадет пользователюadministrator.

При таких настройках электронной почты необходимо отдельно указать так называемые *псевдонимы,* или *alias,* использование которых заметно ускоряет маршрутизацию почты внутри локальной сети. Служат они для того, чтобы в случае, если пользователи локальной сети будут направлять письма друг другу, они рассортировывались по их локальным почтовым ящикам напрямую, без отправки в Интернет. Для этого откройте вкладку Псевдонимы в окне Настройки почтового сервера, нажмите кнопку Добавить, затем введите в поле Псевдоним значение info, в меню направить выберите пользователя valentin и щелкните мышью на кнопке OK. Повторите ту же процедуру для пользователя maria и псевдонима webmaster (рис. 7.12)

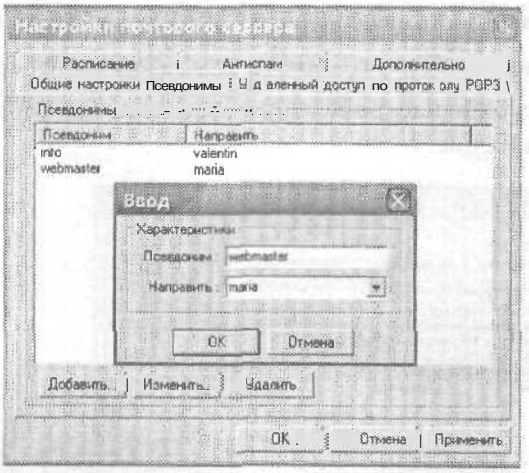


Рис. 7.12. Настройка почтовых псевдонимов в программе WinRoute

При желании вы можете указать псевдонимы для всех используемых вами корпоративных адресов электронной почты.

Глава 8

Краткие сведения о беспроводных технологиях

- Настольные системы беспроводной связи
- Системы Radio Ethernet
- Системы с микросотовой архитектурой
- Технологические особенности организации беспроводных сетей

В этой главе мы кратко рассмотрим основные технологии передачи данных в беспроводных локальных сетях. В настоящее время беспроводные технологии становятся все более доступными и понемногу получают значительное распространение среди прочих способов передачи данных между нескольким объединенными в вычислительную систему компьютерами.

Проектирование локальной сети практически всегда сопряжено со множеством трудностей: следует закупить необходимое оборудование и программное обеспечение, проложить кабель и смонтировать разъемы, расположить компьютеры таким образом, чтобы соединяющие их провода не мешали окружающим свободно перемещаться по помещению. Однако еще на стадии предварительных расчетов зачастую выясняется, что некоторые участки сети по тем или иным причинам невозможно связать между собой. Известно, что при организации связи в локальной сети с использованием коаксиального кабеля или кабеля «витая пара» максимально допустимое расстояние между двумя компьютерами без использования дополнительных технических средств составляет всего лишь десятки метров. А как быть, если, например, склад предприятия находится на расстоянии полукилометра от административного корпуса, где расположена бухгалтерия и другие вспомогательные службы, и между ними просто необходимо обеспечить бесперебойный обмен информацией? Или офис вашей компании размещается в охраняемом государством историческом здании, являющемся памятником архитектуры, где прокладка кабеля затруднена установленными администрацией правилами? Вполне возможна и иная ситуация: нескольким

друзьям, живущим в соседних домах, расположенных на расстоянии нескольких сотен метров, захотелось объединить свои компьютеры в локальную сеть. До недавнего времени эта проблема была фактически неразрешимой.

Вместе с тем технические средства, позволяющие обеспечивать беспроводную связь между несколькими компьютерами в локальной сети, существовали уже довольно давно — их разработка началась в США еще в пятидесятые годы. Правда, как это обычно и случается с практически любым ноу-хау из сферы информационных технологий, данные разработки предназначались в основном для нужд военной промышленности. Пионером в указанной области стала американская корпорация Proxim.

Компания Proxim, Inc была создана в 1984 году с целью создания оборудования беспроводной передачи данных для военных приложений. В 1989 году, после того как Федеральная комиссия по телекоммуникациям (FCC) США разрешила использование беспроводных технологий для коммерческих целей, Proxim переориентировался на потребительский рынок. Тем не менее, активное развитие рынка аппаратных средств, предназначенных для организации беспроводной передачи данных в локальной сети предприятия или канала связи для Интернет-провайдеров тормозилось чрезвычайно высокой стоимостью конечного оборудования даже для корпоративных заказчиков. Далеко не все коммерческие организации могли позволить себе приобрести беспроводную сетевую карту ценой от пятисот до семисот долларов США за штуку, не говоря уже о более дорогостоящих аппаратных средствах подобного класса. Именно поэтому беспроводные сети считались до недавнего времени элитными, профессиональными системами, недоступными большей части потребителей. «Свет в конце тоннеля» наметился лишь тогда, когда на российском рынке появилось недорогое беспроводное сетевое оборудование, ориентированное, в первую очередь, на использование в сфере малого, среднего бизнеса, а также в домашних локальных сетях. На сегодняшний день такие системы представлены несколькими семействами аппаратных средств, о которых нам хотелось бы рассказать чуть подробнее.

Настольные системы

Семейство продуктов для домашних и малых корпоративных сетей обеспечивает пользователю практически все преимущества, которые характерны для обычной локальной сети, включая еще одну немаловажную особенность: такая сеть является беспроводной. В настоящее время на рынке присутствует относительно недорогое оборудование данного класса различных производителей: это серия устройств Symphony производства уже упомянутой выше компании Proxim, а также устройства производства компаний LinkSys и Z-com.

Связь между компьютерами с применением таких устройств осуществляется на частоте 2,4 ГГц, мощность, потребляемая подобными аппаратными средствами, не превышает обычно 100 мВт, максимальное расстояние, на которое могут быть удалены друг от друга связанные в сеть компьютеры, без использования направленных антенн, составляет 100-200 м, в том числе сквозь стены и перекрытия зданий. Скорость передачи данных в такой системе составляет от 1,6 до 10 Мбит/с. В случае, если вместо традиционных антенн с круговой диаграммой направленности в беспроводной сети используются узконаправленные антенны, расстояние между компьютерами может быть увеличено, но его конечное значение зависит от множества факторов, например от характеристик помещения, в котором располагаются вычислительные машины, наличия стен, их толщины и материала.

