С Е Р И Я

ПИТЕР®

Александр Сергеев

Настройка сетей Microsoft

дома и в офисе

ПИТЕР®

Москва · Санкт-Петербург · Нижний Новгород · Воронеж
Новосибирск · Ростов-на-Дону · Екатеринбург · Самара
Киев · Харьков · Минск
2006

ББК 32.988.02
УДК 004.72
С32

Сергеев А. П.
С32 Настройка сетей Microsoft дома и в офисе. Учебный курс. — СПб.: Питер, 2006. — 348 с.: ил.

ISBN 5-469-01114-3

Сети на основе технологий Microsoft давно стали распространенной средой работы. Без компьютерных сетей давно уже не обходится ни один офис. Эта книга позволит читателю разобраться в основных вопросах создания и настройки сетей Microsoft.

Теоретический материал сопровождается практическими примерами, иллюстрациями, а также пошаговыми инструкциями, позволяющими последовательно и четко воплощать излагаемую теорию на практике. Особое внимание уделено вопросам интеграции с Интернетом, а также обеспечению безопасности.

Книга будет полезна системным администраторам и всем пользователям, интересующимся вопросами создания и поддержания работоспособности сетей Microsoft.

ББК 32.988.02
УДК 004.72

ISBN 5-469-01114-3

Краткое содержание

Содержание

Предисловие

Достаточно трудно сказать что-то новое при рассмотрении такого предмета, как локальные вычислительные сети. Этой теме посвящены многочисленные тома стандартов, переводных и авторских книг. Эта книга создавалась как некий сборник рекомендаций, в котором вы найдете ответы на многие вопросы, возникающие при установке и поддержке в рабочем состоянии сетей Ethernet в среде Windows (от ранних Windows 98 до последних Windows XP). Здесь же вы найдете описание принципов функционирования различных аппаратных сетевых компонентов, включая такие сложные устройства, как маршрутизаторы. Будут рассмотрены сетевые топологии, методики поиска и устранения наиболее распространенных неисправностей в сетях. Теоретический материал сопровождается практическими примерами, иллюстрациями, а также пошаговыми инструкциями, позволяющими последовательно и четко воплощать излагаемую теорию на практике. Уделено внимание вопросам интеграции с Интернетом, а также обеспечению безопасности.

Структура книги

Книга состоит из пяти частей, включающих в общей сложности одиннадцать глав. В конце ее приводится словарь распространенных сетевых терминов.

В первую часть книги включены вводные главы, позволяющие ближе познакомиться с предметом изучения. В первой главе вы найдете краткий исторический обзор, дающий общее представление о предмете рассмотрения книги. Вторая глава содержит описание наиболее распространенных топологий локальных вычислительных сетей на физическом и логическом уровнях. Описание физических принципов функционирования ЛВС, наравне с рассмотрением новейших стандартов Gigabit Ethernet и 10 Gigabit Ethernet, можно найти в третьей главе. В ней же рассматриваются беспроводные сети. Четвертая глава посвящена описанию принципов работы протоколов TCP/IP.

Во второй части книги рассматриваются принципы работы физических компонентов сети. Предметом рассмотрения пятой главы являются такие устройства, как сетевые карты, концентраторы, коммутаторы и маршрутизаторы. Здесь же вы найдете советы по монтажу этих устройств, а также их дальнейшему обслуживанию. В шестой главе приводится описание алгоритма проектирования локальной сети, позволяющего создавать сети на основе заданных исходных данных.

Основным предметом рассмотрения третьей части является установка и настройка локальных вычислительных сетей на различных платформах Windows (98/2000/XP). Пошаговые инструкции, а также большое количество иллюстраций значительно упрощают восприятие излагаемого материала.

Четвертая часть книги включает в себя главы, посвященные обеспечению безопасности локальных вычислительных сетей, подключенных к Интернету, а также процедурам настройки удаленного доступа в Windows 2000/XP.

Пятая часть книги носит технический характер и содержит единственную главу, посвященную поиску и устранению неисправностей в ЛВС. Здесь вы найдете описание аппаратных и программных средств, которые наиболее часто применяются в этих целях.

Книга включает единственное приложение, представляющее собой словарь сетевых терминов.

Автор будет благодарен за замечания и пожелания, которые вы можете отсылать на веб-сайт издательства «Питер».

От издательства

Ваши замечания, предложения и 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 веб-сайте издательства: http://www.piter.com.

Введение

Четыре первых главы, входящие в эту часть, являются, главным образом, вводными. Здесь вы найдете краткий исторический обзор возникновения и развития локальных сетей, описание сетевых топологий, а также рассмотрение некоторых теоретических вопросов, связанных с локальными вычислительными сетями. Я настоятельно рекомендую ознакомиться с материалом этой части, поскольку без излагаемой здесь теории будут невозможны проектирование и монтаж локальных сетей. В третьей главе заинтересованный читатель найдет все необходимые теоретические сведения, относящиеся к физическим принципам, на основании которых базируется работа ЛВС. А теперь стоит перейти к первой главе, в которой будет изложена история возникновения и развития локальных вычислительных сетей.

1 ГЛАВА Краткий исторический обзор

Тем, кто живет в XXI веке, кажется, что персональные компьютеры и локальные вычислительные сети существовали всегда. Слишком уж прочно в нашу жизнь вошли эти произведения научно-технической мысли XX века. Сейчас уже трудно представить те времена, когда основным орудием бухгалтера были счеты, а локальную сеть успешно заменяли сотрудники, хаотично перемещающиеся по офису с папками документов. А ведь эти времена вряд ли можно отнести к эпохе «преданий старины глубокой».

Но все проходит, и вот наступили девяностые годы, когда просторы СНГ захлестнула волна компьютеризации, которая, в свою очередь, породила массовое распространение локальных вычислительных сетей (ЛВС). Как только этот феномен пришел к нам, возникла потребность в специалистах, которые могли бы монтировать и обслуживать сети.

Поначалу так оно и было. Любая уважающая себя организация включала в свой штат сетевого (системного) администратора, который и занимался подобными вопросами. Но шло время, и сейчас сети охватывают целые жилые районы или у многих установлены дома. Впрочем, забудем пока о современности и вспомним о том, как все начиналось.

С момента появления первой универсальной ЭВМ в далеких сороковых годах прошлого века возникла проблема связи с периферийными устройствами. Изначально эта задача решалась при помощи фиксированного подключения этих устройств к центральному вычислительному блоку. Но подобное соединение вряд ли можно назвать практичным, поскольку оно не отличалось повышенной надежностью. К тому же слишком часто требовался «человек с паяльником» для изменения конфигурации подобной «первобытной» сети.

Позднее, в шестидесятых годах появились параллельный и последовательный интерфейсы передачи данных, при помощи которых обеспечивался стандартизированный способ соединений центрального вычислительного блока и периферийных

устройств. Однако «дальнобойность» этих интерфейсов не превышала нескольких метров, в связи с чем говорить о сетях было явно преждевременно.

Но технический прогресс неумолим. Возникшие потребности непрерывно стимулировали технологические разработки, результатом чего стало появление локальных вычислительных сетей. Первой в истории коммерческой сетью, потомки которой «дожили» до сегодняшних дней, стала сеть ALOHA, развернутая на Гавайях. Первая сеть обеспечивала передачу сигналов на расстояние до одного километра со средней скоростью передачи сигналов около 3 Мбит/с между 256 станциями, установленными в корпусах Гавайского университета. Причем использовался радиоканал, а сама передача осуществлялась с помощью коммутации пакетов. Наверное в силу этого подобная сеть получила название «эфирной» сети Ethernet.

В 1976 году появилась статья Роберта Меткальфа и Дэвида Боггса, в которой был описан стандарт, определяющий передачу сигналов в этой и подобной ей сетях. Они использовали метод произвольного доступа к сетям, так называемый CSMA (Carrier Sense Multiple Access, многостанционный доступ с контролем несущей). Чуть позднее, в 1979 году появился стандарт Ethernet II, разработанный тремя компаниями — Digital Equipment Corporation, Intel и Xerox. Ранее этот стандарт именовался DIX (по первым буквам названий этих компаний). Он предусматривал работу с «толстыми» коаксиальными кабелями, передача данных по которым осуществлялась со скоростью до 10 Мбит/с. Позднее этот стандарт получил название 10BASE-5.

1982 год ознаменовался выпуском первой сетевой карты Ethernet для компьютера Apple Computer, а в 1984 мир увидела сетевая карта для IBM PC.

Также развивалась теоретическая основа сетей Ethernet. В частности, в 1980 году организацией ISO была предложена модель OSI (Open System Interconnect). Именно 7 уровней этой модели традиционно рассматриваются в большинстве книг, посвященных теоретическим (да и практическим) аспектам локальных вычислительных сетей. И в этой книге я не буду отступать от традиций.

Деятельность по разработке стандартов локальных (да и глобальных) вычислительных сетей была признана настолько важной, что в 1980 году в рамках Института IEEE был сформирован комитет IEEE 802 LAN/MAN Standards Committee. Благодаря усилиям сотрудников этого комитета в 1985 году появился стандарт 802.3 «Carrier Sense Multiple Access with Collision Detection (CSMA/CD)», в котором специфицировано целое семейство протоколов Ethernet.

В настоящее время насчитывается больше десятка широко применяемых протоколов Ethernet. Часть из них представляет уже исторический интерес (например, тот же 10BASE-5 или появившийся чуть позже 10BASE-2), другие широко используются в офисной и домашней среде (например, 100BASE-TX или 100BASE-FX), а третьи появились сравнительно недавно и не получили до сих пор широкого распространения (например, 10Gigabit Ethernet). О невероятной популярности сетей Ethernet говорит тот факт, что соответствующими адаптерами (среди них встречаются даже Gigabit Ethernet) оборудованы все современные материнские платы. И именно сетям этого типа посвящена настоящая книга.

Разумеется, сетями типа Ethernet все не ограничивается. До сих пор встречаются сети Token Ring и FDDI, функционирующие по принципу передачи кольцевого маркера. Но их «ареал обитания» в настоящее время настолько сузился, что вряд ли имеет смысл рассматривать здесь этот предмет. Сети из этой категории — удел профессионалов, для которых предназначены книги несколько другого рода.

В настоящее время все большую популярность приобретают беспроводные сети, которым будет посвящена отдельная глава книги. Просто обратите внимание на тот факт, что несмотря на то, что первый беспроводной стандарт был принят в начале 90-х годов прошлого века, первая коммерческая беспроводная сеть появилась на 20 лет раньше (вспомните о проекте ALOHA, упоминавшемся в начале этой главы).

На этом можно завершить краткий обзор истории зарождения и развития локальных вычислительных сетей и перейти к рассмотрению топологии ЛВС.

2 ГЛАВА Топологии локальных сетей

Пришло время разобраться подробнее с сетями, а также ввести какую-то классификацию.

Сети бывают самые разные. Придерживаясь «генеральной линии» нашей книги, мы говорим о *компьютерных сетях*, а конкретнее, об их подвиде, называемом *локальными вычислительными сетями* (ЛВС). Разумеется, рассматриваться будут не только такие сети. Будут затронуты и *глобальные вычислительные сети*, но лишь в той степени, в которой они связаны с локальными сетями. На их примере будет рассмотрена технология удаленного доступа. Этому важному вопросу мы уделим внимание в десятой главе. А сейчас следует рассмотреть один из основополагающих моментов — *топологию* локальных вычислительных сетей.

ВНИМАНИЕ Существует еще одна распространенная классификация локальных вычислительных сетей, связанная со способом выполнения сетевых вычислений. Сеть называют одноранговой, когда каждый узел в сети равноправен. Иерархическая сеть предполагает выделение центрального сервера и подключаемых к нему клиентских рабочих станций. Оба типа сетей будут рассмотрены в книге.

Топологии локальных вычислительных сетей

Те, кто изучал высшую математику в институте, наверное, знают об этом, а остальным я просто напомню, что слово «топология» имеет греческие корни и означает не что иное, как науку о путях («топос» и «логос»). Именно в этом случае название является очень удачным, так как оно точно отражает суть дела. Кажущееся хаотичным на первый взгляд переплетение кабелей на самом деле

подчиняется однозначным четко определенным правилам, набор которых и образует топологию локальной сети. Ну а теперь дадим некоторые определения.

Локальная вычислительная сеть моделируется графом, вершины которого соответствуют узлам сети, в качестве которых используются сетевые рабочие станции, концентраторы, маршрутизаторы и другие сетевые компоненты, а ребра графа моделируют физические связи между сетевыми компонентами, которые на практике обычно осуществляются с помощью кабелей или беспроводных (инфракрасные лучи и радиоволны) каналов связи.

Помимо *физической топологии*, которая моделирует пути для электрических сигналов в цепи, существует так называемая *логическая топология*. Она определяется как совокупность маршрутов, предназначенных для передачи данных в сети. Логическая топология может отличаться от физической, поскольку поток данных может управляться соответствующими сетевыми компонентами — маршрутизаторами и коммутаторами, подробное описание принципов работы которых является предметом рассмотрения следующей главы.

При выборе топологии сети приходится решать оптимизационные задачи на графах, одна из которых заключается в построении сильно связного графа, моделирующего соответствующую топологию.

ПРИМЕЧАНИЕ Подробно эта важная и интересная тема рассматривается в пятой главе. Там же можно найти примеры применения теории для решения сугубо практических задач — проектирование оптимизированной сети Ethernet.

Прежде чем перейти к изложению дальнейшего материала, следует уточнить, что предметной областью книги являются сети Ethernet, поскольку именно эти сети широко применяются в Windows. В этой главе будет приведен краткий обзор сетей других типов, отличных от Ethernet.

ПРИМЕЧАНИЕ Термин Ethernet впервые использовался Робертом Меткальфом в его знаменитой статье, посвященной сети ALOHA (см. главу 1). Эти сети являются самыми распространенными на сегодняшний день и применяют метод CSMA/CD для контроля передачи данных.

Теперь пришло время поговорить о различных сетевых топологиях, применяемых на практике.

Шинная топология

Одной из наиболее распространенных до недавнего времени топологий ЛВС являлась *шинная топология*. Она представляет собой линейную структуру, которая моделируется графом без циклов. Физически подобная топология реализуется одним общим кабелем (шиной), к которому подключаются рабочие станции. Шина завершается терминатором, который играет роль *оконечной нагрузки*, а также позволяет исключить такое вредное явление, как отражение сигнала. Именно на базе этой топологии были реализованы первые сети Ethernet. На рис. 2.1 представлен пример сети, характеризующейся шинной топологией.

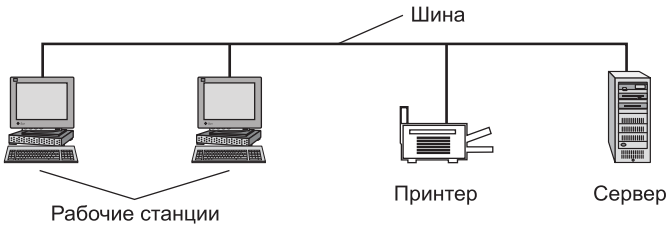


Рис. 2.1. Сеть, характеризующаяся шинной топологией

В настоящее время подобные сети практически не используются на практике, поскольку их эксплуатация сопряжена с наличием нескольких основных проблем:

- невысокая степень надежности, поскольку в случае повреждения единственного кабеля-шины нарушается передача сигналов в сети;
- низкое быстродействие, частично связанное с использованием механизма передачи данных (CSMA/CD, множественный доступ с контролем несущей и обнаружением конфликтов);
- ограничения на предельный размер сети, являющиеся следствием затухания сигнала в процессе его распространения.

ПРИМЕЧАНИЕ На самом деле ограниченное быстродействие связано не только с использованием метода CSMA/CD, а скорее с использованием кабеля, обладающего недостаточной пропускной способностью. Как известно, в современных сетях Fast Ethernet также применяется именно этот метод, но их быстродействие трудно назвать «недостаточным».

ПРИМЕЧАНИЕ Предельный размер сети может быть увеличен, если воспользоваться репитерами, позволяющими усилить сигнал. Подробнее эти устройства рассматриваются в четвертой главе.

Существует несколько разновидностей стандартов, разработанных для описания шинных сетей.

- 10BASE-2. Шинная сеть («тонкий» Ethernet), обеспечивающая скорость передачи данных 10 Мбит/с. Максимальная длина сетевого сегмента составляет 185 м. Подобные сети называются «тонким» Ethernet и еще в 90-х годах прошлого века являлись безусловным лидером по количеству инсталляций. Для подключений рабочих станций к шине используются байонетные коннекторы, а при их монтаже — коаксиальные кабели типа RG-58, волновое сопротивление которых составляет 58 Ом. Не стоит путать их с телевизионными кабелями, так как в данном случае сходство является только внешним. Название «тонкий» относится к толщине сетевого кабеля, который тоньше кабеля, применяемого в сетях 10BASE-5.
- 10BASE-5. Эта тип сети появился раньше, чем 10BASE-2 (альтернативное название — «толстый» Ethernet), и обеспечивает скорость передачи 10 Мбит/с. В данном случае максимальная длина сетевого сегмента составляет 500 м. Несмотря на меньшее затухание сигналов, сети этого типа имеют крупные

недостатки, один из которых связан с трудностями монтажа более толстого кабеля, а также с необходимостью использования специальных внешних трансиверов, с помощью которых осуществляется подключение к рабочим станциям.

Несмотря на практически повсеместное «исчезновение» сетей этого типа, остаются некоторые области, где их применение целесообразно. В частности, эти сети идеальны, если используется не более пяти-шести рабочих станций, а сама сеть предназначается для обмена текстовыми данными.

Звездообразная топология

Наиболее распространенным типом топологии в настоящее время является *звездообразная топология*. Ребра моделирующего ее графа сходятся в одной центральной точке, которая в данном случае выступает в качестве «центрального пульта управления». В качестве такого центрального пункта используются *коммутаторы* и *концентраторы*, подробнее рассматриваемые в пятой главе. Именно эта топология наиболее распространена в настоящее время. На ее основе реализованы современные высокоскоростные версии сетей Ethernet. На рис. 2.2 приведен пример сети со звездообразной топологией.

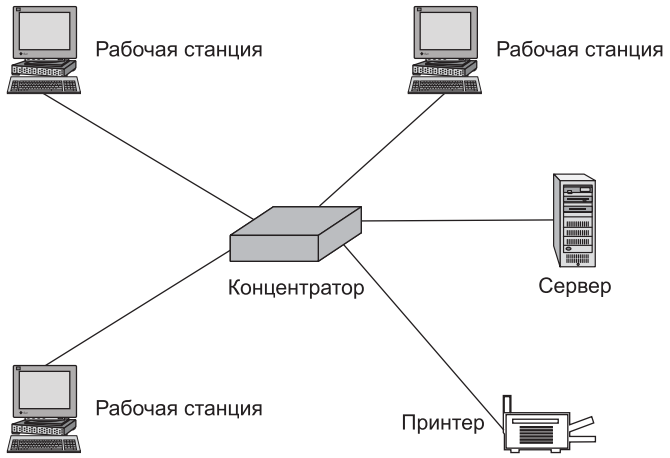


Рис. 2.2. Эта топология является наиболее распространенной в настоящее время

В сетях со сложной структурой могут устанавливаться несколько концентраторов или коммутаторов, которые подключаются каскадным образом. В этом случае топологию называют иерархической звездой. В качестве одного из уровней иерархии может использоваться шина. На рис. 2.3 приведен соответствующий пример.

Как правило, в качестве сетевого кабеля при построении этих сетей используется витая пара, обычно неэкранированная. Потребность в специальном экране не возникает, поскольку жилы кабеля скручены таким образом, что происходит взаимное гашение электромагнитных помех.

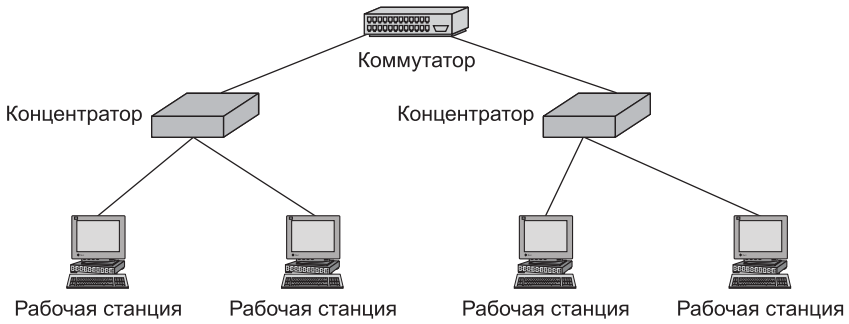


Рис. 2.3. Сеть, топология которой моделируется с помощью иерархической звезды

Существует ряд стандартов, описывающих звездообразные сети, построенные на основе витой пары.

- 10BASE-T. В названии этого стандарта используется буква T (сокращение от слов Twisted Pair). Этот стандарт обладает всеми преимуществами, присущими звездообразной топологии. Если позволяют частотные характеристики используемого кабеля витой пары, возможна модернизация до уровня, описываемого стандартом 100BASE-T (скорость передачи данных — 100 Мбит/с).
- 10BASE-FL. Этот стандарт можно считать устаревшим. Несмотря на то, что для передачи сигнала используется многомодовое оптоволокно (на что указывает аббревиатура FL в названии), скорость передачи данных в сети ограничена значением 10 Мбит/с.
- 100BASE-TX. В сетях этого типа используется кабель пятой категории (впрочем, другие кабели сейчас не применяются), благодаря этому предельное расстояние между рабочей станцией и концентратором составляет 100 м. Передача данных осуществляется с помощью двух пар проводов, объединенных в одном кабеле.
- 100BASE-T4. Эта технология представляет собой своего рода «компромиссное решение», позволяющее выполнить обновление сетей со скоростью передачи данных 10 Мбит/с, в которых используются кабели третьей категории. При этом предельное расстояние между рабочей станцией и концентратором составляет 100 м, а передача данных в сети осуществляется по четырем проводам. Два провода используются для приема данных, а остальные два — для передачи их.
- 100BASE-FX. Аббревиатура FX означает применение волоконно-оптического кабеля (в данном случае идет речь о многомодовом оптоволокне). Для приема и передачи данных используются разные жилы кабеля, а предельное расстояние от концентратора до рабочей станции равно 412 м.
- 1000BASE-SX. Этот стандарт определяет использование в сетях нескольких волоконно-оптических каналов, причем применяется многомодовый кабель. Литера S (short) в обозначении стандарта говорит о том, что применяется коротковолновый участок спектра видимого света (длина волны 850 нм).

Максимальная длина кабельного сегмента, проложенного между концентратором и рабочей станцией, в данном случае составляет 550 м.

- 1000BASE-LX. Этот стандарт описывает волоконно-оптические сети, функционирующие в одномодовом и многомодовом режиме. Символ L в названии указывает на то, что в качестве носителя информации используется длинноволновой «кусок» спектра видимого света (1270–355 нм). Максимальная длина одного сетевого сегмента в этом случае составляет 550 м (многомодовый режим) и до 5000 м (одномодовый режим).
- 1000BASE-CX. Этот стандарт описывает версию сети Gigabit Ethernet, реализованную на основе медного экранированного кабеля. Здесь сказываются существенные ограничения на предельное расстояние между устройствами — всего лишь 25 м.
- 1000BASE-T. Этот стандарт представляет собой версию стандарта 100BASE-T, адаптированного для передачи данных со скоростью до 1 Гбит/с. Как и у предшественника, максимальное расстояние между рабочей станцией и концентратором равно 100 м.
- 10000BASE-T. Официального стандарта с таким названием пока не существует, хотя уже разработан ряд поддерживающих его устройств.

ПРИМЕЧАНИЕ В настоящее время общепринятой практикой является проектирование системных компьютерных плат, снабженных встроенными сетевыми адаптерами, обеспечивающими скорость передачи данных 100 Мбит/с и даже 1 Гбит/с.

ПРИМЕЧАНИЕ Подробнее стандарты высокоскоростных сетей будут рассмотрены в третьей главе.

Кольцевая топология

Кольцевая топология, как и следует из названия, моделирует сеть, форма которой напоминает кольцо (см. рис. 2.4).

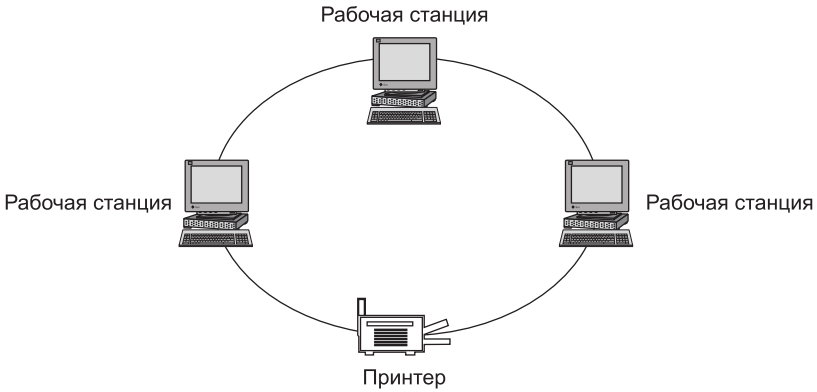


Рис. 2.4. Пример кольцевой топологии

Данные в подобных сетях циркулируют по кольцу, образованному совокупностью рабочих станций, а также соединяющих их кабелей. Как правило, в подобных сетях передача данных рабочими станциями осуществляется только после того, как будет получен специальный *маркер*, разрешающий это действие. Благодаря этому обстоятельству сети с маркерным методом доступа обладают массой преимуществ по сравнению с сетями, в которых применяется метод конкурентного доступа на основе технологии CSMA/CD.

ПРИМЕЧАНИЕ Следует отметить, что метод маркерного доступа возможен не только в сетях с кольцевой топологией, но и в сетях с шинной топологией, хотя в последнем случае он используется очень редко.

Существуют следующие практические реализации сетей с кольцевой топологией:

- ARCnet;
- AppleTalk;
- TokenRing.

Полносвязная топология

В *полносвязной* топологии каждый сетевой компьютер связан с другим компьютером (рис. 2.5). При этом для связи каждой пары компьютеров используется отдельная линия связи. На практике подобный вариант используется сравнительно редко. Это связано с существенными затратами в связи с большим количеством промежуточных кабелей, а также с затруднениями, появляющимися при изменениях конфигурации или наращивании сети.

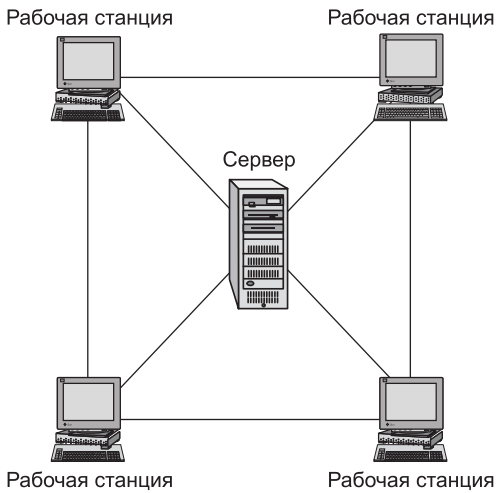


Рис. 2.5. Пример сети с полносвязной топологией

Гибридные топологии

Помимо перечисленных выше «классических» сетевых топологий существует ряд так называемых *гибридных топологий*. Они представляют собой, как правило, комбинации звездообразной и шинной топологий (рис. 2.6). Это весьма практично в том случае, когда проектируется сложная сеть, объединяющая более простые сети. При этом экономически целесообразно формировать простые сети на основе шинной топологии, объединяя их на базе звездообразной топологии.

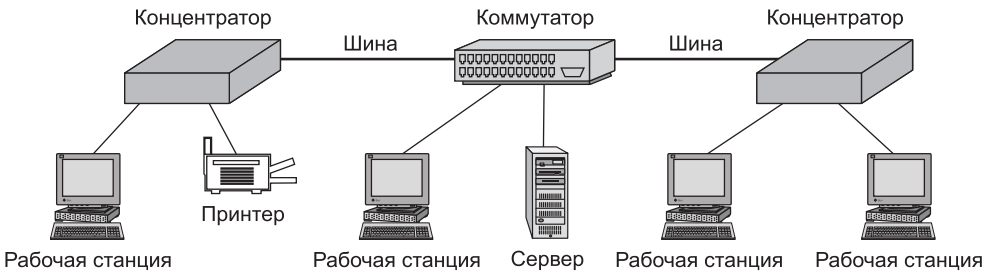


Рис. 2.6. Пример сети, сформированной на основе гибридной топологии

В следующем разделе рассматривается классификация локальных вычислительных сетей в соответствии с применяемой при их формировании архитектурой.