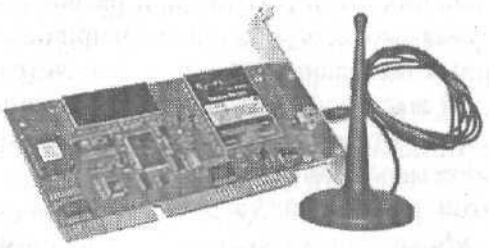


Рис. 8.1. Беспроводной сетевой адаптер

В семейство настольного оборудования входят беспроводные сетевые карты (рис. 8.1), которые могут быть использованы совместно с любым персональным компьютером аналогично обыкновенным сетевым адаптерам, применяющимся в традиционных кабельных сетях, беспроводной модем, который позволяет быстро подключить созданную вами сеть к Интернету по коммутируемой телефонной линии, и совместимый со стандартом lOBaseT мост, с помощью которого можно соединить беспроводной сегмент сети с уже существующей локальной сетью Ethernet или выделенным каналом Интернета. Подобное оборудование обычно поддерживает интерфейсы ISA, PCI и USB, что позволяет устанавливать его в обычных настольных ПК, а также стандарт PCMCIA, благодаря чему в такую сеть можно включить компьютер класса Notebook. Очевидны и другие преимущества беспроводной локальной сети на основе аппаратных средств данного класса по сравнению с обыкновенными кабельными сетями: такая система не требует прокладки проводов и монтажа разъемов, нет необходимости в использовании сетевых концентраторов, беспроводной модем может быть включен в сеть без выделения для него отдельного компьютера, поскольку он может работать в режиме самостоятельного сетевого устройства, эффективный алгоритм передачи информации надежно защищает беспроводную сеть от несанкционированного доступа, а низкий уровень излучаемой мощности

гарантирует полную безопасность этого оборудования для здоровья человека. Однако относительно низкая стоимость подобных комплектующих накладывает жесткие технические ограничения на их функциональные возможности, главное из которых заключается в том, что подобная система в совокупности может содержать не более десяти различных устройств. В частности, в беспроводную сеть Proxim Symphony можно подключить либо десять компьютеров, организовав с их помощью замкнутую структуру передачи данных, либо 9 компьютеров и беспроводной модем, обеспечивающий связь с Интернетом, либо 9 компьютеров и мост, осуществляющий соединение с другой локальной сетью, либо 8 компьютеров, мост и беспроводной модем.

Тем не менее, использование беспроводных малых сетей является оптимальным решением для небольших предприятий, при расширении корпоративной локальной сети в случаях, когда по тем или иным причинам прокладка кабеля в офисных или жилых помещениях не представляется возможной, такие сети незаменимы для выставок, семинаров, конференций и презентаций, поскольку беспроводная сеть может быть развернута в сжатые сроки и быстро свернута по окончании мероприятия при минимальных затратах. Доступные цены позволяют этой технологии уверенно конкурировать с традиционными кабельными сетями. В некоторых случаях, например, при соединении значительно удаленных сегментов сетей, решения на основе беспроводного оборудования могут быть даже дешевле аналогичных сетевых решений на базе кабельных сетей. При этом требования к системе также весьма демократичны: процессор Pentium 200 МГц или выше, свободный слот ISA, PCI или PCMCIA Type 2, RAM от 16 Мбайт, ОС Windows 95/98/NT4/2000/XP и свободное пространство на жестком диске не менее 10 Мбайт.

Системы Radio Ethernet

В своем изначальном варианте системы Radio Ethernet были предназначены для организации связи по принципу «точка—точка» и использовались, как правило, для объединения нескольких удаленных локальных сетей Ethernet в единую вычислительную систему. Основной недостаток технологии Radio Ethernet заключается в том, что такие системы обеспечивали исключительно поочередный алгоритм передачи данных, то есть в случае, если к каналу связи было одновременно подключено несколько абонентов, каждый из них вынужден был ожидать, пока другой абонент завершит прием и передачу информации. Это неизбежно приводило к возникновению «заторов» в сети и невозможности «достучаться» до удаленного сегмента LAN, если канал занят. Общая схема двухсегментной сети Radio Ethernet показана на рис. 8.2.

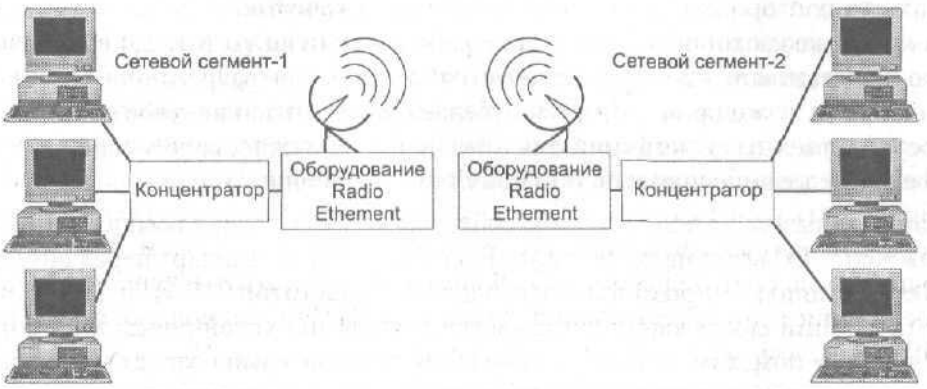


Рис. 8.2. Общая схема сети Radio Ethernet

Современные технические решения позволяют организовывать соединения Radio Ethernet с пропускной способностью до 54 Мбит/с и обеспечивают дальность связи от 100 м до 24 км. В спецификации Института инженеров по радиотехнике и электронике (Institute of Electrical and Electronic Engineers, IEEE) данный стандарт, утвержденный в 1997 году, получил обозначение IEEE 802.11, а среди англоязычных пользователей «прижился» под названием Wireless Local Aria Network (WLAN).

Архитектура Radio Ethernet реализуется на основе механизма общего и равноправного доступа всех абонентов к каналу передачи данных. Для организации канала при этом используются либо световые волны инфракрасного диапазона, либо широкополосный радиосигнал с расширяемым спектром или скачкообразной перестройкой частоты, причем в случае применения радиоволн сигнал передается на частотах 915 МГц или 2,4 ГГц — в зависимости от типа применяемого оборудования, — что позволяет обеспечить скорость передачи данных от 1 до 6 Мбит/с. Вот здесь-то и возникает целый ряд объективных сложностей, которые заметно сужают возможность применения данных технологий в нашей стране. Поскольку аппаратура, использующая в качестве среды передачи данных инфракрасные волны, требует установки приемника и передатчика сигнала в пределах прямой видимости, а качество связи сильно зависит от погодных условий, влажности и задымленности, использовать такие устройства имеет смысл только внутри зданий в пределах одного помещения. Радиодиапазон 900 МГц в России и большинстве стран СНГ занят операторами сотовой связи и радиоканалами различных государственных ведомств и служб, в связи с этим такая аппаратура применяется в основном в пределах здания для организации связи между сегментами сети, расположенными в различных помещениях. В случае установки соединения между соседними зданиями, а также внутри офисных центров, где одновременно присутствует множество владельцев мобильных и высокочастотных комнатных телефонов, высокий

уровень посторонних помех заметно снижает качество и скорость соединения. Что же касается оборудования, работающего на частоте 2,4 ГГц, то для его использования в России требуется специальное разрешение Госсвязьнадзора (в то же время нигде за рубежом получать какие-либо санкции от государственных инстанций для этих целей не нужно, вследствие чего такое оборудование чрезвычайно популярно в Европе и США).

Таким образом, наиболее оптимальным способом связи в рамках технологии Radio Ethernet на территории России является стандарт передачи данных с помощью широкополосных радиоволн частотой 915 МГц. При такой организации связи канал оказывается достаточно устойчивым к широкополосным помехам, однако данное оборудование само создает множество помех с низкой спектральной плотностью. Связь осуществляется на основе собственного канального протокола, обеспечивающего автоматическое определение несущей и предварительное резервирование канала передачи данных, который освобождается по окончании трансляции очередного потока информационных пакетов. Помимо протоколов канального уровня стандарт Radio Ethernet опирается на протокол MAC (Medium Access Control) — протокол доступа к среде передачи данных, также в сетях Radio Ethernet используется специальный протокол обеспечения безопасности WEP (Wired Equivalent Privacy), в задачу которого входит ограничение несанкционированного доступа к сети с использованием алгоритмов аутентификации пользователей и шифрования.