Архитектура локальных вычислительных сетей

В настоящее время используются локальные вычислительные сети, которые делятся на следующие разновидности (в соответствии с применяемой архитектурой):

- ARCnet;
- Token Ring
- Ethernet.

Предметом рассмотрения книги являются сети Ethernet, хотя остальные архитектурные решения также заслуживают краткого рассмотрения.

Сети ARCnet

Трудно предположить, что современному работнику придется столкнуться с этими сетями в реальной жизни, но иметь некоторое представление о них все же полезно.

Сети ARCnet появились в семидесятых годах прошлого века и изначально предназначались для связи между собой промышленного оборудования, а также кассовых терминалов в больших магазинах. Характеризуются высокой степенью надежности, а также устойчивостью к помехам, поэтому иногда применяются до сих пор.

В сетях этого типа управление доступом рабочих станций к сетевому кабелю осуществляется с помощью маркера (как в сетях с кольцевой топологией), хотя фактически используется звездообразная или шинная топология.

Скорость передачи данных в «классической» сети ARCnet составляет 2,5 Мбит/с, что на сегодняшний день не отвечает стандартным ожиданиям пользователей. Но все же существует ряд приложений, для которых скорость передачи данных совершенно не критична.

Каждому узлу в сети ARCnet назначается адрес в восьмеричном формате от 1 до 255. Следовательно, максимальное количество компьютеров в сети ограничивается значением 255. Обход сети маркером осуществляется в порядке возрастания этих адресов, которые назначаются с помощью установки перемычек на сетевых адаптерах ARCnet. Следует уделить особое внимание процессу настройки, поскольку при этом определяется путь прохождения маркера в сети, который может быть оптимальным, а может быть и далеким от оптимального.

Сети ARCnet допускают использование практически любых сетевых кабелей (коаксиальный кабель, витая пара, волоконно-оптический кабель), что является несомненным их преимуществом. К недостаткам можно отнести небольшую скорость передачи данных, а также «экзотичность» применяемого оборудования.

Сети Token Ring

Архитектура сетей Token Ring была разработана компанией IBM в качестве альтернативы сетям Ethernet. Основной отличительной особенностью сетей этого типа является использование *маркерного* метода доступа. Этот метод исключает конфликт между циркулирующими в сети данными. При этом используется кольцевая логическая топология. Физическая же топология сети является звездообразной. Структура сети показана на рис. 2.7.

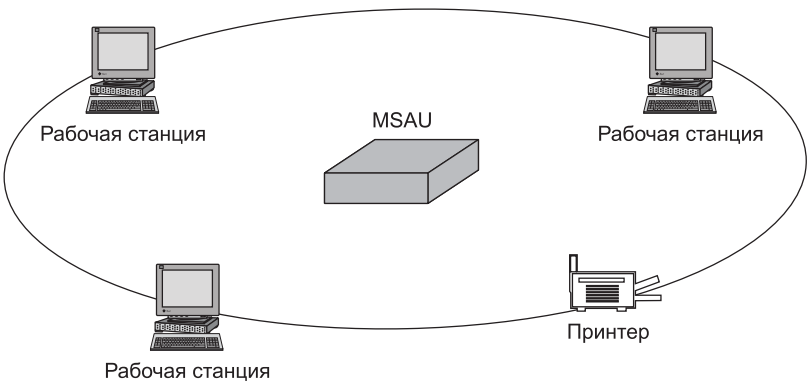


Рис. 2.7. Пример сети Token Ring

Эта сеть характеризуется несколькими базовыми принципами:

- все компьютеры подключены к центральному концентратору, который в данном случае именуется модулем многостанционного доступа (MAU, Multistation Access Unit);

- порты концентратора образуют логическое кольцо, по которому циркулирует маркер;
- используются специальные кабели типа экранированной витой пары.

Передача данных в сетях этого типа осуществляется с помощью *маркера*, который «путешествует» по сети. Как только маркер достигает рабочей станции, готовой передавать данные, производится его перехват данной станцией. При этом в маркер добавляется адрес назначения пакета. Затем маркер и пакет передаются далее по сети. После достижения компьютера, который должен получить пакет, в маркер добавляется подтверждение о получении пакета, а затем передается еще один пакет данных либо сам маркер с отметкой о том, что он не занят. После этого процесс циклически повторяется.

К числу основных преимуществ сетей Token Ring является устойчивость к перегрузкам, при наличии которых наблюдается лишь плавное падение производительности. Поскольку применяемая в этом случае топология является активной, не требуется использование повторителей для усиления сигнала. Серьезным недостатком сетей этого типа является невысокая скорость передачи данных (не более 16 Мбит/с в новейших модификациях), а также достаточно высокие цены на оборудование.

Сети Ethernet

Именно сети этого типа рассматриваются в данной книге. Как упоминалось ранее, таким сетям присуща звездообразная или шинная топология, а доступ рабочих станций к сетевому кабелю обеспечивается с помощью метода множественного доступа с контролем среды и обнаружением конфликтов (CSMA/CD, Carrier Sense Multiple Access Collision Detect). Ниже кратко описан алгоритм, на основе которого функционирует этот метод:

- Проверка сетевой среды. Перед тем как начать передачу данных в сетевой среде, следует узнать, не выполняется ли подобная операция другим компьютером.
- Выполнение множественного доступа. Это означает, что возможен одновременный доступ к сетевой среде для нескольких компьютеров.
- Обнаружение конфликтов. Если в ходе выполнения первого этапа обнаруживается сигнал, передаваемый «чужим» компьютером, передача отменяется. Но может случиться так, что передачу сигналов начнут одновременно два или большее количество компьютеров.
- Ожидание. Для преодоления возникших конфликтов компьютеры «выжидают» на протяжении определенного промежутка времени, заданного случайным образом, а затем повторяют передачу *фреймов* данных. Поскольку вероятность повторного конфликта не столь уж и велика, сохраняется приемлемая производительность при передаче данных в сети.

Существует разновидность метода CSMA/CD, которая называется CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, множественный доступ с контролем среды и предотвращением конфликтов). Этот метод предусматривает не только «прослушивание» сетевой среды, но и передачу специального

сигнала RTS (Request to Send, запрос на передачу). Тем самым объявляется о намерении начать передачу данных. И только после этого начинается фактическая передача данных. Большим преимуществом в этом случае является принципиальная невозможность конфликта между фреймами данных, хотя остается вероятность одновременной передачи сигналов RTS. Но это уже не ведет к столь трагическим последствиям.

Протоколы локальных вычислительных сетей

Локальные вычислительные сети делятся на типы в соответствии с применяемыми ими протоколами. Ниже перечислены основные виды протоколов, используемые в современных сетях.

- NetBEUI. Этот протокол применяется в простых локальных сетях Microsoft Windows, не требующих маршрутизации. В настоящее время практически не используется, хотя в некоторых ситуациях его применение может быть целесообразным.
- IPX/SPX. Этот набор протоколов применяется в сетях NetWare, но может использоваться в сетях Microsoft Windows. В последнем случае повышается степень безопасности локальной сети, поскольку обеспечивается естественная «изоляция» от Интернета.
- TCP/IP. Этот набор протоколов универсален и применяется для обеспечения функционирования как локальных, так и глобальных сетей. Именно ему будет уделяться повышенное внимание в этой книге.

На этом можно завершить краткое рассмотрение видов локальных вычислительных сетей. В следующей главе будут рассмотрены современные высокоскоростные локальные сети, включая их беспроводные варианты.

3 ГЛАВА Физические принципы работы локальных вычислительных сетей

В предыдущей главе уже рассматривались основные топологии сетей Ethernet, теперь же следует рассмотреть законы, на основе которых функционируют сети, относящиеся к этой категории. В этой же главе повышенное внимание будет уделено высокоскоростным кабельным, а также беспроводным сетям. В частности, рассматриваются физические принципы работы беспроводных сетей, а также стандарты беспроводных и кабельных высокоскоростных сетей, применяемых в настоящее время. Подобные сети переживают период бурного развития, в связи с чем представляют большой интерес.

ПРИМЕЧАНИЕ

Разумеется, в настоящее время находится применение и устаревшим сетям. Вряд ли целесообразно модернизировать сеть 10BASE-2, если единственная исполняемая ей функция заключается в том, чтобы передавать текстовые файлы или управляющие сигналы. Свою «нишу» в современном мире занимает и «динозавр» под названием ARCnet — объединение кассовых терминалов в торговом зале супермаркета.

Прежде чем приступить к рассмотрению стандартов высокоскоростных и беспроводных сетей, стоит обратить внимание на организации, занимающиеся разработкой стандартов вообще, и стандартов, имеющих отношение к локальным сетям, в частности.

Законодатели мод в области стандартов

Как известно, любая промышленная технология, получившая широкое распространение, должна быть стандартизирована. Необходимость этого диктуется тем,

что производители оборудования, поддерживающего ту или иную технологию, нуждаются в выработке единого свода правил, определяющего физические характеристики устройств. Тогда любой пользователь сети может быть уверен в том, что приобретенные у различных фирм устройства будут совместимы. Естественно, что вопросами разработки стандартов занимаются специализированные международные организации. Ниже перечислены основные игроки, выступающие на этом поле:

- IEC;
- IEEE;
- IETF;
- ISO;
- ITU.

А теперь посмотрим, что скрывается за этими аббревиатурами.

IEC

Полное название, скрывающееся за этой аббревиатурой, — International Electrotechnical Commission. Вполне естественным выглядит перевод этого названия на русский язык — Международная электротехническая комиссия.

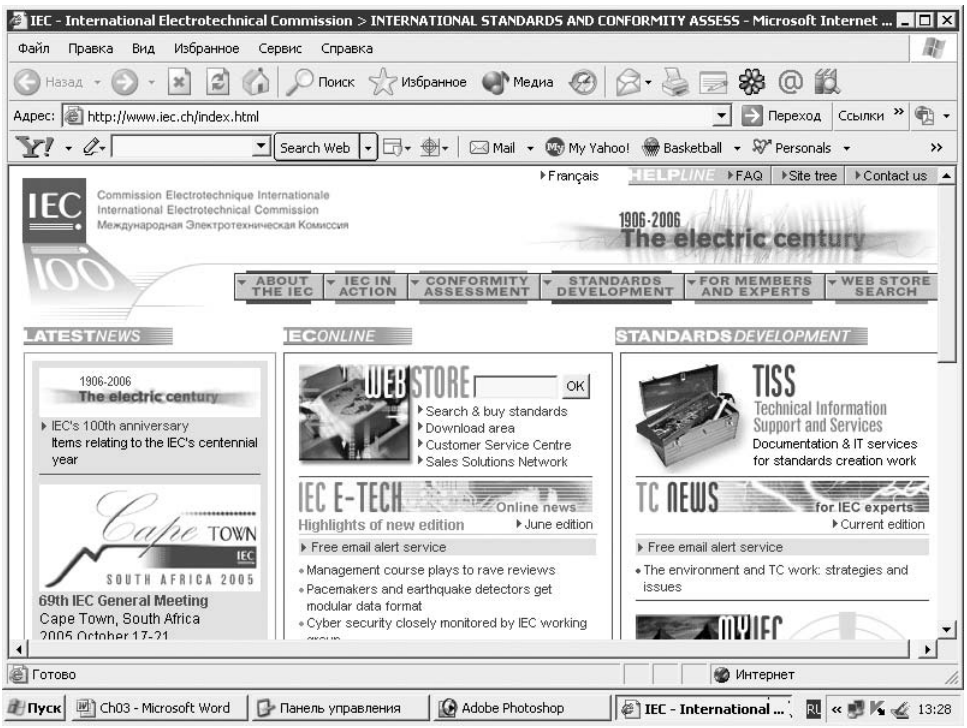


Рис. 3.1. Добро пожаловать в IEC

Эта почтенная организация была основана в фантастически далеком 1906 году, а ее специализацией является разработка и утверждение стандартов в области электротехники. До 1967 года сотрудники этой организации творили в гордом одиночестве, а затем был заключен договор о совместном сотрудничестве с организацией ISO. После этого многие стандарты разрабатываются совместно, а их название приобрело специфический вид, а именно, ISO/IEC. Желающие подробнее ознакомиться со структурой и спецификой деятельности этой организации могут посетить соответствующий веб-сайт, находящийся по адресу www.iec.ch/index.html. На рис. 3.1 показана начальная страница этого веб-сайта.

IEEE

Эта аббревиатура известна многим читателям, имеющим дело с сетевыми технологиями. И расшифровывается она следующим образом — Institute of Electrical and Electronics Engineers (Институт инженеров по электротехнике и электронике). Эта организация имеет непосредственное отношение к разработке стандартов в области сетевых технологий. Ее деятельность началась со стандарта IEEE 802. Смысл этого названия достаточно «прозрачен» (цифра 80 означает год принятия — 1980, а 2 — месяц принятия (февраль)). Далее перечислены основные стандарты локальных сетей, разработанные IEEE.

- 802.1. Вводные замечания. Здесь можно найти описание основ управления сетями различного уровня, описание функционирования сетевых мостов (подуровень MAC) и сведения об алгоритме обхода дерева, при помощи которого предотвращается бесконечное блуждание сигнала в сети.

ПРИМЕЧАНИЕ Не пугайтесь, если некоторые термины из данного перечня покажутся вам незнакомыми. Все они будут подробно объяснены в следующих главах книги.

- 802.2. В этом стандарте описано разделение канального уровня модели OSI с образованием двух подуровней — LLC и MAC.
- 802.3. Данный стандарт описывает метод CSMA/CD (Carrier Sense Multiple Access with Collision Detection, множественный доступ с контролем несущей и разрешением конфликтов). Он обеспечивает полудуплексный режим работы Ethernet. Первая версия этого стандарта предусматривала использование исключительно коаксиального кабеля, последующая редакция предусматривает применение кабеля витой пары (стандарт 10BASE-T).

ПРИМЕЧАНИЕ В новейших высокоскоростных сетях 10 Gigabit Ethernet используется дуплексный режим передачи данных, поэтому необходимость в использовании метода CSMA/CD отсутствует.

- 802.4. С помощью этого стандарта определяется практическая реализация логической и физической топологии на основе волоконно-оптического или коаксиального телевизионного кабеля (с электрическим сопротивлением 75 Ом). Подобная сеть имеет альтернативное название Token Bus, причем предусматривает маркерный метод доступа к среде передачи данных.

- 802.5. Этот стандарт определяет физическую и логическую топологии локальных сетей, реализованных на основе Token Ring. В подобных сетях применяется маркерный метод доступа к сетевой среде, а также кабели неэкранированной и экранированной витых пар.
- 802.6. Данный стандарт описывает сети MAN (Metropolitan Area Network, городские локальные сети). Сети этого типа являются своего рода промежуточным звеном между локальными и глобальными вычислительными сетями.
- 802.7. Под этим названием скрывается группа стандартов, описывающих широкополосные сети. Примером подобной сети является локальная сеть, организованная на основе телевизионного кабеля, когда для одновременной передачи телевизионных и сетевых сигналов применяется методика FDM (Frequency Dividing Multiplexing, мультиплексная передача с частотным разделением каналов).
- 802.8. Данный стандарт описывает волоконно-оптические сети, сформированные на основе волоконно-оптических кабелей. Здесь же описаны сети FDDI (Fiber Distributed Data Interface, Распределенный интерфейс передачи данных по волоконно-оптическим каналам).

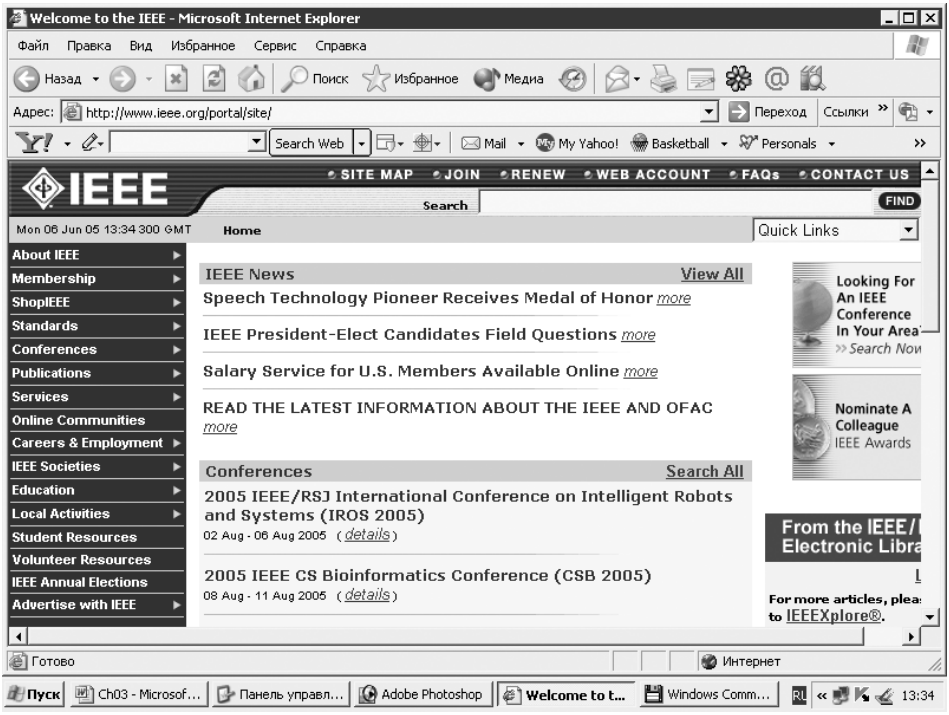


Рис. 3.2. Начальная страница веб-сайта IEEE

- 802.9. Этот документ описывает смешанную передачу голоса и данных по телефонным сетям ISDN (Integrated Services Digital Network, цифровая сеть связи с комплексными услугами).

ПРИМЕЧАНИЕ Стандарты, регламентирующие функционирование сетей ISDN, разрабатываются организацией под названием CCITT.

- 802.10. В этом стандарте описаны методы, применяемые для формирования сетей VPN (Virtual Private Network, виртуальная частная сеть).
- 802.11. Этот документ специфицирует беспроводные сети, в которых для передачи данных вместо кабелей применяются радиоволны и инфракрасные лучи.
- 802.12. В этом стандарте описана технология 100 VG AnyLAN, в которой предусмотрено использование методов доступа к сетевой среде на основе гибридизации существующих методов, применяемых в сетях ATM, Ethernet, Token Ring.

Начальная страница веб-сайта IEEE (www.ieee.org/portal/site/) показана на рис. 3.2.

IETF

Аббревиатура IETF расшифровывается как Internet Engineering Task Force (Проблемная группа проектирования Интернета). В состав этой организации входят разбросанные по всему миру несколько десятков рабочих групп, каждая из которых специализируется на разработке тех или иных технических вопросов, имеющих отношение к функционированию сети Интернет. Все рабочие группы делятся на категории в соответствии с их специализацией. В табл. 3.1. перечислены рабочие группы, занимающиеся разработками в области протоколов Интернета (Internet Area).

Таблица 3.1. Рабочие группы IETF

Название рабочей группы	Область деятельности
6lowpan	Протокол IP версии 6 поверх маломощной WPAN (IPv6 over Low power WPAN)
dhc	Протокол динамической конфигурации узла (Dynamic Host Configuration)
dna	Протокол обнаружения подключения к сети (Detecting Network Attachment)
dnsext	Протокол расширения DNS (DNS Extensions)
eap	Протокол расширенной идентификации (Extensible Authentication Protocol)
hip	Протокол идентичности узла (Host Identity Protocol)
ipdvb	Протокол IP поверх DVB (IP over DVB)
ipoib	Протокол IP поверх InfiniBand (IP over InfiniBand)
iporpr	Протокол IP поверх эластичных пакетных колец (IP over Resilient Packet Rings)
ipv6	Протокол IP версии 6 рабочей группы (IP Version 6 Working Group)
l2tpext	Расширения протокола туннелирования уровня 2 (Layer Two Tunneling Protocol Extensions)
l2vpn	Виртуальные частные сети уровня 2 (Layer 2 Virtual Private Networks)

Название рабочей группы	Область деятельности
l3vpn	Виртуальные частные сети уровня 3 (Layer 3 Virtual Private Networks)
magma	Альтернативное и широковещательное членство в группе (Multicast & Anycast Group Membership)
mip4	Переносимость для IPv4 (Mobility for IPv4)
mip6	Переносимость для IPv6 (Mobility for IPv6)
mipshop	Оптимизация передачи сигналов и автоматизации MIPv6 (MIPv6 Signaling and Handoff Optimization)
nemo	Сетевая переносимость (Network Mobility)
ntp	Протокол сетевого времени (Network Time Protocol)
pana	Протокол переноса идентификации доступа к сети (Protocol for carrying Authentication for Network Access)
pppext	Протокол двухточечного соединения (Point-to-Point Protocol Extensions)
pwe3	Межфронтальная псевдоэмуляция кабеля (Pseudo Wire Emulation Edge to Edge)

Начальная веб-страница IETF (www.ietf.org) показана на рис. 3.3.

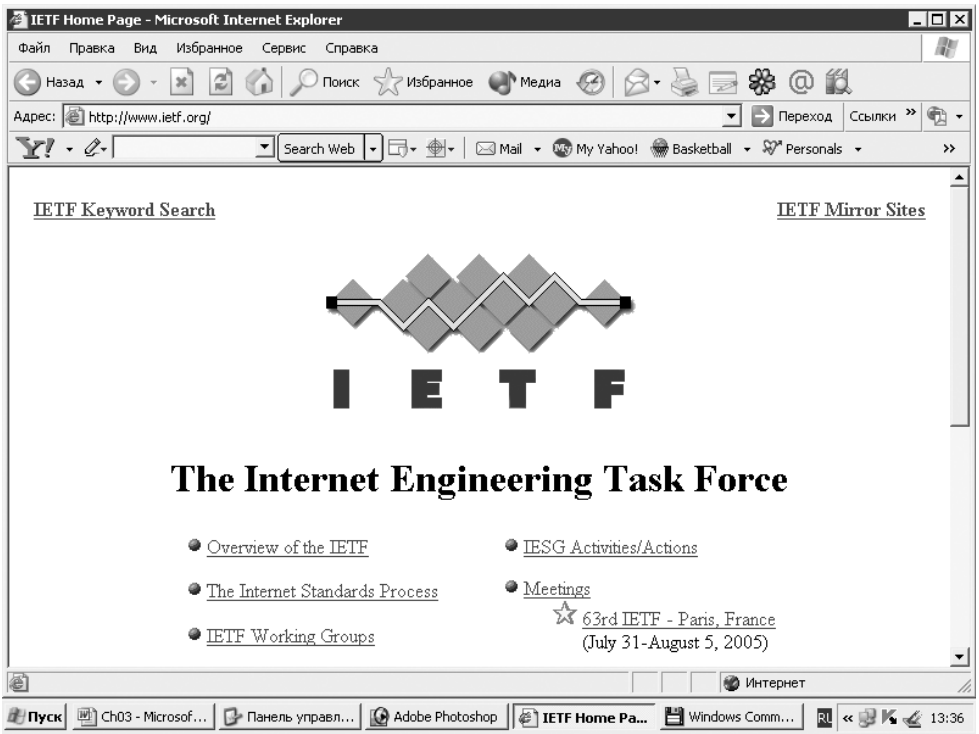


Рис. 3.3. Начальная веб-страница IETF

ISO

Название этой организации знакомо практически каждому, поскольку оно встречается на упаковке товара, если этот товар произведен легально и прошел обязательную процедуру стандартизации. Существует «сверхорганизация», объединяющая все национальные организации, занятые разработкой стандартов. Эта организация и носит имя ISO. Создана она была в 1947 году.

Ранее Советский Союз имел свои стандарты, которые назывались ГОСТами и порой существенно отличались от более жестких международных стандартов. После распада Советского Союза бывшие республики стали активно сотрудничать с иностранными организациями, в связи с чем на повестку дня встал вопрос об использовании международных стандартов ISO.

Естественно, эта организация имеет непосредственное отношение к разработке стандартов локальных вычислительных сетей. Эта деятельность осуществляется в сотрудничестве с такими организациями, как IEC (International Electrotechnical Commission, Международная электротехническая комиссия), ITU (International Telecommunications Union, Международный союз по телекоммуникациям) и WTO (World Trade Organization, Международная торговая организация).

Желающие подробнее ознакомиться со структурой ISO, а также с выполняемыми этой организацией функциями, могут обратиться к ее веб-сайту, который находится по адресу www.iso.org/iso/en/ISOOnline.frontpage.

Рис. 3.4. Начальная страница веб-сайта ISO

ITU

Основная задача этой организации заключается в осуществлении «общего руководства», суть которого заключается в финансовой поддержке международных конференций, разработке и публикации различных документов и стандартов, относящихся к телекоммуникациям. Всем, кто хочет подробнее ознакомиться со структурой этой организации, а также с выполняемыми ею задачами, стоит обратиться к соответствующему веб-сайту (www.itu.int/home), начальная страница которого приведена на рис. 3.5.

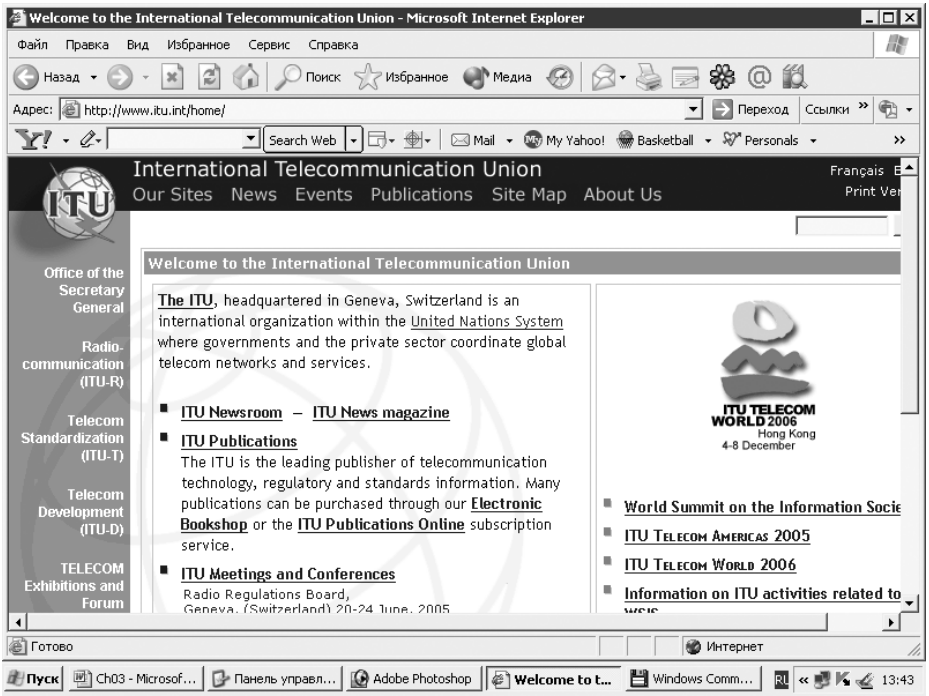


Рис. 3.5. Начальная страница веб-сайта ITU

Физические принципы работы Ethernet

После обзора организаций, разрабатывающих стандарты локальных вычислительных сетей, стоит перейти к рассмотрению физических принципов, на основе которых функционируют эти сети.

Сигналы, циркулирующие в локальных сетях

Передача информации в локальных вычислительных сетях осуществляется с помощью дискретных сигналов — электрических импульсов (при использовании металлических проводников) или вспышек света (при использовании оптоволокна). Передаваемые по кабелям сигналы бывают *аналоговыми* или *цифровыми*.