Технология Radio Ethernet принципиально позволяет строить беспроводные сети с микросотовой архитектурой (рис. 8.3). В такой системе роль приемников и передатчиков информации играют специальные устройства, называемые точки доступа, или Access Points (AP). Каждая точка доступа обеспечивает двустороннюю передачу данных на определенной площади в зоне своего действия; благодаря использованию нескольких точек доступа можно организовать некую зону покрытия, в пределах которой пользователь сможет подключиться к локальной сети. Такая сеть может быть создана на основе различных топологий: «точка—точка», «звезда», «точка—много точек» и т. д.

Расширение стандарта Radio Ethernet, принятое в 1999 году и получившее обозначение IEEE 802.11a, описывает возможность передачи данных в беспроводной среде с пропускной способностью канала связи в 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с на частоте 5 ГГц. Для оборудования, работающего в этом частотном диапазоне, характерна более высокая устойчивость к помехам, но в то же время и большая потребляемая мощность в сочетании с меньшим расстоянием между узлами сети.

Существует и еще один стандарт: IEEE 802.11b, также известный под названием Wi-Fi (Wireless Fidelity), в котором описаны сети Radio Ethernet,

работающие в частотном диапазоне 2,4 ГГц и обеспечивающие пропускную способность до 11 Мбит/с. В рамках данного стандарта предусмотрен специальный алгоритм автоматического понижения скорости передачи данных в случае возникновения устойчивых помех. В рамках стандарта 802.11e, предварительно утвержденного в конце 2001 года, помимо разрешения целого ряда спорных вопросов совместимости предполагается включение дополнительных механизмов передачи по беспроводным каналам потоков мультимедийных данных. В настоящее время Институтом инженеров по радиотехнике и электронике рассматривается еще целый ряд стандартов, в рамках которых, как предполагается, будут решены проблемы распределения радиочастот, а также некоторые вопросы безопасности.

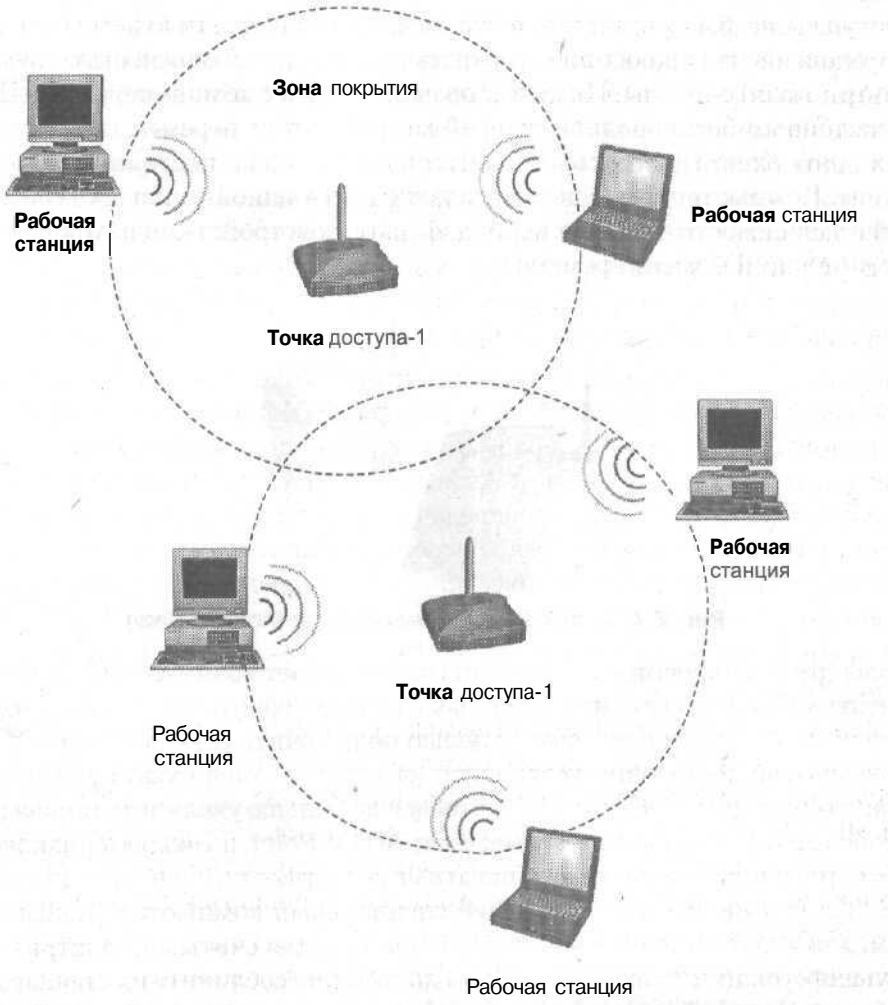


Рис. 8.3. Беспроводная локальная сеть с микросотовой архитектурой

Оборудование для систем с микросотовой архитектурой

Высокотехнологичное оборудование для организации микросотовой беспроводной связи в настоящее время стоит несколько дороже «настольных» устройств, но вместе с тем более высокая стоимость этого класса устройств оправдывается чрезвычайной широтой их функциональных возможностей. При сходных с «настольными» системами технических характеристиках такие комплектующие позволяют создавать до пятнадцати независимых беспроводных сетей в одном физическом пространстве общей пропускной способностью 24 Мбит/с, со средней скоростью передачи данных на канале связи в 1,6 Мбит/с и выше. Подключение нескольких беспроводных точек доступа (рис. 8.4) к различным участкам кабельной сети Ethernet позволяет организовать микросотовую архитектуру связи с возможностью роуминга внутри такой системы. Иными словами, человек с компьютером Notebook, оснащенным беспроводной сетевой картой, может перемещаться в пределах зоны охвата испускаемого антеннами сигнала, постоянно оставаясь в сети. Компьютер сам будет переключаться от одной точки доступа к другой в зависимости от того, к какому из данных устройств он находится ближе в текущий момент времени.

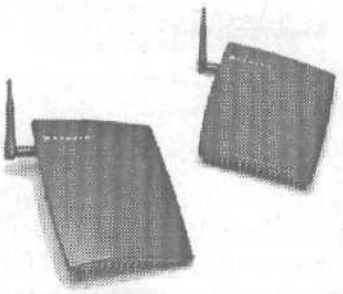


Рис. 8.4. Беспроводные точки доступа (Access Points)

Более того: микросотовая архитектура открывает возможность не прокладывать кабельную сеть на удаленных участках территории, где необходимо обеспечить стабильную связь, с целью подключить еще одну точку доступа — вполне достаточно установить на границе зоны охвата репитер, ретранслирующий сигнал дальше, чтобы еще больше увеличить площадь радиопокрытия. Устройства, называемые Access Point, позволяют подключать к беспроводной сети любые аппаратные средства с интерфейсом стандарта RS232, не выделяя для этих целей специальный компьютер. Таким образом, для включения в сеть принтера, прибора для считывания штрих-кода или информации с магнитной карты достаточно соединить их стандартным кабелем с устройством Access Point — с этого момента они могут быть

доступны оператору любого находящегося в сети компьютера. Помимо репитеров, беспроводных сетевых карт стандарта ISA и PCMCIA для MS Windows и беспроводных адаптеров для устройств с интерфейсом RS232 такое оборудование нередко включает в себя сетевые карты стандарта PCMCIA, совместимые с Windows CE и предназначенные для использования на портативных и миникомпьютерах, а также беспроводные мосты стандарта Ethernet и Token Ring мощностью 100 и 500 мВт.

Беспроводные мосты

Высокочастотные беспроводные мосты — это специальные устройства, обеспечивающие высокопроизводительную передачу голоса и данных в сетях Radio Ethernet. Наиболее известным оборудованием из этого семейства являются устройства Stratum производства компании Proxim (рис. 8.5).

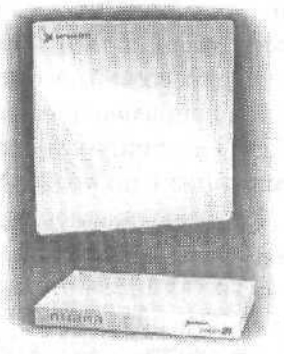


Рис. 8.5. Беспроводной мост

Оборудование этого класса обладает достаточной пропускной способностью для всех типов трафика, включая IP и Voice Over IP. Предусмотрена функция автоматического определения типа сети 10 BaseT/100BaseT Ethernet. В дополнение к стандартным функциям стомегабитного моста, обеспечивающего связь между различными сегментами сети, Stratum располагает двумя дополнительными интерфейсами, обеспечивающими транспорт потоков T1, например для передачи голосовых данных в цифровом виде между учрежденческими АТС.

Беспроводные мосты используют полосу частот, выделенную в соответствии с рекомендациями FCC для широкополосных соединений типа «точка—точка». Высокочастотный диапазон обеспечивает независимость эффективности работы оборудования от погодных условий. При использовании стандартной антенны в виде плоско-панельной фазированной решетки обеспечивается дальность связи до 6,5 км, а применение внешней параболической антенны позволяет увеличить дальность связи до 11 км. Связь обеспечивается при условии прямой видимости.

Долгие годы оптоволоконные сети оставались стандартом производительности для телекоммуникаций. Сегодня, с появлением высокочастотных беспроводным мостов, устанавливаются новые стандарты организации связи на большие расстояния для беспроводных коммуникаций, ранее доступные только оптоволоконным системам. Эффективные алгоритмы коррекции ошибок в сочетании с высоким соотношением сигнал-шум позволяют обеспечить надежность связи, сопоставимую с аналогичными показателями для сетей на основе оптоволоконных линий. Широкополосные возможности оборудования делают его идеальным выбором для решения задач, когда требуется высокая пропускная способность, таких как высокоскоростной доступ к Интернету, передача голоса поверх протокола IP или трансляция видео в реальном времени.

Оборудование для беспроводной сети может быть установлено в течение нескольких часов, кроме того, оно обычно не требует обслуживания или настройки в течение всего срока службы. Для хранения системного программного обеспечения в данном аппаратном комплексе используется Flash-память. Мониторинг оборудования возможен с использованием стандартных протоколов SNMP или Telnet, например посредством таких управляющих программ, как HP Open View или SunNet Manager. Соответствие индустриальным стандартам обеспечивает полный SNMP-доступ ко всем параметрам и настройкам системы. Для управления используется стандартный HTML-интерфейс пользователя, организованный в виде контекстных меню; предусмотрена многоуровневая организация паролей для защиты в случае доступа со стандартных веб-браузеров.

Комбинация высокой пропускной способности, соответствия промышленным стандартам, легкости в инсталляции и управлении, возможности передачи не только данных, но и голоса обеспечивает высокую конкурентоспособность оборудования Radio Ethernet по сравнению с другими аналогичными системами, в том числе основанными на использовании кабельного соединения или оптической линии связи.

Наблюдая динамику развития беспроводных сетевых систем не только в нашей стране, но и во всем мире, можно смело судить о том, что данный класс оборудования уверенно завоевывает значительную долю рынка информационных технологий, и, возможно, в не столь уж отдаленном будущем сети с беспроводной архитектурой станут доминирующими среди массы традиционных кабельных сетей, постепенно перейдя из сферы технических новинок в разряд обыденных и общепризнанных явлений.

Глоссарий

iOOOBaseT (Gigabit Ethernet) — один из классов сетей *Ethernet.* Обеспечивает скорость передачи данных до 1000 Мбит/с (1 Гбит/с). В архитектуре сетей 1 OOOBaseT используется топология «звезда» на базе высококачественного кабеля «витая пара» категории 5, в котором задействованы все восемь жил, причем каждая из четырех пар проводников используется как для приема, так и для передачи информации. По сравнению с технологией 1 OOBaseT, несущая частота в сетях 1 OOOBaseT увеличена вдвое, благодаря чему достигается десятикратное увеличение пропускной способности линии связи.

100BaseFX — расширение технологии *100BaseT* для локальных сетей, созданных с использованием *оптоволоконного кабеля.*

100BaseT (Fast Ethernet) — один из классов сетей *Ethernet.* Обеспечивает скорость передачи данных до 100 Мбит/с. Локальные сети Fast Ethernet имеют звездообразную топологию и могут быть собраны с использованием различных типов кабеля, наиболее часто применяемым из которых является *витая пара.* В 1995 году данный стандарт вошел в спецификацию IEEE 802.3 (это расширение спецификации получило обозначение IEEE 802.3u).

100BaseT4 — расширение технологии *100BaseT.* В таких сетях также используется *витая пара,* однако в ней задействованы все восемь жил проводника: одна пара работает только на прием данных, одна — только на передачу, а оставшиеся две обеспечивают двунаправленных обмен информацией.

100BaseTX — расширение технологии *100BaseT,* В таких сетях используется стандартная *витая пара* пятой категории, в которой задействовано только четыре проводника из восьми имеющихся; два — для приема данных и два — для передачи.

10Base2 (Thin Ethernet) — один из классов сетей *Ethernet* Для соединения компьютеров используется тонкий экранированный коаксиальный кабель с волновым сопротивлением 50 Ом, оснащенный *Т-коннекторами и терминаторами.* Максимальная длина одного сегмента сети 10Base2 может достигать 185 м, при этом минимальное расстояние между точками подключения составляет 0,5 м. Наибольшее число компьютеров, подключаемых к одному сегменту такой сети, не должно превышать 30, максимально допустимое

количество сегментов сети составляет 5. Пропускная способность данной сети, как это следует из обозначения ее класса, составляет 10 Мбит/с.

10Base5 (Толстый Ethernet) — один из классов сетей *Ethernet.* Сети стандарта 10Base5 использовали топологию «общая шина» и создавались на основе коаксиального кабеля с волновым сопротивлением 50 Ом и пропускной способностью 10 Мбит/с.

lOBaseF (Fiber Optic) — один из классов сетей *Ethernet.* К этому классу принято относить распределенные вычислительные сети, сегменты которых соединены посредством магистрального оптоволоконного кабеля, длина которого может достигать 2 км. Такие сети имеют звездообразную топологию и обладают пропускной способностью до 10^{12}бит/с.

lOBaseT — один из классов сетей *Ethernet,* Обеспечивает скорость передачи данных 10 Мбит/с, использует звездообразную топологию, в качестве среды передачи данных применяется кабель *витая пара.* В качестве центрального звена в звездообразной структуре локальной сети 10BaseT применяется специальное устройство, называемое *хабом* или *концентратором.*

Access Points — см. *Точки доступа.*

Advanced Research Projects Agency, ARPA — см. *Агентство перспективных исследований.*

AUI (Attachment Unit Interface) — 15-контактный разъем для подключения *трансивера* в оптоволоконных сетях *lOBaseF.*

AWG (American Wide Gauge) — американский стандарт исчисления диаметра кабеля *витая пара.* Чем меньше диаметр, тем больше величина AWG.