В первом случае амплитуда сигнала изменяется плавно. Подобные сигналы используются для передачи голоса по линиям обычной телефонной связи. Аналоговый сигнал характеризуется плавным изменением всех присущих ему характеристик. Как правило, на практике применяются три величины, характеризующие подобные сигналы.

- Амплитуда. Модуль значения высоты волны, моделирующей сигнал.
- Частота. Эта величина характеризует количество циклических изменений сигнала за единицу измерения (обычно за 1 секунду). В физике частота электромагнитных колебаний измеряется в герцах (1 Гц = 1 колебание за одну секунду).
- Фаза. Смещение фронта волны, моделирующей электрический импульс. Обычно фаза измеряется в радианах, хотя может применяться традиционный способ измерения угловых величин (в градусах).

ПРИМЕЧАНИЕ

С частотой связана еще одна величина, характеризующая электромагнитные волны — длина. Между длиной и частотой волны существует простое отношение, выражаемое формулой $\lambda = c/\nu$. Здесь λ — длина волны (в метрах), ν — частота электромагнитных колебаний (в герцах), c — скорость распространения света в вакууме ($3 \cdot 10^8$ м/с).

В локальных вычислительных сетях используются цифровые сигналы, изменяющиеся по дискретному закону (0 или 1). Благодаря «цифровой» природе подобные сигналы мало чувствительны к помехам, а также могут легко преобразовываться при помощи простой аппаратуры, реализованной на основе специализированных микросхем.

ПРИМЕЧАНИЕ

Более подробно кабели, применяемые в локальных вычислительных сетях, будут рассмотрены несколько позже.

Структура локальной вычислительной сети

Структура типичной локальной вычислительной сети показана на рис. 3.6. Легко заметить, что ЛВС состоит из *каналов связи*, соединяющих между собой *терминальное оборудование* (Data Terminal Equipment, DTE).

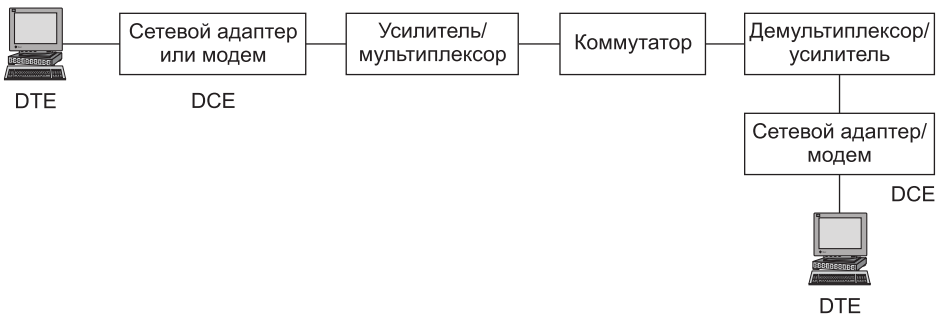


Рис. 3.6. Структура обобщенной вычислительной сети

Канал связи, который также называется *линией связи*, состоит из аппаратных средств, осуществляющих усиление и преобразование электрических сигналов, а также *физической среды*, переносящей информацию. В качестве среды передачи данных применяется электрический кабель (традиционная среда) или электромагнитные волны (инфракрасный и радиодиапазон). В последнем случае говорят о беспроводной локальной сети, которая будет рассматриваться в следующих разделах главы.

Наибольшее распространение в наше время получили кабельные линии связи. Это связано с целым рядом причин, среди которых чаще всего отмечаются относительная дешевизна электрических кабелей, а также их высокая *помехозащищенность* и *пропускная способность* (до 10 Гбит/с).

ПРИМЕЧАНИЕ Подробнее высокоскоростные кабельные сети рассматриваются в следующих разделах этой главы.

Кабели

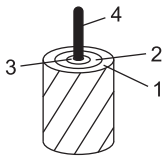
В современных локальных сетях применяются *медные* и *волоконно-оптические* кабели. Названия кабелей показывают, какой материал применяется в качестве проводника, передающего данные. Конечно, помимо данных кабели неизбежно будут передавать так называемый шум (или электромагнитные помехи). На самом деле современные кабели достаточно неплохо защищены от влияния помех, а волоконно-оптические кабели вообще не подвержены влиянию подобных помех.

Любой сетевой кабель характеризуется целым набором электрических параметров, наиболее важные из которых приводятся в следующем перечне.

- Активное сопротивление. В данном случае рассматривается сопротивление постоянному току, присущее любой проводящей среде. Этот вид сопротивления определяется материалом кабеля, а также его геометрическими размерами (длина и диаметр). Активное сопротивление не зависит от характеристик передаваемого сигнала.
- Емкостное (волновое) сопротивление. Этот вид сопротивления зависит от частоты передаваемого сигнала. С ростом частоты увеличивается емкостная составляющая сопротивления. Этот параметр зависит от такой важной характеристики кабеля, как собственная емкость.
- Импеданс. Эта величина рассчитывается как сумма активного и пассивного сопротивлений. При не слишком больших значениях частоты (менее 100 МГц) величина импеданса является относительно постоянной и зависит исключительно от применяемого кабеля. Так, для коаксиальных кабелей величина импеданса составляет около 50 Ом. Для сравнения стоит отметить, что величина импеданса для телевизионного кабеля равна 75 Ом. Поэтому, несмотря на внешнюю схожесть, телевизионный кабель и коаксиальный кабель, применяемый в сетях Ethernet, не являются взаимозаменяемыми.
- Затухание. Под затуханием понимается ослабление сигнала в процессе его передачи по кабелю. Величина затухания оценивается в децибелах на метр (дБ/м).

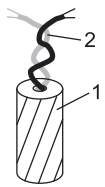
- Перекрестные помехи на ближнем конце (NEXT, Near End Cross Talk). Этот показатель может варьироваться в зависимости от частоты передаваемого сигнала и измеряется в децибелах.

Медные сетевые кабели бывают коаксиальными (рис. 3.7) и основанными на витой паре (рис. 3.8).



1. Внешняя изоляция
2. Экран
3. Изоляция центральной жилы
4. Центральная жила

Рис. 3.7. Коаксиальный кабель в разрезе



1. Изоляция
2. Двужильные кабели витой пары

Рис. 3.8. Структура кабеля витой пары

Коаксиальные кабели применяются для распространения телевизионных сигналов, а также в устаревших разновидностях сетей Ethernet (10BASE-2, 10BASE-5). Недостатки подобных сетей связаны, прежде всего, с достаточно большим весом кабелей и совершенно недостаточной по современным меркам пропускной способностью.

В следующем списке приводятся основные типы применяемых на сегодняшний день коаксиальных кабелей.

- «Толстый» коаксиальный кабель (10BASE-5). Альтернативное обозначение — RG-8, RG-11. Импеданс кабелей этого типа равен 50 Ом, диаметр составляет около 0,5 дюйма. Благодаря достаточно большому диаметру токопроводящих жил этот кабель обладает очень небольшим затуханием (не более 18 дБ/км на частоте 100 МГц). Основной недостаток этого кабеля заключается в трудности монтажа из-за его повышенной жесткости.
- «Тонкий» коаксиальный кабель (10BASE-2). Альтернативное обозначение — RG-58/U, RG-58 A/U и RG-58 C/U. Несомненным преимуществом кабелей этого типа является простота монтажа, а также повышенная гибкость, облегчающая его прокладку в труднодоступных местах. По сравнению с «толстым» кабелем он обладает большим импедансом, из-за чего максимальная длина сегментов составляет всего 185 метров. А у предыдущей разновидности кабеля длина сегмента может достигать 500 метров. Именно этот тип кабеля получил наибольшее распространение в сетях Ethernet, применяющих коаксиальный кабель.
- Кабель для сетей ARCNet с импедансом 93 Ом (альтернативное обозначение — RG-62). Этот кабель практически не применяется, поскольку область распространения сетей ARCNet в настоящее время очень мала.

Следующим шагом вперед явилось появление *кабелей витой пары*, которые представляют собой скрученную специальным образом пару проводов (с внешним экраном или без него). Благодаря скрутке практически устраняется эффект влияния внешних электромагнитных помех. Все кабели неэкранированных витых пар делятся на категории в зависимости от пропускной способности.

- Первая категория. Применяется в телефонных сетях общего применения (ТСОП) исключительно для передачи речи. В настоящее время даже для этих целей используются кабели с лучшими частотными характеристиками. Его можно применять для передачи данных, но предельная пропускная способность в этом случае не превысит 20 Кбит/с.
- Вторая категория. Эти кабели обеспечивают скорость передачи данных, не превышающую 4 Мбит/с. Они были разработаны фирмой IBM и применялись в ее собственных сетях.
- Третья категория. Кабели этого типа появились в 1991 году и обеспечивают передачу данных с максимальной скоростью до 16 Мбит/с. Основная область их применения — передача данных и голоса.
- Четвертая категория. Кабели этого типа представляют собой усовершенствованный вариант кабелей третьей категории и позволяют передавать данные со скоростью до 20 Мбит/с. Они обеспечивают лучшую помехозащищенность и меньшее затухание сигнала. Так, предельная длина сегмента кабеля витой пары может составлять до 135 метров вместо 100 метров, которые обеспечивают кабели третьей категории. Кабели четвертой категории применяются в сетях Token Ring.
- Пятая категория в настоящее время является наиболее популярной. Пропускная способность кабелей пятой категории варьируется от 100 Мбит/с до 1 Гбит/с. Этот параметр зависит от производителя. Область применения подобных кабелей — сети Fast Ethernet (100 Мбит/с), FDDI, 100VG-AnyLAN, ATM (155 Мбит/с), а также Gigabit Ethernet.
- Шестая и седьмая категории. Кабели, относящиеся к этим категориям, обеспечивают скорость передачи данных от 1 Гбит/с. Область их применения — сети Gigabit Ethernet. Следует обратить внимание на то, что кабели седьмой категории выполняются в экранированном исполнении.

Кабели экранированной витой пары (STP) отличаются от кабелей неэкранированной витой пары наличием *экрана*, благодаря которому в значительной степени уменьшается электромагнитное излучение во внешнюю среду. Следует обратить внимание на то обстоятельство, что экран требует качественного *заземления*, иначе его эффективность резко уменьшается.

ВНИМАНИЕ Волновое сопротивление кабеля экранированной витой пары примерно в полтора раза превышает этот показатель для кабеля неэкранированной витой пары. Причина этого явления связана с влиянием дополнительной емкости, образуемой экраном. Именно по этой причине кабели STP и UTP не являются взаимозаменяемыми, что и следует учитывать при выполнении модернизации ЛВС.

В настоящее время все большее количество высокоскоростных сетей реализуется на основе волоконно-оптического волокна. Во второй главе уже упоминались стандарты сетей, реализованных на основе оптического волокна (рис. 3.9). Как правило, волоконно-оптические сети обеспечивают большую скорость передачи, чем сети, созданные на основе металлических кабелей, даже если в качестве проводника применяется медь. Причина этого явления заключается в том, что световой луч, применяемый в качестве носителя данных, обладает огромной информационной емкостью.

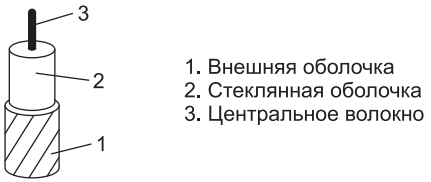


Рис. 3.9. Волоконно-оптический кабель в разрезе

Благодаря использованию оптоволокна достигается следующие преимущества.

- Возрастает степень защиты передаваемых данных, поскольку излучение света не сопровождается электромагнитными наводками, которые легко перехватить при помощи специального оборудования. Нелегальная врезка к такому кабелю тоже весьма затруднена.
- Поскольку оптическое волокно обладает большой степенью прозрачности, то затухание сигнала происходит очень медленно. Поэтому возможна передача сигнала без дополнительного его усиления на расстояние более двух километров.

Все волоконно-оптические кабели делятся на две большие группы. Различают *одномодовые* и *многомодовые* кабели. Кабели первого типа обычно состоят из единственного световода (оптоволокна), по которому параллельно оси этого волокна распространяется световой луч. При этом применяется волокно, диаметр которого соизмерим с длиной световой волны (5–10 мкм). Это обеспечивает большую скорость передачи данных (до 10 Гбит/с), а также позволяет использовать более короткие световые импульсы.

В качестве источников световых импульсов, передаваемых одномодовым оптоволокном, используются полупроводниковые лазеры. Это связано с тем, что при использовании иных источников светового излучения очень трудно сфокусировать световой луч и направить его по оптоволокну столь малого диаметра. Основной недостаток одномодовых кабелей заключается в достаточно большой их стоимости, связанной с трудностями изготовления оптоволокна с малым поперечным сечением.

Если волоконно-оптический кабель состоит из нескольких волокон, он обычно работает в многомодовом режиме. Это позволяет передавать несколько световых импульсов одновременно по каждому волокну или даже несколько импульсов по одному волокну. Волокна, образующие многомодовый кабель, обычно имеют диаметр 62,5 (125 мкм), где первый показатель характеризует центральное волокно, а второй показатель — внешнее волокно. В качестве источника света в этом случае применяется полупроводниковый лазер. Основной недостаток

многомодового волоконно-оптического кабеля обусловлен меньшей полосой пропускания из-за дополнительных потерь энергии светового излучения, связанных с интерференцией, а также с отражениями.

Передача данных по волоконно-оптическим кабелям осуществляется с использованием длин волн 0,85 мкм, 1,3 мкм и 1,55 мкм. Легко заметить, что рабочая область этих кабелей находится в ближнем и дальнем инфракрасном диапазонах. Полупроводниковые светодиоды способны излучать свет с длиной волны 0,85 и 1,3 мкм. Полупроводниковые лазеры — 1,3 и 1,55 мкм соответственно.

ПРИМЕЧАНИЕ У читателя может возникнуть закономерный вопрос о том, почему используются именно указанные длины волн. На самом деле этот выбор не случаен и обусловлен тем, что именно эти волны этих длин меньше всего затухают в процессе передачи по оптоволокну.

Теоретические принципы работы локальных сетей

Как известно, именно Ethernet на сегодняшний день является наиболее распространенным типом сетей. Подобная популярность объясняется распространенностью соответствующего сетевого оборудования, а также достаточно высокой надежностью и скоростью передачи данных.

Начать стоит с рассмотрения модели OSI, описание которой стало правилом «хорошего тона» во всех книгах, посвященных описанию сетевых технологий.

Модель OSI

С момента выхода на арену локальных вычислительных сетей предпринимались попытки стандартизации процесса разработки локальных сетей. Эти попытки увенчались успехом в начале восьмидесятых годов прошлого века, когда на свет появилась модель OSI (Open System Interconnection, модель взаимодействия открытых систем). В условиях этой модели взаимодействующие сетевые устройства относят к семи уровням. Различают *физический*, *канальный*, *сетевой*, *транспортный* уровни, уровни *сеанса* и *представления* и *прикладной* уровень (рис. 3.10).

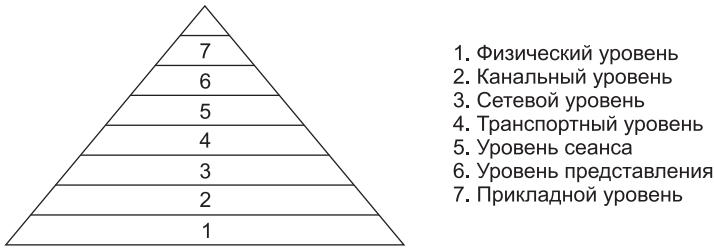


Рис. 3.10. Семь уровней модели OSI

Физический уровень

На этом уровне осуществляется фактическая передача битов и байтов данных через сетевые среды, будь то коаксиальный/волоконно-оптический кабель, витая пара или радиоканал. Именно на этом уровне рассматриваются такие характеристики сред передачи данных, как волновое сопротивление, скорость передачи данных и величина затухания сигнала и т. д.

Присущие этому уровню функции выполняются всеми сетевыми устройствами (сетевая карта, последовательный порт, мост). Протоколы физического уровня определяют на уровне «битов и байтов» передачу сигналов по средам передачи данных. Примером такого протокола может служить Fast Ethernet (100BASE-T), определяющий использование кабеля неэкранированной витой пары категории 5 с волновым сопротивлением 100 Ом и предельной длиной одного сегмента 100 метров.

ПРИМЕЧАНИЕ Подробнее физические характеристики сетевых кабелей будут рассматриваться несколько позднее.

Канальный уровень

Как упоминалось ранее, физический уровень несет ответственность за транспортировку битов, а доступом к среде передачи данных занимается следующий, *канальный уровень* (Data Link Layer). Функция этого уровня заключается в обнаружении и коррекции ошибок. Биты данных организованы на этом уровне в виде *фреймов*, причем для контроля корректности при передаче применяется проверка соответствия контрольной суммы. Если контрольная сумма для принятого фрейма не совпадает с контрольной суммой, указанной отправителем, то этот фрейм передается повторно. К протоколам канального уровня можно отнести Ethernet, FDDI, Token Ring.

Сетевой уровень

В обязанности *сетевого уровня* входит доставка данных между различными сетями. Практическая реализация этой функции относится к компетенции *маршрутизаторов*.

ПРИМЕЧАНИЕ Подробнее маршрутизаторы рассматриваются в четвертой главе, посвященной различным сетевым компонентам.

На этом же уровне реализуется передача данных между разнородными локальными вычислительными сетями и упрощенная схема адресации в сетях.

Данные, имеющие отношение к этому уровню, называются *пакетами*. Примерами протоколов этого уровня могут служить протокол определения адресов (ARP, Address Resolution Protocol), протокол маршрутизации, а также протокол IP, являющийся основой набора протоколов TCP/IP.

Транспортный уровень

Как и следует из его названия, этот уровень несет всю полноту ответственности за доставку данных в сети, которые на длинном пути между отправителем и получателем могут быть повреждены или вообще потеряны. Именно этот уровень создает надежное соединение, обеспечивающее передачу данных верхним уровням модели OSI (приложений и сеанса). На этом уровне определяются пять классов обслуживания. Поддерживаются обнаружение и коррекция ошибок при передаче данных, срочность предоставляемых услуг, возможность восстановления ранее прерванной связи, мультиплексирование нескольких установленных ранее соединений.

«Прозрачным» примером протокола транспортного уровня может служить протокол TCP/IP, входящий в стек протоколов TCP/IP, а также протокол передачи пользовательских дейтаграмм (UDP, User Datagram Protocol).

Уровень сеанса

И снова название уровня говорит само за себя. На этом уровне обеспечивается установка сеанса связи между сетевыми станциями. Данный уровень достаточно редко выделяется и обычно реализуется в составе прикладного уровня.

Уровень представления

На этом уровне реализуется представление данных, передаваемых по локальной сети. В данном случае имеется в виду внешняя форма, а не содержание информации. Благодаря этому уровню достигается «понятность» информации, передаваемой между прикладными уровнями взаимодействующих между собой систем. Именно на уровне представления реализовано шифрование/дешифрование данных и функционируют такие протоколы, как, например, IPSec.

Прикладной уровень

Фактически, этот уровень является набором протоколов, обеспечивающих доступ сетевым пользователям к различным совместно используемым ресурсам. Протоколы обмениваются информацией между собой при помощи рассылки различных *сообщений*. Подобных протоколов на сегодняшний день существует очень много. К этому семейству относятся такие протоколы, как FTP и TFTP.

Функционирование сетей Ethernet определяется стандартом IEEE 802.3, в котором определялись модификации 10BASE-2, 10BASE-5, 10BASE-T, 10BASE-FB и 10BASE-FL. Обо всех этих разновидностях локальных сетей уже упоминалось во второй главе. В 1995 году этот стандарт был дополнен разделом (IEEE 802.3u), в котором описывается функционирование сетей Fast Ethernet (скорость передачи данных до 100 Мбит/с). В 1998 году появился стандарт (IEEE 802.3z), в котором описывается функционирование сетей Gigabit Ethernet. В сетях Ethernet, включая модификации Fast Ethernet и Gigabit Ethernet, но исключая 10 Gigabit Ethernet применяется метод доступа к общей сетевой среде, называемый CSMA/CD. Этот метод иногда шутливо называют «разделяй и властвуй». Его следует рассмотреть подробнее.

Как избежать конфликтов в сетях Ethernet?

В сетях с общей шиной, к которым относится Ethernet, неизбежно возникают *конфликты*. Причина их в данном случае стара как мир — единая среда передачи данных и огромное количество рабочих станций и другого сетевого оборудования, которые пытаются получить доступ к этой среде в совершенно непредсказуемые моменты времени. Что же делать в подобной неприятной ситуации? Выход напрашивается сам собой — поставить «диспетчера», который будет управлять доступом к единой среде передачи данных. В сетях Ethernet роль подобного «диспетчера» исполняет метод CSMA/CD (Carrier Sense Multiple Access with Collision Detection, множественный доступ с контролем несущей и обнаружением конфликтов).

Данные, циркулирующие в сетях Ethernet, помещаются во *фреймы*. В настоящее время применяются четыре вида фреймов Ethernet, что связано с достаточно длительной историей развития сетей этого типа. Подробнее фреймы будут рассмотрены чуть позже, а сейчас стоит остановиться подробнее на описании этапов доступа к сетевой среде передачи данных.

1. Сначала рабочая станция, которая собирается передать сигнал, выполняет «прослушивание» сетевой среды в целях обнаружения несущей частоты, при обнаружении которой, делается пауза на некоторый период времени, после чего предпринимается повторная попытка передачи данных.
2. Если несущая в общей сетевой среде не обнаружена, то станция начинает передачу сетевого фрейма. В начале каждого сетевого фрейма находится раздел, называемый преамбулой, длина которого составляет 64 бита (8 октетов). Этот раздел позволяет обеспечивать синхронизацию между передающей и приемными станциями.
3. В состав фрейма включен адрес станции назначения.
4. После получения фрейма посылается ответный фрейм, подтверждающий факт получения данных.

В идеале все выглядит достаточно просто. Но, как известно, наш мир весьма далек от идеала, поэтому в процессе передачи данных одной станцией вполне вероятна ситуация, когда эту же операцию пытается осуществить другая станция. Или даже передача сигнала может начинаться второй станцией чуть позднее, но из-за конечной скорости распространения электрических сигналов по кабелям локальной сети может возникнуть ситуация, когда сигнал уже отправлен первой станцией, но до второй станции он просто еще не дошел. Вне зависимости от причины при «столкновении» нескольких сигналов порождается конфликт, называемый *коллизией*, в результате которого серьезно искажается форма сигналов, из-за чего их распознавание становится невозможным.

Но не все так уж плохо. Ведь метод CSMA/CD предусматривает обнаружение подобных конфликтов. Суть этого метода заключается в том, что во время передачи данных рабочей станцией одновременно «прослушивается» сетевая среда для обнаружения несущей частоты, сопровождающей передачу данных другой рабочей станцией. Если подобная несущая обнаружена, передача данных немедленно прекращается и пересылается служебная последовательность, состоящая

из четырех октетов. После некоторой паузы посылка данных повторяется. Если и в этот раз обнаруживается состояние конфликта, снова наступает состояние паузы, длительность которой увеличивается в два раза. И так далее, пока сигнал не будет передан.

Используемый при этом алгоритм называется *алгоритмом двойного экспоненциального отката* (binary exponential backoff). Благодаря его применению обеспечивается передача. Если конфликты возникают слишком часто, следует уменьшить загрузку локальной сети, сократив величину трафика или уменьшив количество рабочих станций, подключенных к сегменту. Еще одним вариантом решения проблемы может быть переход на более скоростную версию Ethernet.

Необходимое условие бесперебойного функционирования Ethernet заключается в однозначном обнаружении сетевых конфликтов всеми станциями, подключенными к сети. Если конфликт не будет обнаружен вовремя, то фрейм данных, переданный сетевой станцией, будет утерян безвозвратно, поскольку контрольная сумма перестанет соответствовать изначально заявленной. В этом случае за дело возьмется сетевой протокол более высокого уровня, и требуемая информация, скорее всего, будет восстановлена. Но при этом возникает неизбежная задержка, время которой будет составлять несколько секунд. А при корректном распознавании конфликтов задержка исчисляется микросекундами. Поэтому в том случае, когда конфликты не будут гарантированно определяться станциями, подключенными к сегменту сети Ethernet, произойдет серьезное снижение производительности сети в целом.

Гарантированное распознавание конфликтов в сети возможно, только если время передачи фрейма минимальной длины превышает время, требуемое для передачи сигнала о конфликте наиболее удаленной сетевой станции. Если это условие выполняется, передающая станция в состоянии обнаружить конфликт, возникновение которого связано с передаваемым ею фреймом. Выполнение этого условия во многом зависит от длины минимального фрейма Ethernet, а также от размеров сетевых кабелей и скорости распространения электрических сигналов по кабелю. Значение этой скорости зависит от типа применяемого кабеля.

При разработке стандарта Ethernet учитывались условия, требуемые для распознавания возникающих в локальной сети конфликтов. При этом минимальная длина раздела данных фрейма составляет 46 байт. Учитывая разделы служебных данных, можно получить значение длины фрейма, равное 64 байтам. Если добавить длину раздела преамбулы, то величина фрейма составит 72 байта. Используя это значение, можно определить предельное расстояние между сетевыми станциями.

Предположим, что в нашем распоряжении имеется сеть 10BASE-5, скорость передачи данных в которой равна 10 Мбит/с. При этом время, затрачиваемое на передачу фрейма минимальной длины, составляет 57,5 мкс ($575/10 \cdot 10^6$). Если применяется «толстый» коаксиальный кабель, то предельное расстояние, на которое распространяется сигнал, составляет около 13 000 м. Это расстояние рассчитывается исходя из свойств материала и геометрических размеров кабеля. Поскольку в наших расчетах учитывается время, требуемое на передачу и получение сигнала, эту величину следует уменьшить в два раза, в результате чего будет получено значение, равное 6500 м. Следует отметить, что в документах,

описывающих стандарт 10BASE-5, задается более серьезное ограничение. Это происходит из-за того, что необходимо учитывать предельно допустимое затухание полезного сигнала. Именно исходя из этих соображений максимальная длина сегмента кабеля 10BASE-5 выбирается равной пятистам метрам.

Разумеется, эта величина выбрана с определенным запасом, но тут имеется в виду возможность создания составных сетей, сконструированных на основе нескольких сегментов, соединенных повторителями. Этим устройства увеличивают мощность передаваемых между сегментами сигналов, благодаря чему можно построить мультисегментную сеть, обладающую значительной длиной. Для сетей стандарта 10BASE-5 максимальное количество сегментов ограничено пятью, а поскольку длина каждого из них составляет 500 метров, общая длина сети не превышает 2500 метров. Даже в такой мультисегментной сети условие обнаружения конфликтов выполняется с большим запасом, поскольку эта величина существенно меньше ранее определенного предельного значения, равного 6500 метрам. Реальная избыточность в данном случае будет несколько меньшей, поскольку повторителями вносятся искажения, а физические параметры кабеля и прочих сетевых устройств отклоняются от идеальных физических характеристик.

ПРИМЕЧАНИЕ Предельный размер сети, вычисленный на основе характеристик кабеля и скорости передачи данных по ней, называется диаметром сети. Методики, применяемые для определения этого показателя, подробно рассматриваются в пятой главе.

В новых более скоростных версиях Ethernet (Fast Ethernet и Gigabit Ethernet) из-за большей скорости передачи фреймов уменьшается предельно допустимое расстояние между рабочими сетевыми станциями. Так, например, в сети Fast Ethernet эта величина равна 210 метрам, а в стандарте Gigabit Ethernet (по крайней мере, в его «медной» разновидности) не превышает 25 метров.

Оценка пиковой производительности Ethernet

Иногда бывает полезным знать «идеальную» пропускную способность сети Ethernet, когда отсутствует влияние дополнительных сетевых устройств и на быстродействии не сказываются конфликты. Это полезно на практике, когда требуется оценить максимальную производительность, требуемую от устройств, приобретаемых в целях модернизации существующей или прокладки новой сети.

Для сетевых компонентов критически важным показателем является скорость обработки сетевых фреймов, имеющих наименьшую длину. Это связано с тем, что накладные расходы, связанные с обработкой подобных фреймов, будут такими же, как и при обработке фреймов большей длины, а частота следования первых будет значительно выше.

Используя характеристики уровня MAC Ethernet, можно рассчитать максимальную пропускную способность сегмента сети Ethernet. Ранее уже упоминалось о том, что минимальная длина фрейма Ethernet равна 576 битам. Соответственно, в сети 10BASE-5 на его передачу уходит 57,5 мкс. Промежуток между фреймами составляет 9,6 мкс, поэтому передача фрейма вместе с промежутком занимает 67,1 мкс.

Выполнив несложные математические вычисления, можно получить максимальную пропускную способность сегмента сети Ethernet для фреймов минимальной длины, которая будет составлять 14 880 фреймов/с.

Естественно, подключение к сегменту нескольких рабочих станций приводит к уменьшению этого показателя из-за того, что станции ожидают доступа к общей сетевой среде, а также по причине возникающих конфликтов, инициирующих повторную передачу фреймов.

Теперь подсчитаем максимальную скорость передачи данных в случае использования фреймов максимальной длины. Известно, что длина подобных фреймов составляет 1526 байт (включая преамбулу), что составляет 12 208 бит. Время, затрачиваемое на передачу такого фрейма (вместе с промежутком между фреймами), составляет 1221,9 мкс, а пропускная способность сети составляет 818 фреймов/с. Как видите, при обработке фреймов максимальной длины потенциальные возможности сети в значительной степени не используются.

На практике также применяется показатель, называемый полезной скоростью передачи данных в сети. При его расчете используют сведения о длине раздела данных фрейма, а также показатель максимальной скорости передачи данных в сети.

Для начала рассчитаем полезную скорость передачи данных в случае фреймов минимальной длины. В этом случае длина раздела данных составляет 46 байт, а показатель максимальной скорости передачи данных — 14 880 бит/с. Следовательно, величина полезной скорости передачи данных рассчитывается следующим образом: $14\,880 \cdot 46 \cdot 8$, что составляет 5,476 Мбит/с.

Полезная скорость передачи данных в случае фреймов максимальной длины рассчитывается по формуле $818 \cdot 1500 \cdot 8 = 9{,}816$ Мбит/с.

В первом случае наблюдается явная «недогрузка» локальной сети, а во втором случае полезная скорость передачи данных практически равна максимальной скорости передачи данных.

Существует еще один важный показатель, характеризующий локальную сеть, — *коэффициент утилизации сети*. Он рассчитывается как отношение текущей скорости передачи данных к максимально возможной скорости передачи данных в этой сети. Чем больше значение этого показателя, тем меньше «запас прочности» сети, т. е. устойчивость к конфликтам.

Структура фреймов Ethernet

Необходимо подробнее рассмотреть структуру единиц информации, переносимой сетями Ethernet, а именно, фреймов Ethernet.

В документе IEEE 802.3, описывающем стандарт Ethernet, приводится структура единственного формата фрейма, относящегося к MAC-уровню. Поскольку фрейм этого уровня включает в себя фреймы, имеющие отношение к уровню LLC (описывается в стандарте IEEE 802.2), то, в соответствии со стандартами IEEE, в сетях Ethernet допускается применение фрейма канального уровня единственного типа. Причем его заголовок представляет собой своего рода симбиоз между заголовками, имеющими отношение к заголовкам на подуровнях MAC и LLC.

Однако на практике все выглядит несколько иначе. Фактически в сетях Ethernet применяются фреймы четырех различных типов. Отчасти это объясняется тяжелым наследием длительного периода эволюции сетей Ethernet.

Еще в 1980 году консорциум, образованный фирмами Digital, Intel и Xerox (DIX), предложил собственный вариант стандарта Ethernet, в котором был описан новый вариант формата фрейма. В свою очередь, комитет 802.3 принял собственный вариант стандарта, подразумевающий иной формат фрейма. Третий вариант фрейма был разработан фирмой Novell, а четвертый вариант появился в ходе разработки комитетом 802.2 некоего «общего знаменателя», обобщающего выполненные ранее разработки.

Описанные различия в форматах фреймов могут привести к появлению сбоев в процессе функционирования различных сетевых аппаратных и программных средств, ориентированных на единственный стандартный фрейм Ethernet. Но это было в прошлом. В настоящее время практически все сетевые карты, повторители, коммутаторы и другие сетевые средства могут адекватно реагировать на все форматы фреймов Ethernet, поскольку идентификация фрейма выполняется в автоматическом режиме.

Итак, в настоящее время в сетях Ethernet используются фреймы следующих четырех типов:

- Ethernet 802.2;
- Ethernet 802.3;
- Ethernet II, называемый также Ethernet DIX;
- Ethernet SNAP (версия от фирмы Novell).

Для примера стоит рассмотреть заголовок фрейма 802.3 (рис. 3.11). Фреймы остальных четырех типов имеют схожую структуру.

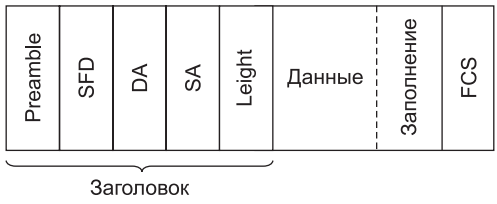


Рис. 3.11. Структура фрейма 802.3/LLC

- Поле Preamble (преамбула). Включает семь байтов вида 10101010, которые требуются для синхронизации.
- Поле SFD (Start of frame delimiter, начальный ограничитель фрейма). Включает один байт вида 10101011. Эта последовательность битов является указанием на то, что следующий байт будет первым байтом заголовка кадра.
- Поле DA (Destination Address, адрес назначения). Это поле определяет адрес узла в сети, которому передается фрейм. Как правило, размер этого поля составляет 6 байт. Первый бит старшего байта в этом поле определяет тип адреса. Может использоваться как однонаправленный адрес (unicast), так и групповой

(multicast). Первый тип адреса определяется нулевым битом, а для второго типа адреса этому биту присваивается единица. Групповой адрес определяет пересылку данных всем узлам сети или же определенным сетевым узлам.

- Поле SA (Source Address, исходный адрес). В этом поле задается адрес сетевого узла, отправляющего фрейм. Для этого типа адреса первый бит всегда имеет нулевое значение.
- Поле Length (длина). В этом двухбайтовом поле определяется длина поля данных для текущего фрейма.
- Поле Data (данные). Размер этого поля может варьироваться от 0 до 1500 байт. В том случае, когда длина этого поля не превышает 46 байт, используется поле заполнения с тем, чтобы длина поля данных соответствовала минимально допустимому значению 46 байт.
- Поле Padding (заполнение). Это поле позволяет дополнить поле данных до значения 46 байт. Выполнение этого условия необходимо в целях корректного функционирования механизма, ответственного за обнаружение конфликтов в сетях Ethernet. Это поле используется в том случае, когда длина поля данных меньше 46 байтов.
- Поле FCS (Frame Check Sequence, контрольная сумма). Это поле включает 4 байта контрольной суммы, вычисляемой в соответствии с алгоритмом CRC-32. Значение контрольной суммы вычисляется повторно непосредственно после получения фрейма станцией, адрес которой указан в поле адреса назначения.

На этом можно завершить краткое введение в теорию сетей Ethernet и перейти к рассмотрению «скоростной» версии этих сетей — 10 Gigabit Ethernet.

Сегодня в моде ускорение — 10 Gigabit Ethernet

Наиболее интересная особенность стандарта IEEE 802.3ae, описывающего сети 10 Gigabit Ethernet, заключается в том, что его изначально предполагалось его использовать не в тесных рамках локальных сетей, а в глобальных сетях. Несмотря на это структура фрейма, циркулирующего в этих сетях, идентична структуре фрейма для обычных сетей Ethernet.

Наиболее революционное изменение, касающееся этих сетей, заключается в полном отказе от использования метода CSMA/CD. Это достигается при помощи полнодуплексного режима, в котором работают сети 10 Gigabit Ethernet. Еще одно радикальное изменение заключается в том, что в этих скоростных сетях применяется только оптоволокно. Различные виды оптоволокна описываются стандартами 10GBASE-LR, 10GBASE-ER, 10GBASE-SR, 10GBASE-LW и 10GBASE-LX4. Отказ от использования медного кабеля связан с его плохими частотными характеристиками при работе на таких скоростях.

Применяемые в этом случае физические интерфейсы используют два уровня: PCS (Physical Coding Sublayer, подуровень физического шифрования), отвечаю-

щий за управление передаваемыми битовыми последовательностями, и PMD (Physical Media Dependent, зависимый от физической среды). Последний уровень выполняет преобразование последовательностей битов в сигналы, передаваемые по оптоволокну. Перечисленные уровни спроектированы таким образом, что не зависят друг от друга.

Как упоминалось ранее, для сетей Ethernet (Fast Ethrernet и Gigabit Ethernet) использовались два типа стандартизованных оптических интерфейсов, подразумевающие применение одномодового или многомодового оптоволокна. В сетях 10 Gigabit Ethernet предусматривается использование трех различных длин световых волн (850, 1310 и 1550 нм), причем каждой волне соответствует свой подуровень PMD. В свою очередь, каждому PMD соответствует два типа физических интерфейсов — для локальных (LAN PHY) и территориально распределенных (WAN PHY) сетей. В то время как другие PMD-интерфейсы преобразуют биты в световые сигналы последовательно, интерфейс 10GBASE-LX4 использует технологию спектрального уплотнения WWDM для передачи битов одновременно на четырех длинах волн. Этот интерфейс является наиболее гибким, поскольку поддерживает как многомодовое оптоволокно с диаметром сердцевины 62,5 мкм для связи на близких (до 300 м) расстояниях, так и одномодовое волокно диаметром 9 мкм в целях осуществления связи на дальних расстояниях (до 10 км).

Изначально стандарт 10 Gigabit Ethernet предназначался для использования в региональных городских сетях (MAN, Metropolitan Area Networks). Об этом свидетельствует первая экспериментальная сеть, развернутая в 2002 году в городе Лас-Вегас (США). Но на самом деле область применения этих сетей намного шире. На их основе можно создавать корпоративные сети, охватывающие огромные территории.

Таблица 3.2. Сравнение сетей Gigabit Ethernet и 10 Gigabit Ethernet

Gigabit Ethernet	10 Gigabit Ethernet
Применяется метод доступа CSMA/CD, а также дуплексный метод	Только дуплексный метод
Управляемый физический интерфейс Fibre Channel	Новые стандарты интерфейса с применением волоконно-оптического кабеля
Повторно используемое шифрование 8B/10B	Новые схемы шифрования 64B/66B
Медный/волоконно-оптический кабель	Только волоконно-оптический кабель
Предельная длина сети до 5 км	Предельная длина сети до 40 км

Распространению любой новой технологии, как правило, мешает высокий уровень цен. Это высказывание справедливо и по отношению к 10 Gigabit Ethernet. Поэтому, если приходится выбирать между Fast Ethernet, Gigabit Ethernet и 10 Gigabit Ethernet, вполне естественно, что пользователь остановится на первых двух технологиях, несмотря на все преимущества, присущие последней технологии. Массовое снижение цен на оборудование сетей 10 Gigabit Ethernet по прогнозам произойдет не ранее 2006 года. Именно тогда и ожидается массовое

распространение сетей этого типа. Стоит обратить внимание на таблицу 3.2, где сравниваются характеристики сетей Gigabit Ethernet и 10 Gigabit Ethernet.

Теперь можно перейти к рассмотрению беспроводных сетей. Эта перспективная технология используется все чаще и чаще в современных условиях.

Беспроводные сети

Еще совсем недавно передача данных «по воздуху» казалась бесперспективным занятием из-за низкой пропускной способности и нестабильности сетевой аппаратуры. Хотя, как известно, первая коммерческая сеть ALOHA, развернутая на Гавайях, была как раз беспроводной.

На самом деле *беспроводные сети* не являются беспроводными в полном понимании этого слова. Обычно беспроводные каналы связи объединяют между собой обычные «кабельные» сети, носящие локальный характер. Поэтому фактически мы имеем дело с *гибридной* сетью.

Идея развертывания *беспроводной среды* весьма привлекательна, поскольку ее компоненты обеспечивают временное подключение к существующей кабельной сети, позволяют организовать резервное копирование в существующую кабельную сеть, гарантируют определенный уровень мобильности и снимают ограничения на максимальную протяженность сети, связанные с применением медных или даже волоконно-оптических кабелей.

Трудность прокладки кабелей в определенных ситуациях — фактор, который дает беспроводной среде неоспоримое преимущество. Эта среда может оказаться особенно полезной при временном развертывании сети на выставке, в приемной секретаря и в иных похожих случаях. В списке перечислены ситуации, когда использование беспроводного решения является целесообразным:

- для пользователей, которые не привязаны к своему рабочему месту;
- в изолированных помещениях и зданиях;
- в помещениях, планировка которых часто меняется;
- в строениях (например, памятниках истории или архитектуры), где прокладывать кабель просто невозможно.

В зависимости от применяемой технологии беспроводные сети можно разделить на три типа:

- локальные вычислительные сети;
- расширенные локальные вычислительные сети;
- мобильные сети (переносные компьютеры).

Основное различие между этими типами сетей заключается в используемых параметрах передачи. Локальные и расширенные локальные вычислительные сети используют передатчики и приемники, принадлежащие той организации, в которой функционирует сеть.

Типичная беспроводная сеть выглядит и функционирует практически так же, как обычная. Но главное отличие состоит в используемой среде передачи.

Беспроводной сетевой адаптер с трансивером установлен в каждом компьютере, и пользователи работают точно так же, как в обычной локальной сети.

Трансивер, называемый также *точкой доступа* (access point), обеспечивает обмен сигналами между компьютерами с беспроводным подключением и остальной сетью. В беспроводных сетях используются небольшие настенные трансиверы. Они устанавливают радиоконтакт между переносными устройствами. Такую сеть нельзя назвать полностью беспроводной именно из-за использования этих трансиверов.

Беспроводные локальные сети используют четыре способа передачи данных:

- инфракрасное излучение;
- лазер;
- радиопередачу в узком спектре (одночастотная передача);
- радиопередачу в рассеянном спектре.

Как и следует из названия, в инфракрасных беспроводных сетях для передачи данных применяются инфракрасные лучи. В подобных системах необходимо генерировать очень сильный сигнал, так как в противном случае значительное влияние будут оказывать другие источники, например, излучение солнца. Этот способ позволяет передавать сигналы с большой скоростью, поскольку инфракрасный свет имеет широкий диапазон частот. Инфракрасные сети способны нормально функционировать на скорости 10 Мбит/с. Существует четыре типа инфракрасных сетей:

- Сети прямой видимости. Как говорит само название, в таких сетях передача возможна лишь в случае прямой видимости между передатчиком и приемником.
- Сети, использующие рассеянное инфракрасное излучение. В случае применения этой технологии сигналы, отражаясь от стен и потолка, воспринимаются приемником. Диаметр сети в этом случае ограничивается примерно 30 метрами, и скорость передачи данных относительно невелика из-за большого уровня внешних помех.
- Сети, использующие отраженное инфракрасное излучение. В этих сетях оптические трансиверы, расположенные рядом с компьютером, передают сигналы в определенную точку, из которой они перенаправляются соответствующему компьютеру.
- Широкополосные оптические сети. Эти инфракрасные беспроводные сети предоставляют широкополосные услуги, соответствуют жестким требованиям мультимедийной среды и практически не уступают кабельным сетям.

Хотя скорость и удобство, сопровождающие использование инфракрасных сетей, весьма привлекательны для пользователей, очень часто возникают трудности при передаче сигналов на расстояние более 30 м. К тому же такие сети подвержены помехам со стороны сильных источников света, которые есть в большинстве организаций.

Лазерная технология похожа на инфракрасную тем, что требует прямой видимости между передатчиком и приемником. Если возникают какие-то преграды для распространения луча лазера, обмен данными в подобных сетях будет невозможен.

Обратите внимание на рис. 3.12, где приводится структура типичной беспроводной сети.

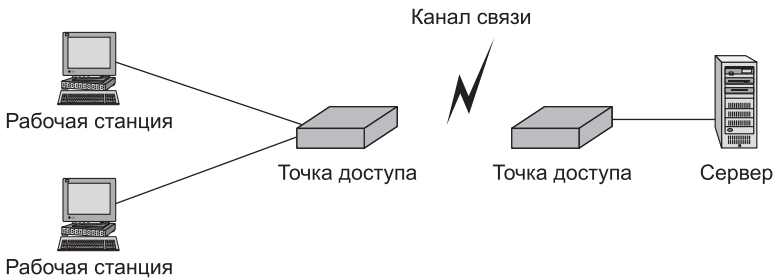


Рис. 3.12. Структура типичной беспроводной сети

Радиосети

В этом разделе подробнее остановимся на описании *радиосетей*, начав с краткого введения.

В радиосетях обычно применяют передачу данных либо на одной несущей частоте, либо используя рассеянный спектр радиоизлучения. Первый вариант напоминает работу обычной радиостанции. Передатчики и приемники настраиваются на заранее выбранную частоту. Хотя высокочастотный радиосигнал не проникает через металлические или железобетонные преграды, прямая видимость все же не является необходимым условием.

Получили некоторое распространение также радиосети, использующие рассеянный спектр, когда передатчик и приемник случайным образом перестраиваются в пределах выделенного радиодиапазона. Благодаря этому обеспечиваются высокая помехозащищенность и защита передаваемых данных.

Повсеместное распространение беспроводных сетей, развитие инфраструктуры хот-спотов, появление мобильных технологий со встроенными беспроводными решениями привело к тому, что конечные пользователи (не говоря уже о корпоративных клиентах) стали обращать все большее внимание на возможность применения беспроводных сетей. Такие решения рассматриваются прежде всего как средство развертывания мобильных и стационарных беспроводных локальных сетей и средство оперативного доступа в Интернет. Однако конечный пользователь, не являющийся сетевым администратором, как правило, не слишком хорошо разбирается в сетевых технологиях, поэтому ему трудно сделать выбор при покупке беспроводного оборудования, особенно учитывая многообразие предлагаемых сегодня продуктов. Бурное развитие технологии беспроводной связи привело к тому, что пользователи, не успев привыкнуть к одному стандарту, вынуждены переходить на другой, предлагающий еще более высокие скорости передачи.

Семейство стандартов беспроводной связи объединено под общим названием IEEE 802.11 и включает в себя разновидности 802.11, 802.11b, 802.11b+, 802.11a и 802.11g. Различные типы беспроводных сетей отличаются друг от друга и радиусом действия, и поддерживаемыми скоростями соединения, и технологией шифрования данных. Так, стандарт IEEE 802.11b предусматривает максимальную

скорость соединения 11 Мбит/с, стандарт IEEE 802.11b+ — 22 Мбит/с, стандарты IEEE 802.11g и 802.11a — 54 Мбит/с.

Блестящие перспективы имеет новый стандарт 802.11g. Основным его преимуществом является полная совместимость со стандартами 802.11b и 802.11b+, то есть любое устройство, поддерживающее стандарт 802.11g, будет работать (правда, на меньших скоростях соединения) и в сетях стандарта 802.11b/b+, а устройство, поддерживающее стандарт 802.11b/b+ — в сетях стандарта 802.11g.

Совместимость стандартов 802.11g и 802.11b/b+ обусловлена тем, что они предполагают использование одного и того же частотного диапазона. Также следует принять во внимание, что все режимы, предусмотренные в стандартах 802.11b/b+, реализованы и в стандарте 802.11g. Поэтому стандарт 802.11b/b+ можно рассматривать как подмножество стандарта 802.11g.

А теперь подробнее остановимся на описании физических основ стандарта 802.11.

Стандарт 802.11, как и все остальные стандарты данного семейства, предусматривает использование частотного диапазона от 2400 до 2483,5 МГц, который разбит на несколько каналов.

ПРИМЕЧАНИЕ Скорость передачи данных в современных радиосетях варьируется от 1 Мбит/с (базовый стандарт IEEE 802.11) до 100 Мбит/с (стандарт IEEE 802.11n).

В основе всех беспроводных протоколов семейства 802.11 лежит технология *распределения спектра* (SS, Spread Spectrum). Эта технология позволяет узкополосный информационный сигнал в процессе передачи преобразовать таким образом, что его спектр оказывается значительно шире спектра первоначального сигнала. То есть спектр сигнала «распределяется» по частотному диапазону. Одновременно с распределением спектра сигнала происходит и перераспределение спектральной энергетической плотности сигнала, которая тоже «распределяется» по спектру. В результате максимальная мощность преобразованного сигнала оказывается значительно ниже мощности исходного сигнала. При этом уровень полезного информационного сигнала может критически «проваливаться», теряясь на фоне естественного шума.

Именно в изменении спектральной энергетической плотности сигнала и заключается идея распределения спектра. Дело в том, что если подходить к проблеме передачи данных традиционным способом, когда каждой радиостанции отводится свой диапазон вещания, то мы неизбежно столкнемся с проблемой, что ограниченный радиодиапазон, предназначенный для совместного использования, не может «вместить» всех желающих. Поэтому необходимо найти такой способ передачи информации, при котором пользователи могли бы сосуществовать в одном частотном диапазоне и при этом не мешать друг другу. Именно эту задачу и решает технология распределения спектра.

На практике применяется несколько различных технологий распределения спектра, но в данном случае достаточно ознакомиться лишь с технологией распределения спектра методом прямой последовательности (DSSS, Direct Sequence Spread Spectrum).

В процессе кодирования методом потенциалов биты–носители информации интерпретируются в качестве прямоугольных импульсов напряжения. Прямоугольному импульсу соответствует спектр, ширина которого обратно пропорциональна длительности импульса. Поэтому чем меньше длительность информационного бита, тем больший спектр занимает такой сигнал.

Для распределения спектра изначально узкополосного сигнала в технологии DSSS в каждый передаваемый информационный бит (логический 0 или 1) встраивается *последовательность элементарных сигналов* (chips). Если информационные биты при кодировании информации методом потенциалов можно представить в виде последовательности прямоугольных импульсов, то каждый отдельный элементарный сигнал представляет собой прямоугольный импульс. Но его длительность в несколько раз меньше длительности информационного бита.

Последовательность чипов является серией прямоугольных импульсов, то есть нулей и единиц. Однако эти нули и единицы не являются информационными. Поскольку длительность одного элементарного импульса в несколько раз меньше длительности информационного бита, то и ширина спектра преобразованного сигнала будет в это же количество раз больше ширины спектра первоначального сигнала. При этом и амплитуда передаваемого сигнала также уменьшится в это количество раз.

Последовательности элементарных сигналов, встраиваемые в информационные биты, называют *шумообразными кодами* (PN-последовательности), что подчеркивает то обстоятельство, что результирующий сигнал становится шумоподобным и его трудно отличить от естественного шума. Каким образом можно распределить спектр сигнала и сделать его неотличимым от естественного шума? Для этого можно воспользоваться произвольной последовательностью элементарных сигналов.

Однако, необходимо определиться, как такой сигнал принимать. Ведь если он становится шумообразным, то выделить из него полезный информационный сигнал не так-то просто. Оказывается, это вполне возможно, но для этого нужно соответствующим образом подобрать последовательность элементарных сигналов. Используемые для распределения спектра сигнала последовательности элементарных сигналов должны удовлетворять определенным требованиям *автокорреляции*. Под этим термином в математике подразумевают степень подобия функции самой себе в различные моменты времени.

Если подобрать такую последовательность элементарных сигналов, для которой функция автокорреляции будет иметь резко выраженный пик лишь для одного момента времени, то такой информационный сигнал можно будет выделить на уровне шума. Для этого в приемнике полученный сигнал умножается на ту же последовательность элементарных сигналов, то есть вычисляется автокорреляционная функция сигнала. В результате сигнал повторно становится узкополосным, поэтому снова фильтруется в узкой полосе частот. Любая помеха, попадающая в полосу исходного широкополосного сигнала, после умножения на последовательность элементарных сигналов становится широкополосной и обрезается фильтрами. А в узкую информационную полосу попадает лишь часть помехи, по мощности значительно меньшая, чем помеха, действующая на входе приемника.

Последовательностей элементарных сигналов, отвечающих указанным требованиям автокорреляции, существует достаточно много, но особый интерес представляют *коды Баркера*, поскольку именно они используются в стандарте 802.11. Коды Баркера обладают наилучшими среди известных псевдослучайных последовательностей свойствами шумоподобности, что и обусловило их широкое применение. В протоколах семейства 802.11 используется код Баркера длиной в 11 элементарных сигналов (11100010010). Для того чтобы передать сигнал, логическая единица передается прямой последовательностью Баркера, а логический нуль — обратной последовательностью.

В стандарте 802.11 предусмотрено два режима передачи данных: со скоростями 1 и 2 Мбит/с. Для кодирования данных на физическом уровне используется метод DSSS с кодами Баркера длиной в 11 элементарных сигналов. При скорости передачи данных в 1 Мбит/с скорость следования отдельных элементарных сигналов в последовательности Баркера составляет $11 \cdot 10^6$ сигналов/с, а ширина спектра такого сигнала составляет 22 МГц. Учитывая, что ширина частотного диапазона составляет 83,5 МГц, можно понять, что всего в данном частотном диапазоне можно разместить до трех неперекрывающихся частотных каналов.

Весь частотный диапазон принято делить на 11 частотных перекрывающихся каналов по 22 МГц, отстоящих друг от друга на 5 МГц. Например, первый канал занимает частотный диапазон от 2400 до 2423 МГц, причем центральная частота в данном случае составляет 2412 МГц. Для второго канала центральная частота будет 2417 МГц, а для последнего канала — 2462 МГц. При таком рассмотрении первый, шестой и одиннадцатый каналы не перекрываются друг с другом и имеют 3-мегагерцевый зазор друг относительно друга. Именно эти три канала могут использоваться независимо друг от друга.

Для модуляции синусоидального несущего сигнала используется *относительная двоичная фазовая модуляция* (DBPSL, Differential Binary Phase Shift Key). При этом кодирование информации происходит за счет смещения фазы синусоидального сигнала по отношению к предыдущему состоянию сигнала. Двоичная фазовая модуляция предусматривает два возможных значения сдвига фазы — 0 и π. Тогда логический нуль может передаваться синфазным сигналом (сдвиг по фазе равен 0), а единица — сигналом, который сдвинут по фазе на π.

Скорость передачи данных 1 Мбит/с является минимально необходимой в условиях стандарта IEEE 802.11, хотя и возможно достижение скорости 2 Мбит/с. В этом случае применяется та же технология DSSS, применяющая коды Баркера, длина которых составляет 11 элементарных сигналов, а для модуляции несущей используется *относительная квадратурная фазовая модуляция* (DQPS, Differential Quadrature Phase Shiftey). При относительной квадратурной фазовой модуляции сдвиг фаз может принимать четыре различных значения: 0, $\pi/2$, π и $3\pi/2$. Используя четыре различных состояния сигнала, можно в одном дискретном состоянии закодировать последовательность двух информационных битов, благодаря чему скорость передачи информации повышается в два раза.

Однако при скорости передачи данных 2 Мбит/с скорость следования отдельных элементарных сигналов последовательности Баркера остается прежней, то есть $11 \cdot 10^6$ сигналов/с, а следовательно, не изменяется ширина спектра передаваемого сигнала.

Стандарт IEEE 802.11b, принятый в июле 1999 года, является своего рода расширением базового стандарта IEEE 802.11. Скорость передачи данных была увеличена до 5,5 и 11 Мбит/с, соответственно. Для работы на скоростях 1 и 2 Мбит/с применяется технология распределения спектра с использованием кодов Баркера, а для организации передачи данных со скоростью 5,5 и 11 Мбит/с — так называемые комплементарные коды (CCK, Complementary Code Keying). Комплементарные коды, или CCK-последовательности, обладают следующим свойством: сумма их автокорреляционных функций для любого циклического сдвига, отличного от нуля, всегда равна нулю.

В стандарте IEEE 802.11b используются комплексные комплементарные последовательности из восьми элементарных сигналов, определенные на множестве комплексных чисел.

Иногда вызывает недоумение наличие скорости передачи данных 5,5 Мбит/с, тогда как доступна величина 11 Мбит/с. Потребность в снижении скорости передачи возникает в том случае, когда возрастает «зашумленность» радиоэфира, то есть уменьшается величина соотношения сигнал/шум.