BNC (Bayonet Network Connector) — разъем для подключения *экранированного коаксиального кабеля* к различным устройствам. Данные разъемы имеют цилиндрическую форму и внешне отдаленно напоминают приемное гнездо штекера телевизионной антенны. На внешней поверхности цилиндрической части разъема, как правило, имеется два небольших выступа высотой приблизительно в миллиметр, предназначенных для фиксации замка *Т-коннектора.*

BootROM — специальная микросхема постоянной памяти в составе *сетевого адаптера,* при использовании которой становится возможна загрузка операционной системы на компьютер с удаленного узла локальной сети.

Coax at a home — технология подключения к Интернету с использованием каналов кабельной телевизионной сети. В обобщенном виде такая информационная структура выглядит следующим образом: стандартное оборудование вещания кабельного телевизионного центра подключается к специальному устройству передачи данных, называемому головным модемом, и далее, через маршрутизатор, — к высокоскоростному каналу Интернет. После этого абоненту достаточно лишь установить на своем компьютере

любую сетевую карту, поддерживающую стандарт 10Base-T, соединив ее с клиентским кабельным модемом, а тот, в свою очередь, подключить к расположенному в квартире антенному выходу.

Cross-over (MDI-X) — способ монтажа разъема *RJ-45* на кабеле витая пара для соединения двух компьютеров напрямую по принципу «точка—точка».

CSMA/CD (Carrier Sense Multiple Access/Collision Detection) — спецификация для локальных сетей, построенных по принципу множественного доступа, определения несущей частоты и автоматического обнаружения сбоев. Соответствует стандарту IEEE 802.3,

Dial-up Access — подключение к Интернету по коммутируемому соединению через телефонную или выделенную линию при помощи модема.

ENS **(Extended Network Support)** — утилита, которая дополняет протокол NAT (Network Address Translation), что позволяет использовать в локальной сети клиентские компьютеры, работающие под управлением отличных от Windows операционных систем и позволяет пользователям взаимодействовать с устройствами на компьютерах, работающих в разных подсетях.

EPROM — специальная микросхема программируемой постоянной памяти в составе *сетевого адаптера*, в которой хранится информация о текущих настройках устройства и используемых им ресурсах.

Ethernet — один из общепринятых стандартов локальных сетей на основе единого алгоритма разделения среды передачи информации — CSMA/CD. На долю сетей Ethernet приходится почти девяносто процентов всех малых и домашних локальных сетей, что неудивительно, поскольку именно эта технология позволяет строить простые и удобные в эксплуатации и настройке локальные сети с минимумом затрат.

Fast Ethernet — см. *100BaseT.*

Fiber Optic — см. *10BaseF.*

FTP (File Transfer Protocol) — протокол прикладного уровня, предназначен для передачи файлов через Интернет.

Gateway (в терминологии *WinGate*)— компьютер, через который в локальной сети осуществляется соединение с Интернетом.

Gigabit Ethernet - см. *1000BaseT.*

HTTP (Hyper Text Transfer Protocol) — протокол прикладного уровня, обеспечивает передачу с удаленных серверов на локальный компьютер документов, содержащих код разметки гипертекста, написанный на языке HTML или XML, то есть веб-страниц. Данный прикладной протокол ориентирован прежде всего на предоставление информации программам просмотра веб-страниц, веб-браузерам, наиболее известными из которых являются такие приложения, как Microsoft Internet Explorer и Netscape Communicator.

Hub — см. *Концентратор.*

ICMP (Internet Control Message Protocol) — межсетевой протокол контроля и управления передачей данных.

ICS (Internet Connection Sharing) — система организации общего подключения локальной сети к Интернету в операционной системе Microsoft Windows XP.

IEEE (Institute of Electrical and Electronic Engineers) — Институт инженеров по радиотехнике и электронике, организация, занимающаяся разработкой международных стандартов, в том числе и для локальных сетей.

IP (Internet Protocol) — универсальный кроссплатформенный стандарт, позволяющий объединять в сеть разнородные вычислительные машины, работающие под управлением разных операционных систем.

IPX (Internet Packet Exchange) — межсетевой протокол, используемый в локальных сетях, узлы которых работают под управлением операционных систем семейства Nowell Netware. Данный протокол обеспечивает передачу дейтаграмм в таких сетях без организации логического соединения, которое организуется протоколом транспортного уровня.

IP-адрес — адрес узла сети, работающей под управлением *протокола IP,* состоит из четырех десятизначных идентификаторов, или октетов (по одному байту каждый), разделенных точкой.

I-коннектор — см. *Переход прямой.*

LAN (Local Area Network) — см. *Локальная сеть.*

MAC (Medium Access Control) — протокол доступа к среде передачи данных в сетях *Radio Ethernet.*

NetBEUI (NetBIOS Extended User Interface) — расширенный интерфейс протокола *NetBIOS,* разработанный корпорацией IBM. Этот протокол рассчитан на поддержку небольших локальных сетей, включающих не более 150-200 машин, и по причине того, что данный протокол может использоваться только в отдельных сегментах локальных сетей (пакеты NetBEUI не могут транслироваться через мосты), этот стандарт считается устаревшим и более не поддерживается операционной системой Microsoft Windows XP, хотя его поддержка имеется в ОС семейства Windows 9x/ME/2000.

NetBIOS (Network Basic Input/Output System) — базовый протокол для локальных сетей, работающих под управлением операционных систем семейств Nowell Netware и OS/2, однако его поддержка реализована также и в ОС Microsoft Windows, и в некоторых реализациях Unix-совместимых операционных систем. Фактически можно сказать, что данный протокол работает сразу на нескольких логических уровнях стека протоколов: на транспортном уровне он организует интерфейс между сетевыми приложениями в качестве

надстройки над протоколами IPX/SPX, на межсетевом — управляет маршрутизацией дейтаграмм, на канальном уровне — организует обмен сообщениями между различными узлами сети.

Path cord — отрезок кабеля *витая пара*, оснащенный двумя разъемами *RJ-45* и предназначенный для соединения соответствующего порта *сетевого адаптера с* соответствующим портом *сетевой розетки* или *концентратора*.

Path panel — устройство, представляющее собой набор *сетевых розеток* для сетей *10BaseT*, смонтированных в одном корпусе.

POP3 (Post Office Protocol) — прикладной протокол, предназначенный для передачи входящих сообщений по каналам электронной почты.

Radio Ethernet — один из способов организации локальной сети с применением беспроводных каналов связи.

Ring — «главный» провод в каждой из пар проводников кабеля *витая пара*. Как правило, имеет защитную оболочку однотонной окраски.

RIP (Routing Internet Protocol) — протокол маршрутизации информационных потоков в Интернете.

RJ-45 — разъем для подключения кабеля *витая пара* к различным устройствам. Имеет вид углубления прямоугольной формы с небольшим пазом для замка сетевой вилки, в нижней части гнезда расположено восемь контактов, соединяющихся с соответствующими контактами вилки сетевого кабеля.