В радиосетях применяется еще один вид кодирования данных — *двоичное сверточное кодирование пакетов* (PBCC, Packet Binary Convolutional Coding). Принципы, лежащие в основе сверточного кодирования, будут следующими. Входящая последовательность информационных битов преобразуется специальным сверточным кодировщиком таким образом, чтобы каждому входному биту соответствовало более одного выходного бита. То есть сверточный кодировщик добавляет определенную избыточную информацию к исходной последовательности. Если, например, каждому входному биту соответствует три выходных бита, то говорят о сверточном кодировании со скоростью 1/3.

При создании сверточного кодировщика используются несколько последовательно связанных запоминающих ячеек и логических элементов, связывающих эти ячейки между собой. Количество запоминающих ячеек определяет количество возможных состояний кодировщика. Если, например, в сверточном кодировщике используется пять запоминающих ячеек, то в кодере хранится информация о пяти предыдущих состояниях сигнала, а с учетом значения входящего бита будет использоваться шесть битов входной последовательности. Такой сверточный кодировщик называется кодировщиком, основанным на шести состояниях. Выходные биты, формируемые в сверточном кодировщике, определяются значениями входного бита и битами, хранимыми в запоминающих ячейках. То есть значение каждого формируемого выходного бита зависит не только от входящего информационного бита, но и от нескольких предыдущих битов.

В технологии PBCC используются сверточные кодировщики, рассчитанные на семь состояний со скоростью преобразования R= 1/2. Основное достоинство сверточных кодировщиков заключается в том, что формируемая ими последовательность сигналов устойчива к помехам. Так происходит потому, что при избыточности кодирования даже в случае возникновения ошибок приема исходная последовательность битов может быть безошибочно возвращена к исходному состоянию. Пара битов, формируемая сверточным кодировщиком, используется в дальнейшем в качестве передаваемого символа, но предварительно к ней применяется фазовая модуляция. Причем, в зависимости от скорости передачи,

используется двоичная, квадратурная или даже восьмипозиционная фазовая модуляция.

Метод сверточного кодирования пакетов рассматривается в качестве альтернативного метода кодирования, применяемого в стандарте IEEE 802.11b. Помимо этого, именно данный режим кодирования заложен в основу стандарта 802.11b+, который является расширением стандарта 802.11b. Собственно говоря, на официальном уровне стандарта 802.11b+ не существует, однако это расширение поддерживается многими производителями беспроводных устройств. В стандарте 802.11b+ предусматривается скорость передачи данных 22 Мбит/с, а также применяется технология PBCC.

При скорости передачи 5,5 Мбит/с для модуляции пары битов, формируемых сверточным кодировщиком, применяется двоичная фазовая модуляция, а при скорости 11 Мбит/с — квадратурная фазовая модуляция. При этом для скорости 11 Мбит/с в каждом символе кодируется по одному входному биту, скорость передачи битов соответствует скорости передачи символов, а при скорости 5,5 Мбит/с скорость передачи битов соответствует половине скорости передачи символов (поскольку каждому входному биту в данном случае соответствует два выходных символа). Поэтому и для скорости 5,5 Мбит/с, и для скорости 11 Мбит/с символьная скорость составляет $11 \cdot 10^6$ символов в секунду.

Передача данных со скоростью 22 Мбит/с имеет две особенности. Во-первых, используется фазовая 8-позиционная фазовая модуляция (8-PSK), то есть фаза сигнала может принимать восемь различных значений, что позволяет в одном символе кодировать уже три бита. Кроме того, в схему кроме сверточного кодера добавлен пунктурный кодировщик. Смысл такого решения довольно прост. Двойная избыточность сверточного кодировщика (на каждый входной бит приходится два выходных) достаточно велика и при низком уровне помех становится излишней, поэтому можно уменьшить избыточность, чтобы, к примеру, каждым двум входным битам соответствовало три выходных бита. При этом можно, конечно, разработать соответствующий сверточный кодировщик, но лучше добавить в схему специальный пунктурный кодировщик, который будет просто убирать лишние биты.

Предположим, что пунктурный кодировщик удаляет один бит из каждых четырех входных битов. Тогда каждым четырем входящим битам будет соответствовать три выходящих. Скорость такого кодера составляет 4/3. Если же такой кодер используется в паре со сверточным кодировщиком, имеющим скорость 1/2, общая скорость кодирования составит уже 2/3, то есть каждым двум входным битам будет соответствовать три выходных бита.

Разобравшись с принципом работы пунктурного кодировщика, вернемся к рассмотрению кодирования PBCC на скорости 22 Мбит/с в протоколе 802.11b+. Сверточному кодировщику (K = 7, R = 1/2) данные передаются со скоростью 22 Мбит/с. После добавления избыточности в сверточном кодировщике биты со скоростью потока 44 Мбит/с передаются пунктурному кодировщику 4:3, в котором избыточность уменьшается так, чтобы на каждые четыре входных бита приходилось три выходных бита. Следовательно, после пунктурного кодировщика скорость потока составит уже 33 Мбит/с. Полученная в результате последовательность направляется в фазовому модулятору 8-PSK, где каждые три бита

упаковываются в один символ. При этом скорость передачи составит $11 \cdot 10^6$ символов в секунду, а информационная скорость передачи данных 22 Мбит/с.

На этом завершается рассмотрение теоретических основ работы набора стандартов IEEE 802.11, на основе которых функционируют радиосети.

ПРИМЕЧАНИЕ Желающие подробнее ознакомиться с теорией могут обратиться на веб-сайт www.wireless.ru, на котором находится масса полезной информации по этой теме.

Новые скорости радиосетей

Как и в случае с кабельными сетями, скорость передачи данных в беспроводных сетях постоянно растет. И доказательством этому служит разрабатываемый Европейским институтом стандартизации в области электросвязи (ETSI) стандарт HiperLAN2 (High Perfomance Radio LAN, радиосеть с высокой производительностью). Именно этот стандарт обещает стать основным конкурентом технологий беспроводных ЛВС, работающих в соответствии со стандартом IEEE 802.11. Инициаторами и активными сторонниками нового стандарта являются компании Nokia и Ericsson.

Так же, как и 802.11a, стандарт HiperLAN2 ориентирован на работу в диапазоне 5 ГГц и способен обеспечить скорость передачи данных до 54 Мбит/с. Оба стандарта используют сходные методы модуляции сигнала на основе мультиплексирования с ортогональным разделением частот (OFDM), однако имеют различные спецификации протоколов доступа к среде MAC. Если для 802.11a он аналогичен Ethernet, то в HiperLAN2 протокол больше напоминает методы, используемые в сетях ATM. Другим отличием HiperLAN2 от 802.11a, которое может дать ему некоторое преимущество над конкурентом, является поддержка мультимедийного трафика и QoS (802.11a ориентирован в основном на передачу данных). По информации ETSI, разработка стандарта ведется с учетом совместимости оборудования с системами 802.11a. Подробнее о новом стандарте можно узнать на веб-сайте по адресу www.etsi.org/technicalactiv/hiperlan2.htm.

Технология Bluetooth

Термин «Bluetooth» настолько широко используется в настоящее время, что не нуждается в особом толковании. И совсем немногие задумываются о том, что Bluetooth представляет собой еще одну инкарнацию радиосети, а не усовершенствованный пульт дистанционного управления телевизором.

Эта технология продвигается в массы консорциумом Bluetooth Special Interest Group (Bluetooth SIG). Ее альтернативное название — стандарт IEEE 802.15.1. Причем усилиями специалистов из этого консорциума были разработаны спецификации Bluetooth v 1.x, на основе которых формируются *персональные беспроводные сети* (WPAN, Wireless Personal Area Network).

Почему их называют персональными сетями? Ответ весьма прост. С их помощью связь осуществляется на небольшие расстояния (несколько десятков метров)

и охватывает устройства, которые обычно относят к категории «персональных» (мобильные телефоны, ноутбуки, персональные компьютеры и т. д.).

Технология Bluetooth позволяет сформировать недорогой радиоинтерфейс, отличающийся сниженным энергопотреблением (мощность передатчика не превышает 1 мВт). Она позволяет создавать персональные сети, в которых обеспечивается передача цифровых данных и звуковых сигналов в режиме реального времени. Изначально дальность действия радиоинтерфейса не превышала десяти метров, однако в современной спецификации Bluetooth радиус действия увеличен до 100 метров. Для работы устройств Bluetooth применяется диапазон 2,45 ГГц. При этом не требуется, чтобы связываемые устройства находились в пределах прямой видимости.

Полная пропускная способность радиоканала Bluetooth составляет 1 Мбит/с, благодаря чему возможно формирование асимметричного канала передачи данных на скоростях 723,3/57,6 Кбит/с или дуплексного канала, обеспечивающего скорость передачи данных до 433,9 Кбит/с. Можно также организовать до трех дуплексных аудиоканалов, обеспечивающих скорость передачи звука до 64 Кбит/с в каждом направлении. Возможна также комбинированная передача данных и звука. Для организации обмена данными технология Bluetooth соответствует спецификации стандарта локальных сетей IEEE 802 и использует сигналы с расширением спектра путем скачкообразной перестройки частоты (FHSS) по псевдослучайному закону со скоростью 1600 переключений в секунду в полосе частот 2400–2483,5 МГц.

Канал Bluetooth работает как многоточечный радиоканал, управляемый, как и мобильная связь стандарта GSM, многоуровневым протоколом. В качестве мер защиты в Bluetooth предусмотрено шифрование передаваемых данных и авторизация устройств. При этом возможны три уровня защиты. На минимальном уровне данные шифруются общим ключом и могут приниматься любыми устройствами без ограничений. Защита на уровне устройств применяется, когда непосредственно в микросхеме кодируется уровень доступа, в соответствии с которым устройство может получать определенные данные от других устройств. Также используется защита на уровне сеанса связи, когда данные шифруются с применением 128-битовых случайных чисел, хранящихся в каждой паре устройств, участвующих в данном сеансе связи.

На этом рассмотрение физических принципов работы сетей Ethernet временно приостанавливается. Некоторые дополнительные моменты будут рассматриваться в соответствующих главах. Сейчас же настало время ближе познакомиться с основными устройствами, применяемыми в сетях Ethernet.

4 ГЛАВА Основные сетевые протоколы

Эта глава завершает теоретическое введение в сети Microsoft. Здесь будет приведено описание базовых протоколов, определяющих функционирование сети в целом, без которых немыслимо представить современную локальную сеть.

Альфа и омега Интернета — TCP/IP

Нелишне будет напомнить, что *протокол* — это набор правил, описывающих и определяющих функционирование сети. Стек протоколов TCP/IP является основой Интернета, который представляет собой суперобъединение локальных сетей. Основное преимущество TCP/IP заключается в его универсальности и независимости от применяемых аппаратных средств. Этот набор протоколов поддерживается всеми версиями Windows начиная с версии Windows 95. Именно поэтому его использование в сетях Windows является оправданным во всех отношениях.

Аббревиатура TCP/IP расшифровывается очень просто — Transmission Control Protocol/Internet Protocol (протокол управления передачей/протокол Интернета). Помимо этих двух основных протоколов, в TCP/IP входит протокол управляющих сообщений Интернета (ICMP, Internet Control Message Protocol), а также протокол дейтаграмм пользователя (UDP, User Datagram Protocol). Все эти протоколы будут рассмотрены в настоящем разделе. А пока стоит обратить внимание на список компонентов TCP/IP.

- Протокол IP относится к категории *ненадежных* протоколов, работающих без установки соединений. Основная его функция заключается в передаче сетевых пакетов между пользовательскими компьютерами, а также в обеспечении адресации сетевых станций, подключенных к локальной сети.
- Протокол TCP относится к категории надежных протоколов, функционирующих с установкой соединения. Именно он организует проверку доставки

пакетов данных, осуществляемую протоколом IP. TCP является надежным, ориентированным на установку соединений протоколом, который требует установки сеанса для управления передачей данных между двумя точками в сети. В результате обеспечивается обнаружение ошибок, а также их устранение, если это возможно.

- Протокол UDP часто называют протоколом пользовательских дейтаграмм (User Datagram Protocol). Он используется теми приложениями, которые не требуют надежной доставки данных.
- Протокол ARP называют протоколом разрешения адресов (Address Resolution Protocol). Он используется для определения MAC-адреса компьютера на основе исходного IP-адреса. Обычно этот протокол применяется маршрутизаторами, принимающими пакеты данных из внешних сетей.
- Протокол RARP часто называют протоколом определения сетевого адреса по местоположению узла (Reverse Address Resolution Protocol). В противовес ARP, протокол RARP применяется для вычисления IP-адреса на базе исходного MAC-адреса. На практике эти функции реализованы протоколами BOOTP и DHCP, область применения которых постоянно сужается.
- Система DNS (Domain Name System, система имен доменов). На практике она является иерархической системой именования узлов сети, которая применяется в Интернете, а также во многих локальных сетях. Так, если пользователь в строке веб-браузера вводит запрос http://www.my_server.ru, сервер DNS пытается найти численный IP-адрес, связанный с данной ссылкой.
- Протокол BOOTP (Bootstrap Protocol, протокол начальной загрузки) ранее широко использовался для загрузки бездисковых рабочих станций, подключенных к сети. При разработке этого протокола основным требованием являлась компактность исходного кода. Это обуславливалось тем, что протокол жестко кодировался в ПЗУ сетевого адаптера.
- Протокол DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации узла) регламентирует процедуру присваивания IP-адресов и другой соответствующей конфигурационной информации сервером клиентским системам.
- Протокол RMON (Remote Monitoring, удаленный мониторинг) предназначается для расширения возможностей администраторов по дистанционному управлению компьютерами и сетевыми устройствами.
- Протокол SNMP (Simple Network Management Protocol, простой протокол управления сетью) изначально разрабатывался для облегчения централизованного управления сетевыми устройствами и компьютерами.
- Протокол SMTP (Simple Mail Transfer Protocol, простой протокол электронной почты) предназначается для управления почтовыми сообщениями, передаваемыми в Интернете.

В следующих разделах главы протоколы IP и TCP описываются подробнее. Но, прежде всего нужно рассмотреть один из базовых протоколов Интернета — протокол IP.

Становой хребет Интернета

Трудно было не заметить, что в аббревиатуре TCP/IP основной протокол Интернета следует вторым. На самом деле причина этого заключается не в том, что этот протокол второстепенный, а в том, чтобы было удобнее запомнить название. Согласитесь, что «IP/TCP» произносится не столь просто. В следующем списке приведены основные свойства протокола IP.

- Протокол IP не ориентирован на установку соединений. Каждый IP-пакет представляет собой отдельный объект, который не зависит от других пакетов, передающихся в сети.
- Протокол IP функционирует без передачи подтверждений о доставке данных, включенных в состав дейтаграммы или пакета.
- Этот протокол считается ненадежным, что следует из первых двух пунктов списка.
- В рамках этого протокола формируется пространство иерархических уникальных IP-адресов.

Стандартная модель функционирования протокола IP достаточно проста. Протокол принимает данные с сетевого уровня модели OSI, а затем разбивает их на меньшие пакеты данных. Затем протокол IP, выполняющийся на рабочей станции, которая является получателем пакетов, производит воссоздание данных в исходном виде. В целях гарантированной доставки каждого IP-пакета в их заголовки помещаются адреса отправителя и получателя, а также вычисляется значение контрольной суммы.

На рис. 4.1 показана структура заголовка IP-пакета. Описание соответствующих полей приводится в следующем за рисунком перечне.

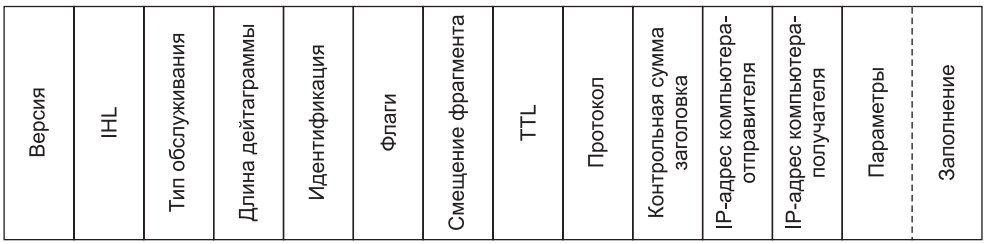


Рис. 4.1. Структура заголовка IP-пакета

- Поле Version (версия) позволяет указывать версию применяемого протокола IP (IPv4 или IPv6).
- Поле IHL (Internet Header Length, длина заголовка IP-пакета) содержит информацию о длине заголовка пакета, передаваемого протоколом Интернета.
- Поле Type of Service (тип обслуживания) позволяет задавать уровень приоритета для данного IP-пакета. Это поле используется версиями Gigabit Ethernet и 10 Gigabit Ethernet, а также версией протокола IPv6.

- Поле Datagram Length (длина дейтаграммы) содержит длину IP-пакета в целом. Длина раздела данных пакета вычисляется при помощи вычитания значения, хранящегося в поле IHL, из данного значения.
- Поле Identification (идентификация). Протокол IP часто разбивает сообщение, полученное протоколом высокого уровня, на меньшие по размеру пакеты в зависимости от максимального размера фрейма, поддерживаемого базовой сетевой технологией. После получения пакетов необходимо выполнить их повторную сборку. Компьютер-отправитель помещает в данное поле уникальный номер, соответствующий каждому фрагменту сообщения. В этом случае для каждого пакета в конкретном сообщении в данном 16-битовом поле будет содержаться одно и то же значение. Компьютер-получатель принимает все требуемые фрагменты, затем воссоздает исходное сообщение.
- Поле Flags (флаги) содержит различные флаговые биты. Нулевой бит резервируется и всегда должен содержать нулевое значение. Первый бит определяет флаг DF (Don't Fragment, Не фрагментировать). Второй бит определяет флаг MF (More Fragments, Дополнительные фрагменты).
- Поле Fragment Offset (смещение фрагмента). Если бит MF установлен равным единице, данное поле используется для указания позиции фрагмента в исходном сообщении, благодаря чему обеспечивается успешная повторная сборка пакета.
- Поле TTL (Time to Live, время существования). В этом поле определяется время, в течение которого IP-пакет циркулирует в сети. При каждом прохождении пакета через маршрутизатор значение этого поля уменьшается на единицу.
- Поле Protocol (протокол) содержит числовой код применяемого протокола, присвоенный организацией ICANN.
- Поле Header Checksum (контрольная сумма заголовка) содержит контрольную сумму, вычисляемую по всем полям заголовка IP-пакета. Это значение вычисляется повторно при каждом прохождении IP-пакета через маршрутизатор, поскольку при этом изменяется значение поля TTL.
- Поле Source IP Address (IP-адрес компьютера отправителя). Как и следует из названия, в этом поле находится IP-адрес компьютера, которым был отправлен данный пакет.
- Поле Destination IP Address (IP-адрес компьютера-получателя). Как и следует из названия, в этом поле находится IP-адрес компьютера, которому предназначается данный пакет.
- Поле Options (параметры). В этом поле указываются дополнительные параметры, определяющие различные аспекты дальнейшей обработки пакета данных.
- Поле Padding (дополнение). Назначение этого поля — дополнение заголовка пакета таким образом, чтобы его длина была постоянной и составляла 32 бита.

Теперь следует тщательнее рассмотреть, как в процессе работы формируются и распознаются IP-адреса.

IP-адреса

Интернет представляет собой набор сетей, которые объединены с помощью маршрутизаторов. В результате этого формируется «суперсеть». Образование подобной структуры возможно, поскольку протокол IP обеспечивает правильную адресацию каждой сети, подключенной к Интернету, а также идентификацию узлов, имеющих отношение к конкретной сети. В процессе выполнения маршрутизации пакетов *IP-адрес* применяется для пересылки данных в требуемую локальную сеть. Как только пакет данных достигает маршрутизатора, находящегося в этой сети, в дело вступает MAC-адрес компьютера-получателя данного пакета. При этом используется узловой раздел IP-адреса, а также сведения из таблицы маршрутизации, в которой указано соответствие между MAC-адресами и узловыми разделами IP-адреса в локальной сети. Если соответствие не найдено, в локальной сети используется протокол ARP в целях определения адресов и добавления их в таблицу маршрутизации.

Классы IP-адресов

Существует пять классов IP-адресов (A, B, C, D и E). Класс, к которому относится данный IP-адрес, определяется его первыми четырьмя битами (длина IP-адреса составляет 32 бита в версии протокола IPv4). В данном случае эти четыре бита определяют *сетевой раздел IP-адреса* (адресация сети), в то время как оставшиеся биты образуют *узловой раздел IP-адреса* (адресация узла в сети).

Для IP-адресов из класса A первый бит равен нулю, остальные же биты могут принимать произвольные значения. Если воспользоваться стандартной *точечно-десятичной нотацией*, которую принято использовать для записи IP-адресов, то IP-адреса класса A относятся к диапазону от 0.0.0.0 до 127.255.255.255.

Следует отметить, что сетей класса A меньше всего. Это связано с тем, что в адресах из этой категории для идентификации сети используется только первый байт. Оставшиеся байты адреса используются для идентификации узла в сети. Поскольку первый бит адреса всегда равен нулю, для формирования сетевого адреса используются оставшиеся 7 битов. По этой причине в сетях класса A доступно лишь 127 сетевых адресов (двоичное число 01111111 соответствует десятичному числу 127).

Но, как говорится, нет худа без добра. Сети класса A могут содержать наибольшее количество сетевых узлов, поскольку оставшиеся три байта используются для определения узлового раздела IP-адреса. Эти три байта могут определять значение, которое в десятичной записи соответствует числу 16 777 215 (24 бита, значение каждого из которых равно 1). Учитывая ноль, можно понять, что с помощью трех байтов возможно определение до 16 777 216 IP-адресов (2^{24}). Поэтому в одной сети класса A возможно одновременно «мирное сосуществование» свыше 16 миллионов сетевых компьютеров.

А вот общее количество сетей класса A существенно меньше — не более 127. Диапазон IP-адресов сетей класса A — от 0.0.0.0 до 127.255.255.255. Если некий адрес попадает в этот диапазон, можно с полной уверенностью утверждать, что он является адресом из сети класса A.

IP-адреса, относящиеся к классу B, характеризуются тем, что значения первых двух битов равны единице и нулю, соответственно. Если использовать точечно-десятичную запись, то адреса этого типа попадают в диапазон значений от 128.0.0.0 до 191.255.255.255. В двоичном формате десятичное число 128 эквивалентно 10000000. Десятичное значение 191 преобразуется в двоичное число 10111111. Оба эти значения на первом месте содержат двоичные числа 10, что служит признаком IP-адреса класса B. Поскольку два первых байта адреса класса B используются для адресации сети, два оставшихся байта применяются для определения адресов узлового компьютера. Простые вычисления позволяют сказать, что в данном классе имеется до 16384 допустимых сетевых адресов. В каждой сети класса B может располагаться не более 65536 (216) отдельных компьютеров.

Характерный признак IP-адресов из класса C заключается в том, что первые три бита равны 1, 1 и 0, соответственно. После преобразования в точечно-десятичный формат получим, что IP-адреса из класса C относятся к диапазону от 192.0.0.0 до 223.255.255.255. В данном случае первые три байта используются для сетевого раздела адреса, а один байт применяется для формирования адреса узла. Общее количество сетей из класса C достигает 2097152. В каждой сети этого класса может находиться до 256 узловых компьютеров. Таким образом, общее количество сетей класса C является наибольшим, а в каждой сети находится минимальное количество компьютеров.

ПРИМЕЧАНИЕ В настоящее время для вновь создаваемых сетей назначаются IP-адреса, относящиеся к классу C. Это связано с тем, что именно этот класс обладает небольшим избытком IP-адресов, тогда как классы адресов A и B уже давно закрыты.

До сих пор шла речь об IP-адресах, применяемых для адресации в локальных сетях. Следует упомянуть еще два класса адресов, применяемых в служебных целях. Диапазон адресов из класса D зарезервирован для широковещательной рассылки, когда сетевые пакеты отсылаются нескольким сетевым узлам одновременно. Адреса из класса D (в точечно-десятичной нотации) относятся к диапазону от 224.0.0.0 до 239.255.255.255. Причем в данном случае отсутствуют специфические байты, используемые для идентификации сетевого или узлового раздела IP-адреса. Это означает, что потенциально может существовать до 268435456 уникальных IP-адресов из этого класса.

IP-адреса из класса E относятся к диапазону от 240.0.0.0 до 255.255.255.255. Эти адреса зарезервированы для применения в будущем.

IP-адрес 127.0.0.1 (попадающий в диапазон адресов класса A) называется *адресом закольцовки* и применяется для тестирования локального стека протоколов TCP/IP. Этот адрес применяется совместно с командой `ping` в целях проверки корректности сетевых настроек для данного компьютера. Так, например, в результате выполнения команды `ping 127.0.0.1` на экране отображается соответствующая информация о локальной системе (рис. 4.2).

Этот IP-адрес можно использовать для тестирования других программ. Например, можно воспользоваться Telnet, указав адрес закольцовки для проверки возможности запуска этого сервиса на данном компьютере.

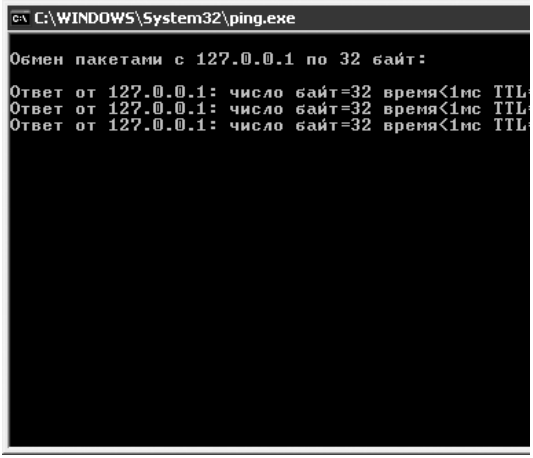


Рис. 4.2. Пример использования адреса закольцовки

Подсети

Хотя и пространство IP-адресов достаточно велико, но, как известно, все познается в сравнении, особенно если вспомнить о количестве сетевых компьютеров, подключенных к Интернету в настоящее время. Любая серьезная организация, которой приходится развертывать десятки и сотни локальных сетей, нуждается в нескольких сотнях IP-адресов. Суть формирования подсетей заключается в разбиении единого непрерывного множества IP-адресов с образованием нескольких подмножеств, которые называются *подсетями*. Например, если идет речь об адресах класса A, в одной сети могут находиться свыше 16 миллионов узловых компьютеров. Это количество настолько велико, что даже такой монстр как Microsoft не использует сети подобных масштабов.

В силу упомянутых выше причин в больших сетях формируются подсети, в которых применяется так называемая *адресация подсетей*. При этом исходный IP-адрес разбивается таким образом, что образуется *сетевой* и *локальный* раздел. Первый раздел применяется в целях идентификации сети в бескрайних просторах Интернета, а второй раздел адресует подсети и узлы внутри локальной сети.

В процессе адресации подсетей для каждой сети, входящей в состав большой сети, формируется *маска подсети*. Алгоритм, положенный в основу ее формирования, весьма прост. Если биты исходного IP-адреса имеют отношение к разделу, определяющему подсеть, соответствующие биты маски подсети выбираются равными 1, если же рассматривается раздел, который определяет IP-адрес узла внутри подсети, то для битов маски подсети выбираются нулевые значения. Так, например, в маске вида 11111111 11111111 00000000 00000000 первые два октета определяют подсеть, а последние два — узел в этой подсети. Структура маски подсети в этом случае соответствует IP-адресу для сети из класса B. Если воспользоваться точечно-десятичным форматом записи, то маска подсети получит обозначение 255.255.0.0. Для IP-адресов из класса A применяется маска подсети 255.0.0.0. а для IP-адресов из класса C — 255.255.255.0.

Например, маска подсети 255.255.255.128 определяет сеть класса C, в которой могут формироваться две подсети. Если применить эту маску к сетевому адресу 193.112.255, то будут созданы две подсети. Диапазон IP-адресов в первой подсети ранжируется от 193.112.255.1 до 193.112.255.128, а во второй подсети — от 193.112.255.129 до 193.112.255.254.