SMTP (Simple Mail Transfer Protocol) — прикладной протокол, предназначенный для передачи исходящих сообщений по каналам электронной почты.

SPX — транспортный протокол, выполняющий функции контроля над передачей информации в IPX-сетях.

Switch — см. *Коммутатор*.

TCP (Transmission Control Protocol) — транспортный протокол, опирающийся на возможности протокола IP. Выполняет функции контроля передачи информации в IP-сетях.

TELNET — протокол прикладного уровня, предназначен для организации терминального доступа к удаленному узлу посредством обмена командами в символьном формате ASCII.

TELNET-клиент — специальное программное обеспечение, предназначенное для работы с удаленными узлами по протоколу *TELNET*.

Tip — «дополнительный» провод в каждой из пар проводников кабеля *витая пара*. Как правило, имеет защитную оболочку полосатой окраски.

UDP (User Datagram Protocol) — прикладной протокол, используется на медленных линиях для трансляции информации как *дейтаграмм*.

Universal Plug&Play (UPnP) — технология, позволяющая организовывать совместное использование конечного оборудования для различных прикладных задач. Universal Plug&Play дает возможность подключать к вашему компьютеру устройства, фактически расположенные на удаленном сетевом компьютере, и пользоваться ими так, словно они работают на вашей машине. Каждому сетевому устройству динамически назначается собственный IP-адрес, благодаря чему различная периферийная аппаратура может самостоятельно обмениваться данными в локальной сети, получать сведения о характеристиках и состоянии другого работающего в сети устройства, сообщать информацию «о себе» и передавать свои ресурсы в распоряжение других пользователей.

URL (Uniform Resource Locator) — форма записи адреса того или иного ресурса сети Интернет вида: http://www.domain.zone/page.htm (.html).

VPN (Virtual Private Network) — технология, позволяющая соединять через Интернет несколько удаленных друг от друга подсетей в одну локальную сеть.

WEP (Wired Equivalent Privacy) — протокол *Radio Ethernet*, в задачу которого входит ограничение несанкционированного доступа к сети с использованием алгоритмов аутентификации пользователей и шифрования.

Wi-Fi (Wireless Fidelity) — один из стандартов *Radio Ethernet* в котором описаны беспроводные сети, работающие в частотном диапазоне 2,4 ГГц и обеспечивающие пропускную способность до 11 Мбит/с.

WinGate — прокси-сервер для ОС Windows, используется для организации общего доступа в Интернет через единственное соединение.

WinRoute — прокси-сервер для ОС Windows, используется для организации общего доступа в Интернет через единственное соединение.

Wireless Local Aria Network (WLAN) — альтернативное название для беспроводных локальных сетей, соответствующих международному стандарту IEEE 802.11.

Агентство перспективных исследований (ARPA) — американская государственная организация, ставящая своей целью финансирование и поддержку исследований в области перспективных технологий.

Адаптер (в терминологии ОС Windows) — это устройство, посредством которого реализуется непосредственное подключение компьютера к сети. В ОС Microsoft Windows 9x/ME различается два типа адаптеров — физические, то есть те сетевые карты, которые непосредственно входят в аппаратную конфигурацию компьютера, и «виртуальные адаптеры», в частности, так называемый *Контроллер удаленного доступа* — программный эмулятор сетевого адаптера, используемый операционной системой.

Адаптер сетевой — специальное устройство, основное назначение которого состоит в обеспечении двунаправленного обмена данными между персональным компьютером и локальной сетью. Являясь одним из элементов аппаратной конфигурации компьютера, таким же, как, например, модем, видеоадаптер или звуковая карта, сетевые адаптеры подключаются к ПК через один из стандартных портов и настраиваются аналогично прочему оборудованию.

В отличие от обычных I-коннекторов стационарные прямые переходы имеют специальную упорную шайбу и вращающуюся гайку, между которыми помещается металлический уголок с отверстием или вырезом под диаметр разъема. Этот уголок, в свою очередь, жестко крепится винтом к стене, боковой стенке стола или к полу.

Виртуальный канал — соединение двух включенных в сеть компьютеров, между которыми осуществляется передача данных.

Дейтаграмма — специальный фрагмент информации, передаваемый через сеть независимо от других аналогичных фрагментов, без образования виртуального канала и подтверждения приема. В заголовок дейтограммы записывается адрес компьютера-получателя пересылаемых данных и сведения о маршруте следования дейтограммы.

Звездообразная топология — одна из *топологий* локальных сетей, в которой компьютеры соединяются между собой параллельно, то есть каждый из узлов сети подключается собственным отрезком провода к соответствующему порту некоего устройства, называемого *«концентратором»*.

Кабель витая пара — кабель, применяемый при построении сетей *10BaseT*, содержит не одну, а четыре пары проводников, перевитых друг относительно друга. Каждая пара также закручивается относительно других пар проводников.

Кабель коаксиальный **экранированный** — применяется в локальных сетях класса *10Base2*. Он имеет четырехслойную структуру: два слоя коаксиального кабеля выполнены из проводника, два — из диэлектрика. Самый внутренний слой — это проводящая жила, по которой в локальной сети передается несущий информацию сигнал. Жила может быть представлена в виде нескольких сплетенных тонких проводников, либо в виде одной толстой медной проволоки, что является более распространенным вариантом. Жила покрыта диэлектрической пленкой, поверх которой расположен второй проводящий слой — так называемый экран, защищающий линию от посторонних помех. Экран выполнен в виде металлической проволочной оплетки, иногда помимо оплетки внутренний изолирующий слой обернут в металлическую фольгу — такие кабели называют кабелями с двойной экранизацией.

Кабель оптоволоконный — кабель на основе волноводов из диэлектрического волокна. Затухание сигнала в такой линии крайне мало: оно составляет величину порядка 0,2 дБ па километр при длине волны 1,55 мкм, что

потенциально позволяет передавать информацию на расстояния около 100 км без использования дополнительных усилителей и ретрансляторов. Кроме того, в оптических линиях связи частота несущего сигнала достигает 10^{14} Гц, а это означает, что скорость передачи данных по такой магистрали может составлять 10^{12} бит в секунду.

Канальный уровень стека протоколов — уровень *стека протоколов,* на котором осуществляется преобразование *дейтаграмм* в соответствующий сигнал, который через коммуникационное устройство транслируется по сети. В самом простом случае, когда компьютер напрямую подключен к локальной сети того или иного стандарта посредством сетевого адаптера, роль протокола канального уровня играет драйвер этого адаптера, непосредственно реализующий интерфейс с сетью. В более сложных ситуациях на канальном уровне может работать сразу несколько специализированных протоколов, каждый из которых выполняет собственный набор функций.

Клиент (в терминологии ОС Windows) — это набор программного обеспечения, обеспечивающего двусторонний обмен данными между локальной сетью и данным компьютером.

Колпачки защитные — пластиковые насадки на разъем *RJ-45,* внешне напоминают небольшие полые изнутри чехлы, повторяющие своей формой очертания разъема, выполнены из мягкого пластика или резины различных цветов. Защитные колпачки призваны предохранять место соединения кабеля «витая пара» с разъемом *RJ-45* от изгибов и заломов.

Коммутатор (switch) — устройство, применяемое в сетях *10BaseT.* Встроенное в switch программное обеспечение способно самостоятельно анализировать содержимое пересылаемых по сети блоков данных и обеспечивать прямую передачу информации между любыми двумя из своих портов независимо от всех остальных портов устройства.