Бесклассовая адресация

Как отмечалось ранее, система классификации IP-адресов (классы A, B, C) устраивала сообщество пользователей Интернета до тех пор, пока Сеть не получила глобальное распространение. Система классов и подсети по-прежнему широко используются маршрутизаторами локальных сетей. Магистральные маршрутизаторы Интернета применяют бесклассовую маршрутизацию между доменами (CIDR, Classless Interdomain Routing) в целях определения оптимального маршрута, используемого для передачи пакетов.

После появления системы классов IP-адресов первый байт адреса традиционно обозначал номер сети, благодаря чему практическая реализация маршрутизации не вызывала особых затруднений. Например, для IP-адреса 130.166.232.233 число 130 являлось признаком диапазона IP-адресов класса B, а подсеть получала номер 130.166.0. Маршрутизация же пакета в самой подсети требовала использования локальной таблицы маршрутизации, поддерживаемой самим маршрутизатором.

ПРИМЕЧАНИЕ Подробнее о маршрутизаторах и таблицах маршрутизации рассказывается в следующей главе.

Но поскольку рост Интернета в последние десятилетия все больше напоминает неуправляемую реакцию деления атомных ядер урана, все это привело к появлению великого множества сетей, относящихся к классам B и C. Это, в свою очередь, вызвало стремительное «разбухание» таблиц маршрутизации, применяемых магистральными маршрутизаторами Интернета. А потому эффективная маршрутизация IP-пакетов стала попросту невозможной.

И тут на помощь пришел метод CIDR. Благодаря этой инновации одна единственная запись в таблице маршрутизации может представлять множество сетевых адресов низкого уровня. Также метод CIDR может служить «противоядием» гипотетическому исчерпанию пространства IP-адресов.

При использовании метода CIDR применяется собственный формат записи, в которой IP-адрес разбивается на сетевой и узловой разделы, причем сетевой раздел IP-адреса обозначается префиксом `/n`, где `n` определяет количество битов в этом разделе. Естественно, что для адреса из класса A используется префикс `/8`, из класса B — префикс `/16`, а из класса C — префикс `/24`.

Поскольку метод CIDR не предусматривает разбиения IP-адресов на классы, возможно применение таких «нестандартных» адресов, как 150.174.121.0/24. Число 150 определяет применение 16 битов в качестве сетевого раздела IP-адреса (как в случае с классами IP-адресов), а префикс `/24` определяет применение для сетевого раздела IP-адреса первых 24 битов, оставшиеся же 8 битов исполь-

зуются для адресации узлов в сети. Благодаря сетевому префиксу можно разбить непрерывное пространство адресов класса B на отдельные меньшие по размеру диапазоны.

В табл. 4.1 приведено соответствие между префиксами CIDR и эквивалентным диапазоном IP-адресов из класса C.

Таблица 4.1. Префиксы CIDR и эквивалентный диапазон из класса C

Префикс CIDR	Эквивалентный диапазон (количество узлов)
/27	1/8 класса C (32)
/26	1/4 класса C (64)
/25	1/2 класса C (128)
/24	1 класс C (256)
/23	2 класса C (512)
/22	4 класса C (1024)
/21	8 классов C (2048)
/20	16 классов C (4096)
/19	32 класса C (8192)
/18	64 класса C (16 384)
/17	128 классов C (32 768)
/16	256 классов C (65 536)
/15	512 классов C (131 072)
/14	1024 класса C (262 144)
/13	2048 классов C (524 288)

Следует обратить внимание на соответствие между количеством сетей из класса C и префиксами CIDR. Так, префикс /16 определяет предельно допустимое количество сетей из класса C (256), соответствующее одной сети из класса B. Следуя этой логике, можно прийти к выводу о том, что префикс /15 определяет две сети из класса B, префикс /14 — четыре сети и т. д.

Все современные маршрутизаторы поддерживают технологию CIDR, благодаря которой ушла в прошлое проблема «нехватки» IP-адресов. Эту проблему был призван решить протокол IPv6, речь о котором пойдет в следующем разделе.

Протокол IPv6

Стандарт, определяющий протокол IPv6, был разработан еще в 1995 году. Немалую роль в его появлении сыграла паника, возникшая из-за слухов о грядущем крахе Интернета по причине быстрого исчерпания доступного пространства IP-адресов. Но после появления IPv6 оказалось, что потребность в нем преувеличена, как это часто бывает.

В последующие годы были разработаны новые технологии, такие как преобразование сетевых адресов (NAT, Network Address Translation) и бесклассовая маршрутизация между доменами (CIDR, Classless Interdomain Routing), «про-

длившие жизнь» старому доброму IPv4. Именно поэтому победная поступь IPv6 несколько замедлилась, и в настоящее время он применяется исключительно в больших корпоративных сетях, а также в работе магистральных маршрутизаторов Интернета. Программная поддержка IPv6 встроена в операционные системы Windows XP и Windows Server 2003.

Протокол IPv6 позволил не только резко увеличить общий объем пространства IP-адресов, но и привнес ряд других свойств, благодаря чему он может постепенно вытеснить протокол IPv4.

Основным «родовым признаком» протокола IPv6 является то, что под IP-адрес отводится 128 битов, вместо прежних 32 битов. Адресный потенциал IPv6 себе даже трудно вообразить, особенно, если вспомнить, что IPv4 может поддерживать свыше 4 миллионов IP-адресов.

Преимущества, связанные с применением IPv6, не сводятся только к «раздуванию» пространства IP-адресов. Ниже перечислен целый ряд новых свойств, привнесенных протоколом IPv6:

- упрощение структуры заголовка IP-пакетов, благодаря чему ускоряется их маршрутизация;
- поддержка нового формата IP-заголовка;
- встроена поддержка идентификации и шифрования.

Ранее уже рассматривалась структура заголовка IP-пакета для протокола IPv4, теперь пришло время ознакомиться со структурой заголовка IP-пакета протокола IPv6 (рис 4.3).

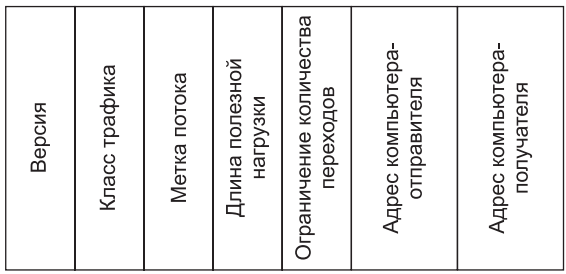


Рис. 4.3. Структура заголовка IP-пакета протокола IPv6

- Поле Version (Версия). Это 4-разрядное поле определяет версию протокола IP. Для протокола IPv4 указывалось значение 4. Для версии IPv6 в поле указывается значение 6. Это значение используется маршрутизаторами и другими сетевыми устройствами для определения типа обрабатываемого IP-пакета.
- Поле Traffic Class (Класс трафика). В этом поле задается так называемый «класс трафика».
- Поле Flow Label (Метка потока). Это 20-разрядное поле функционально схоже с полем Quality of Service, которое обрабатывается протоколом IPv4.

- Поле Payload Length (Длина полезной нагрузки). В этом 16-разрядном поле задается длина раздела IP-пакета, в котором передаются данные.
- Поле Next Header (Следующий заголовок). Одно из наиболее полезных свойств протокола IPv6 заключается в том, что, помимо основного заголовка IPv6, в IP-пакет можно включать дополнительные заголовки.
- Поле Hop Limit (Ограничение количества переходов). Назначение данного 8-разрядного поля аналогично назначению поля Time to Live (TTL), присущего протоколу IPv4. После каждого прохождения IP-пакета через маршрутизатор значение в поле уменьшается на единицу. Если значение в поле становится равным нулю, IP-пакет «списывается в утиль».
- Поле Source Address (Адрес компьютера-отправителя). IP-адрес (разрядностью в 128 битов), соответствующий компьютеру-отправителю IP-пакета.
- Поле Destination Address (Адрес компьютера-получателя). IP-адрес (разрядностью в 128 битов), соответствующий компьютеру-получателю IP-пакета.

Как правило, в большинстве пакетов после раздела заголовка следует раздел «полезной нагрузки», в котором содержатся фактические данные пакета. В некоторых случаях предусмотрен специальный завершающий раздел, который обычно используется для выполнения проверки целостности данных, благодаря чему можно удостовериться в том, что пакет был получен без искажений.

Поле Next Header определяет наличие дополнительного заголовка после текущего заголовка, следующего за исходным заголовком IPv6. Если принимающий узел не распознает следующий заголовок, он отвергает IP-пакет и отправляет ICMP-сообщение компьютеру-отправителю. В этом сообщении кратко описывается суть проблемы. Это ICMP-сообщение используется во многих случаях, связанных с обработкой данных протоколом IPv6.

После заголовка пакета IPv6 могут следовать дополнительные заголовки, указанные в списке.

- Поле Hop-by-Hop (Переход за переходом). При наличии подобного заголовка именно он проверяется маршрутизатором или другим сетевым устройством.
- Поле Destination Options (Параметры компьютера-получателя). Этот заголовок может иметь переменную длину и применяется для передачи некоторых дополнительных данных.
- Поле Routing (Маршрутизация). В этом поле определяются подключенные к сети компьютеры, через которые проходит IP-пакет на пути к пункту назначения. Обычно информация, хранящаяся в этом поле, применяется маршрутизаторами для определения оптимального маршрута следования пакетов в сети. Информация в этом поле носит рекомендательный характер.
- Поле Fragment (Фрагмент). Содержимое этого поля определяет фрагментацию пакетов данных на основе показателя MTU для компьютера-отправителя. Поскольку значения MTU для сетевых компьютеров, находящихся на пути следования пакета, могут отличаться, доставка пакетов по месту назначения не гарантирована. Повторная сборка пакетов компьютером-получателем возможна на основе изучения информации, содержащейся в поле Authentification.

- Поле Authentification (Идентификация). Название этого поля говорит само о себе.
- Поле Encapsulating Security Payload (Инкапсуляция раздела данных, связанного с обеспечением безопасности). Применяется для обеспечения безопасности.
- Поле Upper layer header (Заголовок верхнего уровня). Здесь описываются данные, которые находятся в разделе данных IP-пакета.

Дополнительные заголовки, связанные с протоколом IPv6, приводят к уменьшению полезных данных, «переносимых» IP-пакетом. Эта особенность должна учитываться протоколами верхнего уровня, реализующими управление передачей данных.

Теперь настала очередь протокола TCP, который тоже является одним из базовых сетевых протоколов.

Протокол TCP

Как и протокол IP, протокол TCP отвечает за передачу данных между сетевыми узлами. При использовании этого протокола задействованы дополнительные механизмы, позволяющие назвать его надежным. В отличие от протокола IP, протокол TCP выполняет предварительное согласование параметров канала связи и требует подтверждения доставки сообщения. Здесь уместна аналогия с работой обычной почты. Так, например, протокол IP действует по принципу «бросил письмо в почтовый ящик и забыл». Протокол TCP поступает «хитрее», он требует «уведомления о получении заказного письма». Причем, достаточно одного уведомления в ответ на доставку целой группы IP-пакетов. Данные, передаваемые протоколом TCP, называются *сегментами*.

Протокол TCP логически располагается на более высоком уровне, чем протокол IP. Он позволяет нескольким приложениям параллельно и независимо обмениваться данными с приложениями, запущенными на других машинах. Так же, как и UDP, протокол TCP демультиплексирует входной трафик между несколькими приложениями. Поэтому по аналогии с протоколом UDP, в протоколе TCP также используется понятие номеров портов, позволяющих идентифицировать конкретный компьютер-получатель информации. Каждому из портов для идентификации присваивается соответствующее целое число.

При описании протокола TCP используется понятие абстрактного соединения, осуществляемого с применением *виртуальных каналов связи*. Для каждого соединения назначаются *конечные точки соединения*. В данном случае под конечной точкой понимается целочисленная пара чисел вида *узел, порт*, где параметр *узел* определяет IP-адрес узла сети, а параметр *порт* определяет номер порта TCP для данного узла. Например, запись (139.15.1.5, 13) определяет конечную точку, которая характеризуется TCP-портом с номером 13, относящимся к компьютеру с IP-адресом 139.15.1.5.

Теперь, после формулирования понятия конечной точки, несложно определить термин «соединение». Поскольку любое соединение идентифицируется парой

определяющих его конечных точек, достаточно указать IP-адреса и TCP-порты для этих точек.

На самом деле это упрощенная модель соединения, поскольку в данном случае номера портов для соединений уникальны. На практике же бывает так, что одна и та же конечная точка используется несколькими соединениями. При этом неоднозначности не возникает, поскольку в протоколе TCP все соединения связаны с открытым соединением, определяемым парой конечных точек, а вовсе не с номерами портов.

Концепция абстрактного соединения играет важную роль в программировании. В частности, разработчик может создать программу, выполняющую один и тот же набор функций с несколькими открытыми соединениями. При этом нет необходимости использовать для каждого соединения уникальный номер локального порта. Например, в большинстве операционных систем поддерживается возможность одновременного доступа нескольких клиентов к службе электронной почты. Благодаря этому несколько клиентских компьютеров могут одновременно отправлять почтовые сообщения, а необходимость в этом возникает достаточно часто. Поскольку программа, принимающая входящие сообщения, использует для связи протокол TCP, для ее работы достаточно назначить лишь один локальный порт, несмотря на то, что могут одновременно обрабатываться несколько соединений.

Для реализации передачи данных при использовании протокола TCP требуется предварительная установка соединения. На практике это означает предварительную «договоренность» между конечными точками, участвующими в соединении. При этом «переговоры» ведутся приложениями, функционирующими на компьютерах, между которыми устанавливается соединение. Одно из приложений реализует функцию *пассивного открытия* соединения. Вызов подобной функции сигнализирует о том, что данная сторона готова к приему входящих соединений. После этого операционная система назначает номер TCP-порта для собственной конечной точки текущего соединения.

Приложение, которое выполняется на другом конце виртуального канала, обращается к операционной системе с запросом на *активное открытие* соединения. При этом два экземпляра протокола TCP взаимодействуют друг с другом. В ходе этого взаимодействия проверяется возможность установки соединения.

После того как соединение будет установлено, приложения могут начать процесс обмена данными. При этом экземпляры протокола TCP в фоновом режиме обмениваются служебными сообщениями, гарантирующими надежность доставки данных. Подробнее процесс установки соединения будет рассмотрен после изучения формата сообщения протокола TCP.

В протоколе TCP поток данных разбивается на сегменты, состоящие из последовательности байтов (октетов). Как правило, каждый сегмент данных передается в сети в виде единственной IP-дейтаграммы. Для повышения эффективности передачи данных и управления потоком данных в протоколе TCP используется специальный механизм *скользящих окон*. В этом случае экземпляр протокола TCP может отправлять сразу несколько сегментов данных еще до того, как будет

получено соответствующее сообщение относительно их доставки. Благодаря этому увеличивается общая пропускная способность сети, поскольку сокращается время ее простоя. Также становится реальной «голубая мечта разработчиков» — сквозное управление потоком данных. Получатель может использовать средства, позволяющие ограничить поток передаваемых данных в случае нехватки буферной памяти, используемой для хранения промежуточных данных.

Благодаря использованию скользящих окон протокол TCP оперирует октетами (байтами) данных (рис. 4.4, *а*), а не сегментами или пакетами. При этом октеты потока данных нумеруются последовательно, а компьютер-отправитель запоминает три указателя для каждого открытого соединения. Именно по этим указателям определяется скользящее окно (рис. 4.4, *б*).

Первый указатель обозначает левую границу скользящего окна. Он разделяет октеты на успешно доставленные получателю и те, которые отправлены в сеть, но подтверждение их успешной доставки еще не получено. Второй указатель обозначает правую границу скользящего окна. Он определяет номер старшего октета последовательности, который может быть передан в сеть до получения подтверждения о доставке других октетов, находящихся в окне. Третий указатель обозначает границу внутри окна, разделяющую последовательность октетов на уже отправленные в сеть и те, которые еще только предстоит отправить. Модуль протокола отправляет в сеть все октеты, находящиеся в окне, без задержки. Поэтому граница внутри окна, определяемая третьим указателем, обычно перемещается слева направо очень быстро.

Рис. 4.4. Скользящее окно протокола TCP

Экземпляр протокола TCP, выполняемый на компьютере-отправителе, перемещает окно вдоль последовательности октетов. Экземпляр протокола TCP, выполняемый на компьютере-получателе, формирует точно такое же окно для того, чтобы собрать поток получаемых данных. Следует учитывать, что соединения, устанавливаемые протоколом TCP, являются дуплексными. Это означает, что одновременно по каждому из виртуальных каналов можно передавать два потока данных в противоположных направлениях. Поэтому экземпляры протокола TCP, выполняемые на обоих концах соединения, поддерживают для каждого со-

единения по два окна. Одно окно в этой паре применяется для передачи потока данных, а второе — для их приема.

Размер окна в протоколе TCP не является постоянным. В каждом сообщении, подтверждающем получение данных, которое присылает получатель, указывается количество принятых октетов и *объявление окна*. В этом объявлении определяется количество дополнительных октетов данных, которые сможет принять получатель. В данном контексте объявление окна можно рассматривать в качестве сообщения, присылаемого получателем потока данных, в котором говорится о текущем размере буфера данных.

В ответ на получение объявления окна, в котором говорится об увеличении размеров, отправитель данных соответствующим образом увеличивает размер своего скользящего окна, отправляя дополнительные данные еще до того, как будет получено подтверждение о приеме данных. Если же получено объявление окна, в котором сообщается об уменьшении размеров, отправитель уменьшит размеры собственного скользящего окна, задерживая отправку байтов данных, выходящих за его пределы.

Экземпляр протокола TCP не обязан немедленно реагировать на прием объявления окна, в котором указаны уменьшенные размеры, смещая влево границу окна в потоке данных. Следует просто дождаться подтверждения приема данных, временно «замораживая» их отсылку. Поэтому спустя некоторое время размер окна уменьшится автоматически по мере смещения его левой границы вправо.

Благодаря окну переменного размера повышается надежность передачи данных и обеспечивается управление потоком данных. Чтобы не допустить переполнения буфера, следует по мере его заполнения отсылать объявления окон меньшего размера. Иногда в целях прекращения передачи данных получатель объявляет окно нулевого размера. Если же буфер памяти очистится, получатель отсылает объявление ненулевого окна для возобновления передачи данных.

Механизм управления потоком данных, используемый протоколом TCP, весьма важен для функционирования реальной сети, объединяющей множество других локальных сетей различной протяженности и пропускной способности. При этом возникают некоторые сложности. Первая проблема связана с различной производительностью компьютеров, подключенных к сети. В качестве решения этой проблемы используется сквозное управление потоком данных между компьютером-отправителем и компьютером-получателем. Следует обратить внимание на то, что применяемые в сети промежуточные устройства тоже должны уметь производить сквозной контроль данных. Если промежуточное устройство не справляется с поступающим потоком данных, наступает состояние *перегрузки*. В этом случае задействуются соответствующие механизмы устранения перегрузки.

Структура TCP-сегментов

Выше уже отмечалось, что в протоколе TCP передаваемые данные реализованы в виде сегментов, которые применяются для установки соединения, передачи данных, отправки сигналов подтверждения приема, объявления размера окон и закрытия соединения. Формат сегмента протокола TCP приведен на рис. 4.5.

Рис. 4.5. Структура заголовка сегмента TCP

Каждый сегмент состоит из заголовка и раздела данных. В заголовке располагаются идентификационные данные и управляющая информация. Его структура подробно описана в списке.

- Поле Source port (Порт компьютера-отправителя). Это 16-разрядное поле применяется для идентификации порта, используемого приложением, отсылающим данные.
- Поле Destination port (Порт компьютера-получателя). Это 16-разрядное поле применяется для идентификации порта компьютера-приемника.
- Поле Sequence number (Последовательный номер). Это 32-разрядное поле применяется для повторной сборки фрагментов в одно большое сообщение после получения IP-пакета.
- Поле Acknowledgment number (Номер подтверждения). Это 32-разрядное поле хранит сведения о последовательном номере подтверждения приема IP-пакета.
- Поле Data offset (Смещение данных). В этом 4-разрядном поле указывается количество разделов данных, формирующих заголовок IP-пакета. Именно это поле позволяет определить место нахождения раздела данных в пакете.
- Поле Reserved (Зарезервировано). Это 6-разрядное поле зарезервировано для использования в будущем.
- Поле URG. Это битовое поле определяет «срочность» данных, содержащихся в пакете.
- Поле ACK. Это поле определяет передачу подтверждения (Acknowledgment) о приеме пакета.
- Поле PSH. Это поле определяет состояние «выталкивания» для данных, содержащихся в пакете.
- Поле RST. Это битовое поле определяет переустановку соединения, если ему присвоено единичное значение.
- Поле SYN. Это битовое поле определяет синхронизацию передаваемых последовательных номеров.
- Поле FIN. Данное поле определяет завершение передачи данных.
- Поле Window (Окно). Данное 16-разрядное поле определяет количество блоков данных, принимаемых компьютером-получателем.
- Поле Checksum (Контрольная сумма). Это 16-разрядное поле обеспечивает проверку целостности разделов, содержащих заголовок и данные пакета.

- Поле Urgent pointer (Указатель срочности). Совместно с полем URG данное поле определяет «срочность» передаваемых данных.
- Поле Options (Параметры). При помощи этого поля переменной длины производится определение максимального размера передаваемых сегментов данных.

Поскольку протокол TCP является потоково-ориентированным, приложение, которое выполняется на одном конце соединения, может потребовать внеочередной отправки данных другому приложению. В данном случае речь идет о том, чтобы программа на другом конце соединения получила их сразу, не ожидая приема октетов, которые были отправлены раньше. Например, если протокол TCP используется для установки сеанса связи с удаленным терминалом, пользователю иногда нужно послать удаленной программе специальный сигнал с клавиатуры, который прервет ее выполнение. Обычно подобные сигналы посылаются, если программа, выполняемая удаленным компьютером, зависла или претерпела фатальный сбой. В данном случае управляющие сигналы должны передаваться программе вне очереди, без ожидания, пока она считает из входного потока все посланные ранее октеты. В противном случае, если программа по какой-либо причине прекратит считывание потока данных, то управляющие сигналы никогда не попадут по месту назначения.

Для реализации режима передачи внеочередных сигналов в протоколе TCP для отправителя предусмотрена возможность задавать в сегменте метку срочности. Это означает, что программа-получатель должна быть извещена о поступлении таких данных насколько возможно быстро, вне зависимости от состояния входящего потока данных. В спецификации протокола указано, что после поступления срочных данных экземпляр протокола TCP должен уведомить приложение, открывшее соединение, о переходе в «срочный режим» работы. После того как набор срочных данных будет получен, экземпляр протокола TCP уведомляет приложение о переходе в обычный режим работы.

Естественно, все детали механизма уведомления прикладной программы о прибытии срочных данных зависят от используемой на компьютере операционной системы. Однако при отправке срочных данных этот механизм унифицирован. Для этого полю URG присваивается единица, а полю указателя срочных данных присваивается соответствующее значение. Если полю URG присвоена единица, поле указателя срочных данных определяет позицию в сегменте, где завершается раздел «срочных» данных.

Через открытое соединение отсылаются сегменты данных, имеющие различный размер. Естественно, обе стороны должны заранее «договориться» о максимально допустимой длине передаваемого сегмента. Для обмена информацией с модулем протокола TCP, запущенным на противоположной стороне соединения, используется поле параметров протокола (Options). Один из этих параметров позволяет определить максимальный размер сегмента (MSS, Maximum Segment Size). Например, если небольшой компьютер, оснащенный малым объемом оперативной памяти, подключается к мощному суперкомпьютеру, сначала требуется передать последнему сведения о максимальном размере сегмента. Иначе может сложиться такая ситуация, что получаемые от суперкомпьютера сегменты не поместятся в выделенном для этой цели буфере памяти.

Этот параметр играет важную роль, если компьютеры подключены к высокоскоростной локальной сети. Для увеличения пропускной способности сети максимальный размер сегмента должен быть таким, чтобы он целиком помещался в пакете данных. Поэтому, если отправитель и получатель находятся внутри одной физической сети, экземпляр протокола TCP обычно выбирает максимальный размер сегмента таким образом, чтобы результирующая IP-дейтаграмма соответствовала максимальному размеру модуля данных (MTU), который передается в физической сети. Если же отправитель и получатель находятся в разных физических сетях, то можно попытаться определить минимальный размер MTU сети, находящейся по пути передачи пакетов, или установить максимальный размер сегмента равным 536 байтам. Это значение получается путем вычитания из стандартного размера IP-дейтаграммы (576 байтов) значения стандартного размера заголовков пакетов IP и TCP.

Ранее уже упоминалось, что проблема выбора оптимального размера сегмента данных TCP достаточно сложна, поскольку пропускная способность сети падает при передаче как очень больших, так и слишком малых сегментов. При небольшом размере сегмента эффективность сети будет невысокой. Следует помнить, что сегменты данных TCP в процессе передачи встраиваются в IP-дейтаграммы, а они, в свою очередь инкапсулируются во фреймы данных, передаваемые в сети. Поэтому, помимо раздела данных, каждый сегмент содержит, как минимум еще 40 байтов для заголовков TCP-сегмента и IP-дейтаграммы. Из-за этого при передаче дейтаграммы, содержащей только один байт данных, передача пользовательских данных занимает незначительную часть выделенной полосы пропускания сети. А если учесть минимальный межпакетный промежуток и биты синхронизации фреймов, автоматически добавляемые сетевым оборудованием, то это соотношение будет еще меньше.

Чересчур большие сегменты данных тоже вредны, поскольку их использование приводит к падению пропускной способности сети. Это связано с тем, что большие сегменты данных приводят к формированию громоздких IP-дейтаграмм. В процессе передачи подобной дейтаграммы в сети с малым значением коэффициента MTU происходит ее фрагментация при помощи протокола IP. В отличие от TCP-сегментов, подтверждение получения каждого фрагмента на уровне протокола не выполняется, а отдельные фрагменты дейтаграммы при необходимости не могут быть повторно переданы независимо от всей дейтаграммы. Таким образом, в случае утери или повреждения одного из фрагментов данных повторно должна быть передана вся дейтаграмма. Поскольку отдельные фрагменты время от времени теряются, увеличение размеров сегмента больше порога фрагментации уменьшает вероятность успешного приема дейтаграммы и, следовательно, ведет к уменьшению пропускной способности сети.

Теоретически оптимальный размер сегмента определяется максимально возможным размером формируемых IP-дейтаграмм, которые на протяжении маршрута от компьютера-отправителя до конечного получателя не фрагментируются. На практике определение этого значения затруднено в силу нескольких причин. Во-первых, в большинстве реализаций протокола TCP не используется механизм определения оптимального размера сегмента. Во-вторых, поскольку маршрутизаторы могут динамически изменять маршруты дейтаграмм, возможно

изменение пути их следования между двумя взаимодействующими компьютерами. Следовательно, величина MTU в любой момент может измениться, после чего неминуемо последует фрагментация дейтаграммы. В-третьих, оптимальный размер сегмента зависит от длины заголовков протоколов более низкого уровня. Кроме того, при использовании параметров протокола IP размер сегмента должен быть еще меньше. Поэтому проблема определения оптимального размера сегментов протокола TCP до сих пор не разрешена.

ПРИМЕЧАНИЕ Подробное рассмотрение принципов функционирования маршрутизаторов производится в следующей главе.

Поле контрольной суммы применяется для проверки целостности полученных данных и заголовка TCP-сегмента. В процессе вычисления контрольной суммы экземпляр протокола TCP, выполняющийся на компьютере-отправителе, использует соответствующий алгоритм.

Перед вычислением контрольной суммы к началу сегмента добавляется *псевдозаголовок*, а конец сегмента дополняется требуемым количеством нулевых битов. После выполнения описанных подготовительных действий вычисляется значение 16-разрядной контрольной суммы. Длина псевдозаголовка и битов, добавленных в процессе заполнения, не учитывается в общей длине TCP-сегмента, поскольку они не передаются получателю. Кроме того, при вычислении само значение поля контрольной суммы TCP-заголовка полагается равным нулю.

В процессе вычисления контрольной суммы используется двоичная арифметика, когда отрицательные числа представляются в инверсном виде. Затем полученный результат инвертируется, в результате чего формируется положительное значение контрольной суммы. После получения сегмента данных принимающим компьютером, экземпляр протокола TCP выполняет над ним аналогичные вычисления, а затем сравнивает значения контрольных сумм. Если эти величины совпадают, то процесс передачи сегментов данных выполнен без ошибок.

Благодаря псевдозаголовку компьютер-получатель может удостовериться в том, что сегмент данных доставлен по назначению. Для этого проверяются IP-адреса отправителя и конечного получателя, а также номера порта протокола. В протоколе TCP IP-адреса отправителя и конечного получателя играют очень важную роль, поскольку они используются для идентификации соединения, к которому относится полученный сегмент данных. Поэтому после прибытия дейтаграммы, содержащей TCP-сегмент, экземпляр протокола IP должен передать экземпляру протокола TCP, кроме самого сегмента, еще и IP-адреса отправителя и конечного получателя.

Поскольку в протоколе TCP данные посылаются в виде сегментов переменного размера и в повторно передаваемые сегменты, кроме оригинала, могут быть включены дополнительные данные, получаемые сигналы подтверждения приема не так-то просто соотнести с отправленными дейтаграммами или сегментами. По этой причине сигналы подтверждения приема соотносятся с положением данных в потоке, которым присваиваются порядковые номера. Получатель собирает поступившие в сегментах данные и воспроизводит точную копию передаваемого потока данных. Так как сегменты поступают получателю в виде IP-дейтаграмм,

то для упорядочения сегментов получатель использует их порядковые номера. В какой-то момент у получателя может быть восстановлено произвольное количество байтов.

Кроме того, получателю может быть доставлена некая часть потока в виде полученных вне очереди дейтаграмм. Несмотря на это, получатель всегда посылает сигналы подтверждения приема только на самую большую и непрерывную часть потока, которая была корректно получена. В каждом подтверждении приема указывается порядковый номер, который соответствует положению самого старшего байта в непрерывной части доставленного потока. Таким образом, по мере передачи потока данных отправитель постоянно получает сигналы подтверждения, отражающие состояние принятого потока данных.

Принятую в протоколе TCP систему подтверждения приема называют *накопительной*, поскольку она отражает количество байтов потока данных, накопленных получателем. Следует отметить, что накопительная система подтверждения приема имеет как преимущества, так и недостатки. Одно из преимуществ заключается в том, что сигналы подтверждения приема легко генерируются и являются однозначными. Их просто невозможно истолковать неправильно. Еще одно преимущество заключается в том, что в случае утери сигналов подтверждения приема не требуется повторно передавать ни сами сигналы, ни соответствующие им сегменты данных. Недостатком накопительного метода является то, что отправитель не обладает сведениями о том, что передача данных завершилась успешно. Ему только известно, какая часть потока данных была успешно доставлена получателю.

Описанную технологию может иллюстрировать простой пример. Предположим, имеется окно, расположенное в потоке данных начиная с позиции 201 и включающее 3000 байтов. Предположим также, что отправитель передал все находящиеся в окне данные в виде трех сегментов. Что произойдет в том случае, когда первый сегмент в процессе передачи данных был утерян, а остальные успешно достигли места назначения? Во время получения сегментов, получатель будет отсылать сигналы подтверждения. В каждом из них будет указан порядковый номер байта (201), то есть номер следующего по порядку старшего байта, относящегося к непрерывному потоку данных, который ожидает получить принимающая сторона. При этом получатель лишен возможности сообщить отправителю, что большая часть данных, принадлежащих текущему окну, уже получена.

Как только истечет время ожидания сигнала подтверждения приема, отправитель попытается выйти из сложившейся ситуации, используя один из следующих двух методов. Он может передать либо один сегмент данных, либо все три. Очевидно, что последний метод весьма неэффективен. После того как первый сегмент данных будет успешно доставлен, в распоряжении получателя окажутся данные, образующие окно. Поэтому он подтвердит прием байта с порядковым номером 3001. Таким образом, если отправитель будет действовать согласно принятым стандартам и выполнит повторную передачу первого непринятого сегмента данных, то прежде чем предпринимать дальнейшие шаги, он должен дождаться подтверждения приема этого сегмента. При этом не ощущается преимущество, предоставляемое большим окном.

Метод обработки истекшего времени ожидания и выполнение повторной передачи данных являются основными технологиями протокола TCP. Как и в других надежных протоколах, в протоколе TCP предполагается, что получатель пришлет сигнал подтверждения приема, успешно получив байты из потока данных. Каждый раз при отправке сегмента в модуле протокола TCP устанавливается значение таймера ожидания, определяющего получение сигнала подтверждения приема данных. Если время ожидания истечет прежде, чем будет подтвержден прием отправленного сегмента, экземпляр протокола TCP полагает, что сегмент данных не достиг компьютера-получателя, либо соответствующие данные были искажены в процессе передачи. После этого передача сегмента производится повторно.

Протокол TCP изначально предназначался для применения в межсетевой среде. Пакет данных может передаваться по сетям, обладающими различными скоростными характеристиками, в связи с чем невозможно заранее предсказать, как быстро отправитель получит сигнал подтверждения приема. Ситуация усугубляется еще и тем, что задержка прохождения сигнала через маршрутизаторы зависит от величины трафика в конкретной сети. Поэтому суммарное время задержки на передачу сегмента и получение отправителем подтверждения его приема может колебаться в очень широких пределах.

В целях определения времени задержки сигнала в протоколе TCP используется адаптивный алгоритм повторной передачи. Принцип его работы заключается в том, что отслеживается производительность каждого сетевого соединения, а затем на основании полученных результатов выбирается подходящее время задержки. По мере изменения значения производительности соединения соответственно изменяется и величина задержки.

В процессе сбора данных, требуемых для работы адаптивного алгоритма, экземпляр протокола TCP фиксирует время отправки каждого сегмента, а также время получения сигналов подтверждения приема данных, находящихся в этих сегментах. Затем определяется разность этих значений, соответствующая времени доставки каждого пакета. Этот алгоритм также называется оценкой полного времени доставки пакета. После выполнения очередной оценки экземпляр протокола TCP пересчитывает среднее время доставки для данного соединения. При этом также оценивается средневзвешенная величина полного времени доставки пакетов (RTT, Round Trip Time).

В процессе отправки пакета экземпляр протокола TCP вычисляет величину задержки в виде функции от предполагаемой величины полного времени доставки.

Оценка полного времени доставки пакета не составляет особого труда. Для этого следует из значения времени получения сигнала подтверждения доставки сегмента вычесть значение времени отправки сегмента. В этом случае могут возникать определенные затруднения, поскольку в протоколе TCP используется накопительная система подтверждения приема сегментов данных. Ее суть заключается в том, что сигнал подтверждения приема отражает факт успешного получения данных, но не той дейтаграммы, в которой эти данные находятся.

Следует подробнее рассмотреть процесс повторной передачи данных. Сначала экземпляр протокола TCP формирует сегмент данных, помещает его в дейта-

грамму и отправляет ее компьютеру-получателю. По истечении времени задержки выполняется повторная передача сегмента данных, но уже в составе другой дейтаграммы. Поскольку в обеих дейтаграммах содержатся одни и те же данные, отправитель не может определить, в какой из дейтаграмм (исходной или повторной) содержится полученный сигнал подтверждения приема данных. Здесь возникает проблема неоднозначности сигналов подтверждения приема данных. Рано или поздно сигнал подтверждения приема будет получен, даже если для этого потребуется выполнить одну или несколько повторных передач сегмента данных. В результате экземпляр протокола TCP оценит полное время доставки сегмента относительно времени его первоначальной посылки и на основе этого большого значения вычислит новое значение коэффициента RTT. Таким образом, по сравнению с прежним значением, новое значение коэффициента RTT вырастет незначительно. В следующий раз, когда экземпляр протокола TCP будет отправлять сегмент данных получателю, увеличенное значение коэффициента RTT приведет к заметному увеличению тайм-аута, относящегося к подтверждению приема. Поэтому, если сигнал подтверждения приема данных будет получен также после одной или нескольких повторных передач сегмента данных, полное время доставки сегмента будет еще больше.

Нельзя также соотносить сигнал подтверждения приема со временем самой последней повторной передачи сегмента. Если внезапно возрастет полное время доставки сегмента, то ситуация изменится. При отправке сегмента экземпляром протокола TCP для вычисления времени тайм-аута будет использоваться прежнее невысокое значение предполагаемого полного времени доставки пакета. Предположим, что после успешной доставки сегмента получателю, отправителю был послан сигнал подтверждения приема. Однако из-за перегрузок в сети сигнал подтверждения приема не будет получен до истечения значения таймера. В этом случае модуль протокола TCP выполнит повторную передачу сегмента. Вскоре после этого отправитель получит первый сигнал подтверждения приема и соотнесет его с моментом последней повторной передачи. Оцененное полное время доставки пакета будет небольшим, что приведет к незначительному снижению значения предполагаемого полного времени доставки пакета. К сожалению, уменьшение значения коэффициента RTT приведет к тому, что для передачи следующего сегмента данных экземпляр протокола TCP выберет малое значение тайм-аута.

Впрочем, в конечном итоге значение предполагаемого полного времени доставки пакета стабилизируется. Проведенные исследования показали, что в тех реализациях протокола TCP, где сигналы подтверждения приема соотносятся с моментом последней повторной передачи сегмента, стабильное значение RTT немного меньше половины корректного значения полного времени доставки. Следовательно, при отсутствии потерь сегментов в сети, модуль протокола TCP будет два раза посылать один и тот же сегмент получателю.

В предыдущем разделе шла речь о том, что независимо от того, к какому из моментов времени будет соотнесен полученный сигнал подтверждения приема, оценка полного времени доставки пакета будет неточной. Как же быть в этом случае? Ответ на этот вопрос очень прост. Экземпляр протокола TCP в этом случае не будет повторно подсчитывать значение предполагаемого полного вре-

мени доставки пакета на основе данных, полученных при повторной передаче сегмента. Величина предполагаемого полного времени доставки пакета (*алгоритм Карна*) вычисляется исключительно на основании данных, полученных для однозначных сигналов подтверждения приема.

Теперь стоит рассмотреть ситуацию, которая возникнет, если в момент отправки сегмента данных экземпляром протокола TCP резко увеличится время задержки в сети. Значение тайм-аута вычисляется на основании текущего значения предполагаемого полного времени доставки пакета. Для больших задержек в сети вычисленное значение тайм-аута будет незначительным. Это приведет к повторной передаче сегмента данных. Таким образом, если игнорировать сигналы подтверждения приема для повторно переданных сегментов, новое значение предполагаемого полного времени доставки пакета никогда не изменится, и описанный выше процесс будет продолжаться до тех пор, пока не уменьшится время задержки.

Чтобы устранить подобные недостатки, в алгоритме Карна используется метод коррекции значения тайм-аута (так называемый «откат таймера»). Его суть заключается в том, что начальное значение тайм-аута вычисляется на основании текущих данных. Но если в результате истечения тайм-аута произойдет повторная передача сегмента, то экземпляр протокола TCP увеличит значение тайм-аута. На практике каждый раз перед повторной передачей сегмента модуль протокола TCP увеличивает значение тайм-аута. Чтобы не допустить бесконтрольного увеличения тайм-аута, в большинстве его реализаций имеет место максимально возможное значение, которое всегда больше максимально возможной задержки передачи пакета по любому из маршрутов, проложенных в локальной сети.

Алгоритм вычисления нового значения тайм-аута зависит от конкретной реализации протокола TCP. В большинстве реализаций протокола эта величина вычисляется путем умножения прежнего значения тайм-аута на специальный корректирующий множитель. Обычно величина этого множителя выбирается равной двум. Если эта величина будет меньше двух, система может работать нестабильно.

Для того чтобы решить проблему вычисления постоянного предполагаемого полного времени доставки пакета, в алгоритме Карна используется методика принудительного изменения тайм-аута. При вычислении предполагаемого полного времени доставки пакета игнорируются результаты замеров, относящихся к повторно отправленным сегментам. В целях определения точного времени доставки пакетов в алгоритме Карна используется метод приращения значения тайм-аута при повторной передаче сегмента данных. Учитывая все выше сказанное, можно отметить, что в случае возникновения больших задержек в сети алгоритм Карна позволяет разделить вычисление текущего значения тайм-аута и определение предполагаемого полного времени доставки пакета.

Предполагаемое значение полного времени доставки используется только для вычисления начального значения тайм-аута. При каждой повторной передаче сегмента данных значение тайм-аута увеличивается на некоторую величину до тех пор, пока этот сегмент не будет успешно доставлен получателю. Таким образом, при отправке последовательности сегментов используется значение тайм-аута, полученное в результате принудительной коррекции значения таймера. Это происходит до тех пор, пока не будет получен сигнал подтверждения приема, соответствующий

однократно посланному сегменту данных. После этого экземпляр протокола TCP, основываясь на выполненном замере, пересчитывает предполагаемое значение полного времени доставки и соответствующим образом изменяет значение тайм-аута. Как показывает практика, алгоритм Карна идеален для применения в тех сетях, где потери данных весьма велики.

Исследования, в ходе которых вычислялось предполагаемое значение полного времени доставки пакетов, показали, что описанные методы неприменимы в том случае, если значение времени задержки в сети сильно изменяется. Эта проблема была учтена в спецификации протокола TCP, выпущенной в 1989 году, где требовалось, чтобы оценивалось среднее время полной доставки пакетов, а также величина статистического разброса.

Разработчики протокола TCP предусмотрели ситуации, связанные с возникновением перегрузки в сети. Признаком возникновения подобной ситуации может служить резкое увеличение времени задержки при доставке пакетов. При перегрузке устройства маршрутизации задержка увеличивается, поскольку поступающие дейтаграммы ставятся в очередь и находятся там до тех пор, пока маршрутизатор не сможет их обработать. Следует учитывать то, что емкость памяти маршрутизатора является конечной, поэтому она рано или поздно исчерпывается. Иными словами, при передаче дейтаграмм в сети для каждого TCP-соединения увеличения выделяемой памяти не происходит.

В самом худшем варианте, когда дейтаграммы не могут поместиться в памяти нагруженного маршрутизатора, они просто теряются. Как правило, в конечных точках соединения неизвестно, в каком месте сети и по какой причине возникла перегрузка. Для них перегрузка просто означает увеличение задержки.

К сожалению, в большинстве транспортных протоколов используется стратегия повторной передачи пакетов в случае истечения времени ожидания сигнала. Поэтому увеличение задержки вызывает повторную передачу дейтаграмм, что, в свою очередь, приводит к еще большей задержке. Если ничего не предпринимать, то увеличение трафика вызовет увеличение задержки, а рост времени задержки снова приведет к увеличению трафика в сети, и т. д. до тех пор, пока работа сети не будет полностью парализована. Подобная ситуация называется *полным коллапсом сети*.

Чтобы избежать полного коллапса сети, в случае возникновения перегрузки экземпляр протокола TCP должен уменьшить интенсивность передачи пакетов. Маршрутизаторы постоянно отслеживают длину внутренней очереди дейтаграмм, а в случае ее переполнения сообщают о возникшей перегрузке всем компьютерам-отправителям, используя механизм, подобный рассылке ICMP-сообщений. Однако протоколы транспортного уровня тоже могут регулировать степень перегрузки в сети, автоматически снижая интенсивность передачи данных при возникновении задержек. Применяемые при этом алгоритмы должны быть тщательно продуманы, поскольку даже при обычных условиях полное время доставки пакета в сети может варьироваться в очень широких пределах.

Для предотвращения перегрузки в сети современная версия стандарта TCP рекомендует использовать медленный запуск и мультипликативное уменьшение. Обе методики взаимосвязаны и могут быть легко реализованы на практике. Ранее уже упоминалось о том, что для каждого открытого соединения экземпляр

протокола TCP хранит размер окна получателя. Чтобы избежать перегрузки, в протоколе TCP установлено еще одно ограничение, которое называется ограничением размера окна перегрузки. При возникновении перегрузки оно ограничивает поток данных настолько, чтобы он был меньше размера буфера приема данных.

В стационарном режиме при неперегруженном соединении размер окна перегрузки совпадает с размером окна получателя. При уменьшении размера окна перегрузки уменьшается поток данных, передаваемый экземпляром протокола TCP через конкретное соединение. Чтобы определить ориентировочный размер окна перегрузки, модуль протокола TCP считает, что большая часть дейтаграмм теряется из-за перегрузки. При этом используется описанная далее стратегия мультипликативного уменьшения. Каждый раз после возникновения перегрузки размер окна перегрузки уменьшается в два раза, вплоть до минимума, соответствующего одной дейтаграмме. Для тех сегментов данных, которые попали в окно нового размера, применяется стратегия экспоненциального увеличения значения таймера тайм-аута.

Поскольку в протоколе TCP при каждой потере пакета размер окна перегрузки уменьшается в два раза, размер основного окна передачи уменьшается по экспоненциальному закону. Другими словами, при возникновении перегрузки экземпляр протокола TCP уменьшает величину потока данных в сети. При этом интенсивность повторной передачи сегментов также снижается экспоненциально. При продолжительной перегрузке экземпляр протокола TCP, в конечном счете, ограничивает интенсивность передачи данных до одной дейтаграммы и удваивает значение тайм-аута перед повторной передачей сегмента. Идея состоит в том, чтобы в критических ситуациях система могла резко уменьшить величину потока данных в сети.

В этом случае маршрутизаторы получат время, достаточное для проверки и аннулирования «лишних» дейтаграмм, находящихся в их внутренней очереди. Теперь следует рассмотреть методику восстановления работоспособности системы после устранения перегрузки. На первый взгляд создается впечатление, что все должно выполняться в обратном порядке. То есть, как только сеть возвращается в обычный режим работы, размер окна перегрузки должен удваиваться. Однако следствием подобных действий может стать нестабильность работы системы. Ее состояние будет постоянно изменяться в широких пределах — от перегруженности до полного отсутствия трафика. Поэтому в протоколе TCP для постепенного увеличения интенсивности передачи данных используется *метод медленного запуска*.

Этот метод предназначен для восстановления работоспособности сети после перегрузки, а также для начала передачи данных по новому соединению. При этом первоначальный размер окна перегрузки выбирается равным одному сегменту, и каждый раз после получения сигнала подтверждения приема размер увеличивается на один сегмент. Таким образом, метод медленного запуска позволяет избежать коллапса сети сразу после прекращения перегрузки или при начале передачи данных по новому соединению.

Словосочетание «медленный запуск» не должно никого вводить в заблуждение, поскольку в идеальных условиях запуск механизма передачи данных происходит не столь уж медленно. Первоначально размер окна перегрузки устанавливается равным одному сегменту, после чего выполняется передача этого сегмента,

и система переходит в состояние ожидания. После получения сигнала подтверждения приема этого сегмента размер окна перегрузки устанавливается равным двум сегментам, после чего посылается уже два сегмента и система снова переходит в состояние ожидания. После получения каждого из двух сигналов подтверждения приема этих сегментов размер окна перегрузки снова увеличивается на один сегмент. Поэтому модуль протокола TCP может отправить уже четыре сегмента. После получения четырех сигналов подтверждения приема размер окна перегрузки будет равен уже восьми сегментам. Таким образом, после завершения четырех циклов передачи-приема, модуль протокола TCP может отправить уже шестнадцать сегментов, что часто превышает размеры приемного окна получателя пакетов. Таким образом, перед тем, как модуль протокола TCP сможет отправить N сегментов, он должен выполнить $\log_2 N$ циклов передачи-приема. Очевидно, что даже в случае очень больших размеров окон выход системы на проектную мощность будет довольно быстрым.

Чтобы не допустить слишком быстрого увеличения размеров окна и возникновения перегрузки, в протокол TCP введено дополнительное ограничение. Как только размер окна перегрузки достигнет половины своего первоначального значения, экземпляр протокола TCP переходит к фазе аннулирования перегрузки и снижает скорость нарастания размеров этого окна. Во время этой фазы размер окна перегрузки увеличивается на единицу только в том случае, если для всех сегментов, находящихся в окне, будут получены сигналы подтверждения приема.

Ранее уже отмечалось, что коммуникационные протоколы разделены на логические уровни, благодаря чему значительно облегчается их дальнейшая разработка и модернизация. Однако разделение на уровни имеет недостатки, связанные с тем, что функционирование приложений на каждом из уровней осуществляется независимым образом. Например, протокол TCP ориентирован на обмен данными между двумя конечными точками соединения. Поэтому его работоспособность сохраняется при изменении маршрута следования дейтаграмм между этими точками. Несмотря на это изоляция уровней непосредственно сказывается на возможности взаимодействия между ними. В частности, хотя экземпляр протокола TCP, выполняющийся на компьютере-отправителе, может взаимодействовать с экземпляром протокола, который выполняется на компьютере-получателе, он не может взаимодействовать с экземплярами протоколов более низкого уровня, находящимися на пути следования пакетов. Таким образом, экземпляры протокола TCP компьютеров отправителя и получателя никогда не смогут получить отчет о текущем состоянии сети, а также проинформировать модули протоколов низкого уровня, находящиеся на пути следования пакетов о начале передачи данных.

Отсутствие методов взаимодействия между уровнями часто приводит к тому, что изменение алгоритма работы или программы реализации на одном из уровней кардинальным образом влияет на производительность более высоких уровней. В случае с протоколом TCP от алгоритмов, которые используют маршрутизаторы для обработки дейтаграмм, в значительной степени зависит как производительность одного TCP-соединения, так и суммарная пропускная способность всех соединений. Например, если при обработке одних дейтаграмм в маршрутизаторе будет возникать большая задержка, чем при обработке других, то это приведет

к увеличению тайм-аута при повторной передаче данных протоколом TCP. Если эта задержка превысит величину тайм-аута, будет считаться, что в сети возникла перегрузка. Поэтому, несмотря на то что стандарты протоколов каждого уровня определены независимо от стандартов остальных уровней, разработчики попытались продумать и реализовать механизм взаимодействия между протоколами разных уровней.

Одно из основных взаимодействий между модулями протоколов IP и TCP происходит в случае перегрузки маршрутизатора, из-за которой теряются дейтаграммы. Поскольку маршрутизатор помещает каждую вновь прибывшую дейтаграмму в очередь на обработку, основное внимание инженеров было сосредоточено на алгоритмах манипуляции элементами этой очереди. Если скорость поступления дейтаграмм превышает скорость их обработки в маршрутизаторе, размер очереди будет постоянно увеличиваться. Если же маршрутизатор перенаправляет дейтаграммы быстрее, чем они поступают, размер очереди сокращается. Поскольку объем оперативной памяти маршрутизатора ограничен, размер очереди не может увеличиваться до бесконечности. Поэтому в ранних версиях программного обеспечения маршрутизаторов при переполнении очереди использовалась методика *усечения хвоста очереди*.

Суть этой методики заключается в том, что переполнение буферной памяти маршрутизатора приводит к тому, что все новые дейтаграммы просто отклоняются. Эта методика необычным образом сказывается на работе протокола TCP. В простейшем случае, когда в проходящих через маршрутизатор дейтаграммах содержатся сегменты, относящиеся к одному TCP-соединению, потеря дейтаграмм приводит к использованию методики медленного запуска. В результате производительность TCP-соединения падает до тех пор, пока не начнут приходить сигналы подтверждения приема. Если через маршрутизатор проходят дейтаграммы, относящиеся к разным TCP-соединениям, применение методики усечения хвоста очереди приводит к эффекту глобальной синхронизации.

Чтобы понять суть проблемы, следует отметить, что обычно дейтаграммы поступают на маршрутизатор вперемешку (то есть друг за другом могут быть получены дейтаграммы от разных компьютеров-отправителей). Поэтому усечение хвоста очереди в этом случае вызывает потерю одного сегмента в каждом из N соединений, а не потерю N сегментов, относящихся к одному соединению. Потеря сегментов во всех N соединениях заставляет модули протоколов TCP этих соединений одновременно переходить к медленному запуску.

Как же избежать эффекта глобальной синхронизации в маршрутизаторе? Для этого необходим алгоритм, который позволит избежать усечения хвоста очереди там, где это возможно. И такой алгоритм был найден (RED, Random Early Detection). Для описания принципов работы этого алгоритма применяются три простых правила:

- если количество дейтаграмм в очереди не превышает значение T1, новая дейтаграмма добавляется в конец очереди;
- если количество дейтаграмм в очереди попадает в диапазон между T1 и T2, отклоняется одна из дейтаграмм, выбор которой осуществляется случайным образом с некоей вероятностью;

- если количество дейтаграмм в очереди превышает T2, все вновь поступившие диаграммы отбрасываются.

Благодаря методике случайного выбора, заложенной в RED, маршрутизатор по мере увеличения перегрузки переходит к постепенному и случайному удалению дейтаграмм. В этом ее коренное отличие от алгоритма усечения хвоста очереди, при использовании которого в случае переполнения очереди большое количество TCP-соединений переводится в состояние медленного запуска.

Суть метода RED, используемого маршрутизаторами, заключается в следующем. Если входная очередь дейтаграмм переполнена, то все вновь поступающие дейтаграммы отклоняются. Если же входная очередь не заполнена до конца, но ее размер превышает заранее установленный минимальный порог, то, во избежание эффекта глобальной синхронизации, отменяется одна из поступивших дейтаграмм, выбранная случайным образом в соответствии с заданной долей вероятности. Ключом к эффективной работе метода RED является правильный выбор пороговых значений T1 и T2, а также величины вероятности потери дейтаграммы.

Значение T1 должно быть достаточно большим, чтобы обеспечить высокую пропускную способность выходного канала связи. Когда размер очереди превосходит T2, алгоритм RED работает так же, как и алгоритм усечения хвоста очереди. Поэтому значение T2 должно быть больше T1 по крайней мере на среднюю величину увеличения размера очереди за время одной полной доставки TCP-сегмента. В противном случае использование алгоритма RED может привести к тем же глобальным колебаниям трафика в сети, что и при использовании метода усечения хвоста очереди.

Самой сложной задачей в алгоритме RED является нахождение значения вероятности потери дейтаграммы. Очевидно, что эта величина не может быть постоянной и должна вычисляться заново для каждой из вновь прибывших дейтаграмм. Ее значение зависит от текущего размера очереди и установленных пороговых значений T1 и T2. Применяемая в этом случае идея будет понятнее, если описать алгоритм, используемый в RED, с вероятностной точки зрения.

Если размер очереди меньше величины, определяемой параметром T1, потери дейтаграмм не происходит. Поэтому можно считать, что в этом случае значение вероятности потерь равно нулю. Когда же размер очереди превышает T2, отклоняются все дейтаграммы. Поэтому в последнем случае значение вероятности равно единице. Если размер очереди колеблется между T1 и T2, значение вероятности отклонения дейтаграммы изменяется по линейному закону (в промежутке между 0 и 1).

Линейный алгоритм оценки вероятности может быть положен в основу используемого методикой RED метода вычисления вероятности потери дейтаграммы. Однако в него следует внести изменения, чтобы система не столь бурно реагировала на изменение степени загрузки сети. Это вызвано тем, что в реальной сети значение сетевого трафика постоянно изменяется в весьма широких пределах. В результате размер внутренней очереди маршрутизатора также отличается высокой степенью вариабельности. Если в алгоритме RED применяется упрощенный линейный метод, то вероятность отклонения последних дейтаграмм, поступивших в одном блоке, который и вызвал перегрузку, будет очень большой.

Причина этого заключается в том, что дейтаграммы поступают в память маршрутизатора в тот момент, когда размер его внутренней очереди становится очень большим. Но маршрутизатор не должен без крайней необходимости отклонять полученные дейтаграммы, поскольку это отрицательно сказывается на производительности TCP-соединения. Поэтому при возникновении кратковременной перегрузки в сети нет необходимости удалять дейтаграммы, так как внутренняя очередь маршрутизатора заведомо не переполнится. С другой стороны, удаление дейтаграмм следует производить вовремя, иначе неизбежно наступает момент, когда очередь начнет переполняться очень быстро.