Контроллер удаленного доступа — программный эмулятор *сетевого адаптера,* используемый операционной системой ОС Windows.

Концентратор — специальное устройство, которое является «центральным» звеном в локальных сетях классов *10BaseT* и *100BaseT,* имеющих топологию «звезда». Фактически концентратор представляет собой мультипортовый *репитер,* то есть в его основную функциональную задачу входит получение данных от подключенных к портам концентратора компьютеров или других устройств, реформирование сигнала одновременно с его усилением и дальнейшая его ретрансляция на другие порты.

Локальная сеть — это *распределенная вычислительная система,* позволяющая всем подключенным к ней компьютерам — *узлам или рабочим станциям* — обмениваться данными и совместно использовать различные аппаратные, а также программные ресурсы.

Маршрутизаторы, роутеры — специализированные серверы, осуществляющие маршрутизацию (см. *Маршрутизация).*

Маршрутизация — процесс определения маршрута движения информации внутри локальной сети от отправителя к получателю.

Маска подсети — запись, определяющая принцип, по которому осуществляется распознавание номеров узлов в составе IP-адреса: биты маски подсети, обозначающие номер самой IP-сети, должны быть равны единице, а биты, определяющие номер узла, — нулю.

Межсетевой уровень стека протоколов — уровень *стека протоколов,* на котором реализуется взаимодействие конкретных компьютеров распределенной вычислительной системы и выполняется процедура *маршрутизации.* Получая пакет данных от протокола транспортного уровня вместе с запросом на его передачу и указанием получателя, протокол межсетевого уровня выясняет, на какой компьютер следует передать информацию, находится ли этот компьютер в пределах данного сегмента локальной сети, или на пути к нему расположен шлюз, после чего трансформирует пакет в *дейтаграмму,* передаваемую на *канальныйуровень.* Получая дейтаграмму, протокол межсетевого уровня определяет правильность ее приема, после чего выясняет, адресована ли она локальному компьютеру, или же ее следует направить по сети дальше. В случае если дальнейшей пересылки не требуется, протокол межсетевого уровня удаляет заголовок дейтаграммы, вычисляет, какой из транспортных протоколов данного компьютера будет обрабатывать полученную информацию, трансформирует ее в соответствующий пакет и передает на *транспортный уровень.*

Общая шина — одна из *топологий* локальных сетей, подразумевает последовательное соединение компьютеров в цепочку наподобие «гирлянды».

Пакет данных — конечный объем информации, получаемый от прикладных программ и транслируемый в сеть, помимо самих данных, предназначенных для передачи, может содержать некоторую дополнительную информацию, например, идентификатор программы, для которой предназначены передаваемые данные и контрольную сумму, необходимую для проверки целостности пакета. Пакеты формируются из потоков данных протоколами *транспортного уровня.*

Переход прямой (I-коннектор) — устройства, позволяющие соединить два сегмента сети 10Base2 без подключения между ними дополнительного компьютера. Обычные I-коннекторы представляют собой двухсекционный разъем, позволяющий подключать к каждой из своих секций по одному разъему BNC, установленному на соответствующем отрезке коаксиального кабеля, выполняя таким образом непосредственное соединение между собой двух сегментов сети. I-коннекторы не крепятся к каким-либо внешним предметам, а свободно присоединяются к кабелю.

Подсеть — часть локальной сети, структурированная по сетевому адресу входящих в нее компьютеров. В частности, в IP-сетях подсети различаются значением третьего октета *IP-адреса.* Как правило, в качестве каждой из подсетей используется физическая сеть какого-либо отдела фирмы, скажем, сеть Ethernet, объединяющая все компьютеры бухгалтерии.

Порт программный — идентификатор программы, благодаря которому протоколы определяют, для какого именно приложения предназначена та или иная последовательность данных. В частности, протокол прикладного уровня SMTP, предназначенный для отправки сообщений электронной почты, работает обычно с портом 25, протокол входящей почты POP3 — с портом 110, протокол Telnet — с портом 23. Задача перенаправления потоков данных между программными портами лежит на транспортных протоколах.

Прикладной уровень стека протоколов — уровень *стека протоколов,* который обеспечивает интерфейс с программным обеспечением, организующим работу пользователя в сети. При запуске любой программы, для функционирования которой требуется диалог с сетью, эта программа вызывает соответствующий протокол прикладного уровня. Данный протокол передает программе информацию из сети в доступном для обработки формате, то есть в виде системных сообщений, либо в виде потока байтов. Протокол прикладного уровня выступает в роли своего рода посредника между сетью и программным обеспечением, преобразуя транслируемую через сеть информацию в «понятную» программе-получателю форму.

Прокси-сервер — специальная программа, позволяющая кэшировать (сохранять на диске) запросы к удаленным серверам Интернета от компьютеров локальной сети и передавать им запрошенную информацию. В локальных сетях используются для организации общего доступа в Интернет через единственное соединение.

Протокол передачи данных, протокол — набор спецификаций, позволяющих осуществлять обмен данными между двумя включенными в сеть компьютерами, то есть стандарт, содержащий описание правил приема и передачи между двумя компьютерами команд, текста, графики и иных данных, который служит для синхронизации работы нескольких компьютеров в сети.

Протокол сетевой (протокол передачи данных) — согласованный и утвержденный стандарт, содержащий описание правил приема и передачи между несколькими компьютерами команд, файлов, иных данных и служащий для синхронизации работы вычислительных машин в сети.

Протокол сквозной — протокол, при помощи которого обеспечивается беспрепятственное прохождение IP-пакетов через не IP-сеть.

Репитер (повторитель) — специальное устройство, предназначенное для усиления и очистки от посторонних помех проходящих по сети сигналов.

Репитеры оснащены как минимум двумя, а иногда — большим числом сетевых портов с одним из стандартных интерфейсов, и присоединяются они непосредственно к локальной сети на максимально допустимом расстоянии от ближайшей точки подключения (для сетей класса 10BaseT оно составляет 100 м). Получив сигнал с одного из своих портов, репитер формирует его заново с целью исключить любые потери и искажения, произошедшие в процессе его передачи, после чего ретранслирует результирующий сигнал на все остальные порты.

Розетка сетевая — устройство, оснащенное разъемом *RJ-45* для подключения кабеля *витая пара* в сетях *10BaseT*. Используется для облегчения монтажа и прокладки сети.

Сетевая карта — см. *Адаптер сетевой*.

Службы — подсистемы сетевого программного обеспечения, созданные для выполнения какой-либо одной конкретной задачи, например для организации общего доступа к ресурсам компьютера, удаленного обращения к реестру и т. д.

Стек протоколов — иерархическая система, подразумевающая деление всех сетевых протоколов на логические уровни, каждый из которых выполняет собственный набор функций.

Терминатор — металлическая заглушка, устанавливаемая на оконечных *Т-коннекторах* локальной сети *10Base2 с целью создания необходимого сопротивления нагрузки в 50 Ом*.

Т-коннектор — специальный Т-образный разъем, подключаемый к соответствующему порту сетевого адаптера каждого из узлов сети *10Base2*.

Топология локальной сети — внутренняя архитектура локальной сети, определяемая взаимным расположением *узлов* и подключений.

Точки доступа (Access Points) — специальные устройства, применяемые в сетях *Radio Ethernet* в качестве приемников и передатчиков информации. Каждая точка доступа обеспечивает двустороннюю передачу данных на определенной площади в зоне своего действия; благодаря использованию нескольких точек доступа можно организовать некую зону покрытия, в пределах которой пользователь сможет подключиться к локальной сети.

Трансивер — устройство, применяемое в локальных сетях класса *10Base5*. Термин произошел от сокращения английских понятий transmitter (передатчик) и receiver (приемник). Трансиверы являлись приемниками и передатчиками данных между работающими в сети компьютерами и самой сетью. Помимо функций собственно приемника-передатчика информации, трансиверы обеспечивали надежную электроизоляцию работающих в сети компьютеров, а также выполняли функции устройства, снижающего уровень посторонних электростатических помех.

Транспортный уровень стека протоколов — уровень *стека протоколов,* на котором реализуется контроль правильности передачи данных, а также обеспечение взаимодействия между различными сетевыми приложениями. Помимо этого, протоколы транспортного уровня осуществляют управление передачей информации — например, могут запросить у получателя подтверждение доставки *пакета* и повторно выслать утерянные фрагменты транслируемой последовательности данных.

Трафик — общий суммарный поток информации через один сетевой компьютер.

Хаб — см. *Концентратор,*

Хост — любой работающий в сети компьютер, независимо от его назначения.

Шлюз — программа, при помощи которой можно передавать информацию между двумя сетевыми системами, использующими различные протоколы обмена данными.

Алфавитный указатель

I-L

M

N-O

P

R

S

T

U-V

W

А

В

Г-Д

К

Л

М

П

Р

С

Т

У

Х-Ш

Валентин Холмогоров

Компьютерная сеть своими руками
Самоучитель

Главный редактор	*Е. Строганова*
Заведующий редакцией	*И. Корнеев*
Руководитель проекта	*А. Чижова*
Художник	*Н. Биржаков*
Корректоры	*Н. Лукина, А. Моносов*
Верстка	*А. Круглова*

Лицензия ИД № 05784 от 07.09.01.
Подписано в печать 06.08.03. Формат 70X100/16. Усл. п. л. 14,19.
Тираж 4500 экз. Заказ № 371.
ООО «Питер Принт». 196105, Санкт-Петербург, ул. Благодатная, д. 67в.
Налоговая льгота - общероссийский классификатор продукции
ОК OOS-93, том 2; 953005 - литература учебная.
Отпечатано с готовых диапозитивов в ФГУП «Печатный двор» им. А. М. Горького
Министерства РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
197110, Санкт-Петербург, Чкаловский пр., 15.

КЛУБ ПРОФЕССИОНАЛ

В 1997 году по инициативе генерального директора **Издательского дома «Питер»** Валерия Степанова и при поддержке деловых кругов города в Санкт-Петербурге был основан **«Книжный клуб Профессионал».** Он собрал под флагом клуба профессионалов своего дела, которых объединяет постоянная тяга к знаниям и любовь к книгам. Членами клуба являются лучшие студенты и известные практики из разных сфер деятельности, которые хотят стать или уже стали профессионалами в той или иной области.

Как и все развивающиеся проекты, с течением времени книжный клуб вырос в **«Клуб Профессионал».** Идею клуба сегодня формируют три основные «клубные» функции:

- неформальное общение и совместный досуг интересных людей;
- участие в подготовке специалистов высокого класса (семинары, пакеты книг по специальной литературе);
- формирование и высказывание мнений современного профессионала (при встречах и на страницах журнала).

КАК ВСТУПИТЬ В КЛУБ?

Для вступления в **«Клуб Профессионал»** вам необходимо:

- ознакомиться с правилами вступления в **«Клуб Профессионал»** на страницах журнала или на сайте **www.piter.com;**
- выразить свое желание вступить в **«Клуб Профессионал»** по электронной почте **postbook@piter.com** или по тел. **(812) 103-73-74;**
- заказать книги на сумму не менее 500 рублей в течение любого времени или приобрести комплект **«Библиотека профессионала».**

«БИБЛИОТЕКА ПРОФЕССИОНАЛА»

Мы предлагаем вам получить все необходимые знания, подписавшись **на «Библиотеку профессионала».** Она для тех, кто экономит не только время, но и деньги. Покупая комплект - книжную полку **«Библиотека профессионала»,** вы получаете:

- **скидку 15%** от розничной цены издания, без учета почтовых расходов;
- при покупке двух или более комплектов - дополнительную **скидку 3%;**
- членство в **«Клубе Профессионал»;**
- подарок - журнал **«Клуб Профессионал».**

Закажите бесплатный журнал «Клуб Профессионал».

ИЗДАТЕЛЬСКИЙ ДОМ ПИТЕР®
WWW.PITER.COM

КНИГА-ПОЧТОЙ

ЗАКАЗАТЬ КНИГИ ИЗДАТЕЛЬСКОГО ДОМА «ПИТЕР» МОЖНО ЛЮБЫМ УДОБНЫМ ДЛЯ ВАС СПОСОБОМ:

- по телефону: (812) 103-73-74;
- по электронному адресу: **postbook@piter.com;**
- на нашем сервере: **www.piter.com;**
- по почте: 197198, **Санкт-Петербург, а/я 619 ЗАО «Питер Пост».**

ВЫ МОЖЕТЕ ВЫБРАТЬ ОДИН ИЗ ДВУХ СПОСОБОВ ДОСТАВКИ И ОПЛАТЫ ИЗДАНИЙ:

- Наложенным платежом с оплатой заказа при получении посылки на ближайшем почтовом отделении. Цены на издания приведены ориентировочно и включают в себя стоимость пересылки по почте **(но без учета авиатарифа).** Книги будут высланы нашей службой **«Книга-почтой»** в течение двух недель после получения заказа или выхода книги из печати.
- Оплата наличными при курьерской доставке (для **жителей Москвы и Санкт-Петербурга).** Курьер доставит заказ по указанному адресу в удобное для вас время в течение трех дней.

ПРИ ОФОРМЛЕНИИ ЗАКАЗА УКАЖИТЕ:

- фамилию, имя, отчество, телефон, факс, e-mail;
- почтовый индекс, регион, район, населенный пункт, улицу, дом, корпус, квартиру;
- название книги, автора, код, количество заказываемых экземпляров.

Вы можете заказать бесплатный журнал «Клуб Профессионал».

ИЗДАТЕЛЬСКИЙ ДОМ ПИТЕР®
WWW.PITER.COM

АНТИВИРУС ИГОРЯ ДАНИЛОВА

Dr.WEB

www.drweb.ru

В. Холмогоров

САМОУЧИТЕЛЬ

Компьютерная сеть СВОИМИ РУКАМИ

У вас дома два компьютера? К одному из них подключен принтер, и вам приходится бегать с дискетой, чтобы распечатать документ, подготовленный на другом? Или вы хотите сражаться с друзьями в любимые компьютерные игры? А может быть, вам нужно работать в Интернете, но у вас нет модема, а у ближайшего соседа есть? Или вы хотите самостоятельно спроектировать и проложить небольшую локальную сеть у себя в офисе?.. Решение очевидно — ведь сегодня уже никому не нужно объяснять, насколько эффективнее можно использовать имеющиеся в распоряжении компьютеры и периферийные устройства, если объединить оборудование в локальную сеть!

ISBN 5-94723-646-X

Постройте компьютерную сеть своими руками!

ПИТЕР®
WWW.PITER.COM