Каким же образом в алгоритме RED определять более высокую вероятность отклонения дейтаграмм по мере увеличении размера внутренней очереди и при этом сделать так, чтобы без крайней необходимости не отклонялись дейтаграммы в блоках, вызвавших перегрузку? Для ответа на этот вопрос необходимо вспомнить метод, примененный в протоколе TCP. Суть его состоит в том, что при вычислениях в каждый момент времени не следует использовать реальный размер очереди. Вместо этого в алгоритме RED определяется средневзвешенное значение размера внутренней очереди, которое используется для вычисления вероятности потери дейтаграмм. Величина средневзвешенного значения изменяется по экспоненциальному закону и корректируется каждый раз при получении очередной дейтаграммы.

В результате моделирования работы алгоритма RED и исследования его поведения в реальных условиях было выявлено много преимуществ этого метода. При перегрузке сети он позволяет избежать эффекта глобальной синхронизации, который возникает при применении метода усечения хвоста очереди. Кроме того, при кратковременной перегрузке метод RED без крайней необходимости не аннулирует дейтаграммы.

Сеанс связи TCP

Для установки сеанса связи протоколом TCP применяется *метод трехстороннего квитирования связи*. В простейшем случае процесс квитирования происходит так, как показано на рис. 4.6.

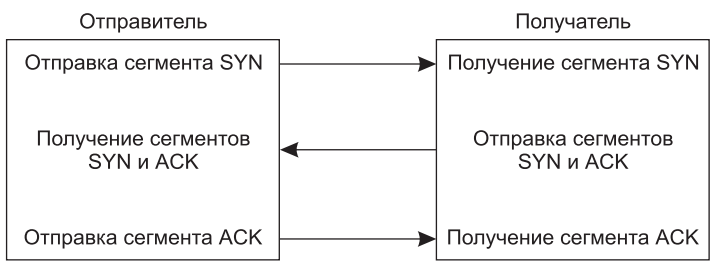


Рис. 4.6. Метод установки сеанса связи TCP

Первый сегмент, посылаемый в процессе квитирования, легко опознать, поскольку его полю SYN присвоена единица. Во втором сегменте данных единица присваивается двум полям, SYN и ACK. Это означает, что в нем находится сигнал

подтверждения приема первого сегмента SYN и данные, предназначенные для продолжения процесса квитирования. В заголовке последнего сегмента единица находится только в поле АСК. Этот сегмент используется только для информирования получателя о том, что обе стороны уведомлены об установке соединения.

Обычно инициатором установки соединения выступает экземпляр протокола, выполняемый на одном из компьютеров, участвующих в сеансе связи. При этом экземпляр, выполняемый на другом компьютере, просто ожидает начала процесса квитирования. Тем не менее, в процессе квитирования предусмотрена ситуация, когда оба компьютера одновременно выступят инициаторами начала соединения. Таким образом, TCP-соединение может быть установлено как по инициативе одной из сторон, так и двух сторон одновременно. После установки соединения данные могут передаваться в обоих направлениях совершенно одинаково. Другими словами, обе стороны TCP-соединения являются равноправными.

Метод трехстороннего квитирования связи является необходимым и достаточным условием выполнения успешной синхронизации между двумя сторонами соединения. В процессе осуществления доставки сегментов данных они могут быть утеряны, задержаны, продублированы или доставлены с нарушением порядка их следования. Для устранения перечисленных проблем в протоколе TCP используется механизм повторной передачи утерянных пакетов, который «включается» после истечения времени ожидания сигналов, подтверждающих прием данных. Серьезная проблема возникает в том случае, если в процессе установки соединения получатель получает два запроса (первоначальный и повторный) либо когда повторный запрос приходит с большой задержкой (после завершения установки соединения, его использования и разрыва). Перечисленные выше проблемы и позволяет решить метод трехстороннего квитирования связи. Кроме того, в протоколе TCP принято правило, согласно которому после установки соединения все дополнительные запросы на его установку попросту игнорируются.

Метод трехстороннего квитирования связи выполняет две важные функции. Во-первых, его применение гарантирует, что обе стороны соединения будут готовы к приему данных, о чем они будут взаимно осведомлены. Во-вторых, с его помощью выполняется процесс согласования начального порядкового номера. В процессе квитирования обе стороны соединения обмениваются начальными порядковыми номерами и ожидают подтверждения их приема. Порядковые номера используются для идентификации потоков данных, посылаемых каждой из сторон открытого соединения. Они выбираются сторонами самостоятельно во время открытия соединения.

Порядковые номера не могут всегда начинаться с одного и того же значения. В частности, экземпляр протокола TCP не может каждый раз при создании нового соединения назначать порядковый номер, равный единице. Естественно, при открытии соединения обе стороны будут согласовывать свои порядковые номера. Это делается для того, чтобы номера байтов, указываемые в сигналах подтверждения приема, соответствовали номерам, используемым в заголовках при передаче сегментов данных.

Чтобы понять, каким образом стороны, обменявшись всего тремя сообщениями, могут согласовать порядковые номера для двух потоков, необходимо вспомнить, что в заголовке любого сегмента содержится как поле порядкового номера, так

и поле номера сигнала подтверждения приема. Предположим, что компьютер *А* является инициатором соединения. Тогда во время трехэтапного процесса квитирования в первом SYN-сегменте он передает второй стороне (то есть компьютеру *Б*) свой начальный порядковый номер *n*. Получив SYN-сегмент, компьютер *Б* сохраняет в памяти начальный порядковый номер компьютера *А*, после чего посылает ответный сегмент синхронизации. В одноименном поле его заголовка она указывает уже свой начальный порядковый номер *y*, а полю номера сигнала подтверждения приема присваивается значение *n*+1. Тем самым компьютер *Б* уведомляет компьютер *А* о том, что его начальный порядковый номер успешно получен, и что компьютер *Б* ожидает получить от компьютера *А* поток байтов, начинающийся с номера *n*+1. В третьем и последнем сегменте процесса квитирования компьютер *А* подтверждает получение порядкового номера для компьютера *Б* и сообщает ему, что он ожидает получить от компьютера *Б* поток байтов, начинающийся с номера *n*+1. В обоих случаях номера в сигналах подтверждения приема соответствуют принятому в протоколе TCP соглашению о следующем ожидаемом сегменте данных.

Ранее уже отмечалось, что в протоколе TCP выполняется процесс трехстороннего квитирования при помощи обмена сегментами, содержащими минимальное количество информации. Протокол TCP спроектирован так, что в нем возможна передача данных вместе с начальным порядковым номером непосредственно в сегментах квитирования. В подобных случаях модуль протокола TCP блокирует данные до завершения процесса квитирования. После того как соединение установлено, экземпляр протокола TCP может разблокировать данные и доставить их ожидающему приложению.

Две взаимодействующие программы могут корректно завершить сеанс соединения, используя процедуру закрытия. Для этого используется модифицированный метод трехстороннего квитирования. Необходимо помнить, что TCP-соединение является дуплексным. Поэтому его можно использовать для передачи двух независимых потоков данных в противоположных направлениях. Получив от приложения сообщение о том, что все данные переданы, экземпляр протокола TCP закрывает соединение со своей стороны. Прежде чем закрыть половину соединения, экземпляр протокола должен отправить компьютеру-получателю все находящиеся в буфере данные, а также подождать подтверждения их приема. После этого получателю отправляется сегмент данных, в заголовке которого полю FIN присваивается единица. После того как FIN-сегмент будет получен компьютером-получателем, соответствующий экземпляр протокола посылает компьютеру-отправителю сигнал подтверждения приема и уведомляет собственное приложение о том, что отправителем переданы все данные. Для этой цели могут использоваться стандартные предоставляемые операционной системой средства, например может устанавливаться признак конца файла при очередной попытке считать данные из открытого соединения.

Закрыв соединение в требуемом направлении, экземпляр протокола TCP отвергает все попытки приложения передать данные в этом направлении. Тем не менее, в противоположном направлении данные могут передаваться до тех пор, пока отправитель не закроет вторую половину соединения. Естественно, даже после закрытия первой половины соединения по ней все равно будут передаваться

отправителю сигналы подтверждения приема. После закрытия соединения в обоих направлениях экземпляры протокола TCP, выполняемые на компьютерах отправителя и получателя, удаляют из своих системных таблиц записи, относящиеся к данному соединению.

На самом деле процесс закрытия соединения выглядит немного сложнее, чем описано ранее. В этом случае протоколом TCP применяется *модифицированный метод трехстороннего квитирования связи*.

После получения первого FIN-сегмента второй FIN-сегмент посылается компьютеру-отправителю не сразу, в отличие от SYN-сегмента. Отправителю посылается сигнал подтверждения приема первого FIN-сегмента, после чего выполняемое на компьютере получателя приложение уведомляется о получении запроса на закрытие соединения. От момента уведомления приложения до получения отклика может пройти достаточно много времени. Отправка сигнала подтверждения приема первого FIN-сегмента позволяет исключить повторную передачу этого сегмента отправителем по истечении тайм-аута. Получив от приложения, выполняемого на компьютере получателя, команду на закрытие соединения, экземпляр протокола TCP отошлет отправителю второй FIN-сегмент, при этом отправитель должен прислать уведомление о получении этого сегмента (третий ACK-сегмент).

Обычно после завершения передачи данных приложение закрывает соединение с помощью специальной команды. Поэтому данную операцию следует рассматривать как неотъемлемую часть нормального функционирования системы по аналогии с операцией закрытия обычного файла. Однако иногда обстоятельства могут сложиться так, что прикладная программа или сетевое программное обеспечение вынуждены разорвать соединение досрочно. Поэтому в протоколе TCP предусмотрены средства обработки подобных ситуаций, которые реализуют сброс соединения.

Для сброса соединения одна из сторон должна инициировать процесс досрочного прекращения передачи данных при помощи отправки сегмента, у которого полю RST присвоена единица. Получив подобный запрос, другая сторона должна немедленно разорвать соединение. При этом о поступившем запросе на сброс соединения экземпляр протокола TCP также уведомляет приложение. Таким образом, операция сброса соединения приводит к немедленному прекращению передачи данных в обоих направлениях и освобождению всех занятых ресурсов, например к очистке буферов памяти.

Ранее уже упоминалось о том, что протоколе TCP разбиение потока данных на сегменты происходит без учета объема данных, переданных экземпляру протокола приложением. Разработчики руководствовались соображениями требуемой эффективности. Благодаря этому экземпляр протокола может накапливать во внутреннем буфере памяти необходимое для эффективной передачи количество данных, что позволяет снизить накладные расходы при передаче по сети сегментов данных небольшого размера.

Хотя благодаря буферизации существенно повышается пропускная способность сети, она может негативно сказаться на функционировании некоторых приложений. Можно рассмотреть процесс передачи символов с клавиатуры терминала на

удаленный компьютер с применением заранее установленного TCP-соединения. Понятно, что пользователю вряд ли понравится замедленная реакция компьютера в ответ на нажатие клавиш. Но если экземпляр протокола TCP перед отправкой символов помещает их в буфер, удаленный компьютер будет реагировать на каждое нажатие клавиши с большой задержкой. Вполне возможно, что удаленный компьютер отреагирует только после нажатия нескольких сотен клавиш, причем на все одновременно. Точно так же экземпляр протокола TCP, выполняемый на компьютере-получателе, реализует буферизацию полученных по сети данных, прежде чем передать их приложению.

Очевидно, что для своевременной доставки данных приложению нельзя просто вынудить отправителя переслать их по сети. Для обеспечения приемлемой работы интерактивных программ протокол TCP предусматривает специальную команду принудительной отсылки данных — push. Именно эта команда применяется для незамедлительной передачи байтов данных, помещенных в выходной поток данных. Во время выполнения этой команды полю PSH присваивается единица. Это гарантирует, что данные будут переданы без задержки приложению, которое выполняется на компьютере-получателе.

А теперь следует рассмотреть стандартные номера портов, используемые протоколом TCP.

Зарезервированные порты протокола TCP

В процессе функционирования протокола TCP применяется статический и динамический метод назначения портов. В этом случае часто используемые приложения, например почтовые клиенты, получают фиксированные номера портов. При этом идет речь о *хорошо известных* портах. Эти номера известны всем программистам и обычно никогда не изменяются. Остальные номера портов распределяются в динамическом режиме операционной системой. Перечень наиболее часто применяемых стандартных номеров портов приведен в табл. 4.2.

Таблица 4.2. Хорошо известные порты TCP

Номер порта	Обозначение	Описание
0	Отсутствует	Зарезервировано
1	TCPMUX	Мультиплексор для протокола TCP
7	ECHO	Эхо-сигналы
9	DISCARD	Отмена
11	USERS	Активные пользователи
13	DAYTIME	Отображение текущей даты
15	NETSTAT	Сетевая статистика
17	QUOTE	Отображение популярной цитаты
19	CHARGEN	Генератор символьных последовательностей
20	FTP-DATA	Данные, имеющие отношение к протоколу FTP.
21	FTP	Протокол передачи файлов (File Transfer Protocol)

продолжение

Таблица 4.2 (*продолжение*)

Номер порта	Обозначение	Описание
22	SSH	Защищенная оболочка передачи данных
23	TELNET	Программа эмуляции терминала
25	SMTP	Простой протокол передачи электронной почты (Simple Mail Transfer Protocol)
37	TIME	Отображение текущего времени
43	NICKNAME	Сведения о пользователе, зарегистрированном в сети
53	DOMAIN	Сервер имен доменов (Domain Name Server)
67	BOOTPS	Сервер BOOTP
77	RJE	Произвольная частная служба RJE
79	FINGER	Программа finger
80	WWW	Сервер World Wide Web
88	KERBEROS	Служба идентификации Kerberos
95	SUPDUP	Протокол SUPDUP
101	HOSTNAME	Сервер имен узлов
102	ISO-TSAP	Служба ISO-TSAP
103	X400	Почтовая служба X.400
104	X400-SND	Программа-отправитель почты X.400
110	POP3	Почтовый протокол версии 3
111	SUNRPC	Удаленный вызов процедур на платформе Sun
113	AUTH	Служба идентификации
117	UUCP-PATH	Служба путей, соответствующая протоколу UUCP
119	NNTP	Сетевой протокол передачи новостей (Network News Transfer Protocol)
123	NTP	Протокол сетевого времени (Networ Time Protocol)
139	NETBIOS-SSN	Сеансовая служба протокола NETBIOS
161	SNMP	Простой протокол управления сетью (Simple Network Management Protocol)

На этом рассмотрение теории, относящейся к сетям Microsoft, завершается.

Аппаратные сетевые компоненты

В двух главах этой части книги рассматриваются устройства, без которых была бы немыслима сеть — сетевые адаптеры, повторители, мосты, коммутаторы, маршрутизаторы. Подробно описываются принципы работы этих устройств, методы настройки, а также методика подбора и тестирования оборудования. В шестой главе описывается методика расчета локальной сети, позволяющая спроектировать эффективную локальную сеть при относительно небольших затратах.

5 ГЛАВА Сетевые адаптеры, коммутаторы и маршрутизаторы

Предметом рассмотрения настоящей главы являются аппаратные устройства, реализующие локальную вычислительную сеть на уровне «железа». И начнем мы наше рассмотрение с сетевых адаптеров.

Сетевые адаптеры

Сетевой адаптер (сетевая карта) — это ключевое аппаратное устройство, соединяющее компьютер пользователя с сетевой средой. В качестве сетевой среды может выступать любая физическая среда (кабель или беспроводная среда), в которой распространяются сигналы, несущие информацию в локальной вычислительной сети. Назначение сетевого адаптера заключается в приеме-передаче сетевых фреймов, причем на практике эта задача осуществляется с помощью драйвера сетевого адаптера, который обеспечивает «мост» между микросхемами сетевого адаптера и стеком сетевых протоколов, выполняемым на компьютере.

В модели OSI сетевой адаптер (в связке с соответствующим драйвером) функционирует на физическом и канальном уровнях. На рис. 5.1 показан типичный сетевой адаптер (Fast Ethernet).

Хотя основным объектом рассмотрения будут сетевые адаптеры, применяемые в сетях Ethernet, в этой главе будут упомянуты и другие устройства из данной категории, имеющие определенные особенности. Например, сетевые адаптеры, предназначенные для сетей ARCnet и Token-Ring, достаточно сильно отличаются от сетевых адаптеров, предназначенных для сетей Ethernet. Независимо от конструктивных особенностей сетевых адаптеров, методы диагностики и устранения неисправностей, которые также рассматриваются в главе, применимы к сетевым адаптерам любых типов.

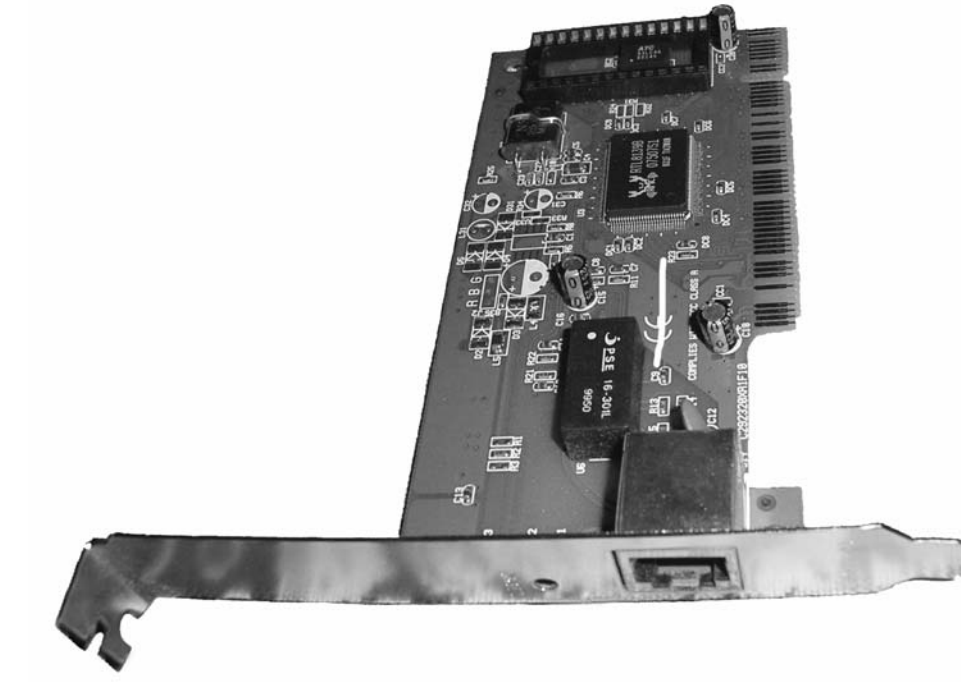


Рис. 5.1. Сетевой адаптер Fast Ethernet

ПРИМЕЧАНИЕ

Современные системные платы ПК снабжены встроенными сетевыми адаптерами, совместимыми со стандартом Fast Ethernet (или даже Gigabit Ethernet). Поэтому вряд ли понадобится приобретать это устройство отдельно. Это нужно сделать, если подключаемый к сети компьютер является достаточно старой моделью либо если необходимо подключить его в локальную сеть, формат которой не слишком широко распространен.

Сетевой адаптер может быть выполнен в виде отдельного устройства, либо входить в состав системной платы компьютера. В любом случае, он, как правило, поддерживает стандарт Plug and Play (PnP). Поэтому подключение компьютера к локальной сети сводится к активизации сетевого адаптера и присоединению сетевого кабеля. Естественно, в практике специалиста по настройке сети могут возникать такие ситуации, когда приходится иметь дело с устаревшими сетевыми адаптерами, не поддерживающими стандарт PnP. Хотя и вероятность подобного события мала, но все же в этой главе отдельный раздел посвящен настройке сетевых адаптеров при помощи джамперов.

Принципы работы сетевых адаптеров

Независимо от аппаратной шины и типа локальной сети любой сетевой адаптер выполняет операции по приему и передаче сетевых фреймов. Сначала следует рассмотреть процесс передачи данных.

1. Прием раздела данных фрейма с подуровня LLC и информациио адресах уровня MAC. При этом используются буферы памяти сетевого адаптера.
2. Формирование фрейма данных на уровне MAC. В этот же фрейм встраивается фрейм LLC. На этом этапе вычисляется контрольная сумма, а также вводится информация в поля, определяющие компьютер-отправитель данных и компьютер-получатель данных.
3. Создание символьного кода с помощью технологии избыточного кода. Благодаря этому обеспечивается более равномерный спектр генерируемого сигнала.
4. Передача сигнала в соответствии с применяемым линейным кодом.

Процесс приема данных, осуществляемый сетевым адаптером, выглядит несколько иначе.

1. Прием сигналов, которыми кодируется битовый поток.
2. Фильтрация сигналов (выделение их из общего шума). Эта операция выполняется на аппаратном уровне.
3. Дешифрование, если передаваемые данные были зашифрованы.
4. Проверка значения поля контрольной суммы. Если значение контрольной суммы изменилось, фрейм отбрасывается. Если же оно осталось неизменным, то выбирается фрейм LLC, изначально вложенный в MAC-фрейм.

Эти операции обычно выполняются центральным процессором компьютера. Если сетевой трафик достаточно велик, то может наступить состояние «затора». Поэтому серверы обычно снабжаются более совершенными сетевыми адаптерами, которые оснащены собственными специализированными микропроцессорами, выполняющими большую часть требуемых операций.

Любой сетевой адаптер характеризуется поддерживаемой аппаратной шиной. В настоящее время практически все доступные на рынке сетевые адаптеры стандарта Ethernet поддерживают шину PCI.

ПРИМЕЧАНИЕ Разумеется, в устаревших компьютерах могут использоваться сетевые адаптеры, поддерживающие шину VESA/ISA/EISA. Эти устройства характеризуются невысокой производительностью, а также чаще всего требуют ручной настройки.

Помимо кабельных сетевых адаптеров существуют разновидности этих устройств, предназначенные для использования в беспроводных сетях (радиоадаптеры). Эти устройства выполняют более сложное преобразование сигнала и зачастую реализуются в виде автономных приборов, подключаемых к компьютеру посредством USB-кабелей. Естественно, подобным адаптерам требуется внешнее электропитание.

Шины

Шина ISA (Industry Standard Architecture, стандартная промышленная архитектура) является «бабушкой» аппаратных шин, а эпоха ее повсеместного примене-

ния началась в восьмидесятых годах прошлого века. Название «ISA» было введено в обиход разработчиками после появления на свет компьютера IBM PC.

Первая версия этой шины предусматривала использование 8-разрядного канала передачи данных. С появлением компьютера IBM AT оригинальная версия шины ISA была усовершенствована. В частности, используемая тактовая частота была повышена до 8 МГц, а для передачи данных применялся 16-разрядный канал. В результате дальнейшего усовершенствования этой архитектуры возникла шина EISA (Extended ISA, расширенная ISA). Разрядность шины данных была повышена до 32 битов, а тактовая частота сохранилась на прежнем уровне — 8 МГц.

С появлением шины PCI производительность ПК многократно возросла. Одним из факторов роста являлась значительно возросшая скорость передачи данных. Это было следствием применения 32- или 64-разрядных шин данных. Устройства, работающие с шиной PCI, получили такое важное свойство, как *управление шиной* (bus mastering). При помощи этой технологии сетевой адаптер может управлять шиной, а также передавать большие объемы данных непосредственно в системную память, не используя ресурсы центрального процессора.

Если сравнивать с шиной EISA, то помимо чисто функциональных преимуществ, шина PCI обладает таким приятным свойством, как возможность конфигурирования в автоматическом режиме. Сетевой адаптер PCI снабжен внутренними регистрами памяти, в которых хранятся данные, применяемые для конфигурации загружаемой системы. Эти данные содержат трехбайтный код класса, к которому относится сетевой адаптер. Признаком сетевого адаптера является значение 02h. Значение 00h — «опознавательный знак» сетевых адаптеров, появившихся еще до того, как сформировались коды классов, а величина FFh свидетельствует о том, что текущее PCI-устройство является «неизвестным науке видом», который не относится ни к одному из известных классов. Здесь же можно найти такие сведения, как системная конфигурация адаптера PCI.

ПРИМЕЧАНИЕ

Термин «прерывание» обозначает способ получения доступа к центральному процессору, используемый периферийными устройствами. К примеру, если сетевой адаптер «сбрасывает» данные из буферной памяти в основную память компьютера, для этого используется соответствующее прерывание. При этом не гарантируется, что устройство тут же получит ответ центрального процессора, поскольку в данный момент он может выполнять важные операции, которые нельзя отложить. При этом возникает так называемое маскируемое прерывание. Оно реализовано как сигнал для ЦПУ, говорящий о необходимости выполнения в ближайшем будущем того или иного действия. Существуют также немаскируемые прерывания, требующие немедленной реакции центрального процессора (например, ошибка памяти). Конечно, процессор может не реагировать даже на этот вид прерываний, но на практике подобное встречается крайне редко.

Обычно в окне настроек адаптера PCI (рис. 5.2) задается возможность выбора номера прерывания (IRQ), доступного в системе. Если не найдено свободное прерывание, адаптер может совместно с другим устройством использовать одно и то же прерывание.

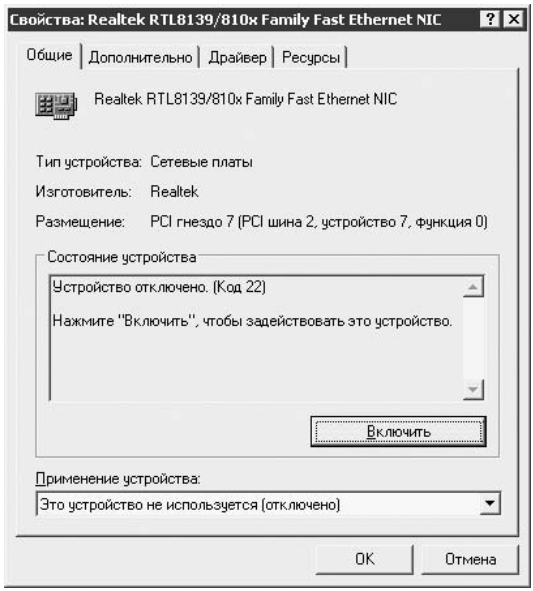


Рис. 5.2. Окно настроек адаптера PCI

В настоящее время существует несколько разновидностей шины PCI: Mini PCI, CompactPCI, Low-Profile PCI, Concurrent PCI и PCI Express. Каждый тип шины используется в собственной нише. Например, шина Mini PCI применяется в портативных компьютерах.

Еще раз подчеркну, что шина PCI обладает несколькими существенными преимуществами по сравнению с шинами ISA и VLB. Она функционирует в независимом режиме, изолирована от процессора, но при этом обеспечивает прямой доступ к системной памяти. Поэтому периферийные устройства стандарта PCI могут работать в асинхронном режиме относительно центрального процессора с тактовыми частотами 25, 30 и 33 МГц. Таким образом, даже при увеличении частоты процессора тактовая частота шины PCI могла оставаться неизменной, как правило, составляя фиксированную долю от тактовой частоты, на которой работает центральный процессор. Кроме того, шина PCI поддерживает примерно вдвое больше плат расширения и устройств, чем VLB, а при необходимости их число можно еще увеличить за счет добавления новых сегментов PCI. Пользователю также доступны расширенные функции конфигурации и энергосбережения. Режим захвата арбитража шиной PCI позволил устройствам получать контроль над ней и обмениваться данными напрямую, без участия процессора. В результате снизились задержки и нагрузка на центральный процессор.

Именно благодаря этим преимуществам в середине девяностых годов прошлого века шина PCI окончательно выиграла «битву между шинами», став доминирующим стандартом. Однако компьютерная индустрия не стоит на месте. С распространением в системах потребительского класса RAID-массивов, 10 Gigabit Ethernet и других высокоскоростных устройств пропускная способность PCI (133 Мбайт/с) стала недостаточной при одновременной работе всех устройств.

В результате на свет появилась шина PCI Express, ранее известная как 3GIO (3rd Generation I/O), которая идет на смену шине PCI. Эта шина позиционируется в качестве универсального решения, призванного формировать универсальный интерфейс ввода-вывода для настольных ПК, портативных компьютеров, серверов, устройств связи, рабочих станций и встроенных устройств. Шина PCI Express совместима с шиной PCI на программном уровне, поэтому существующие операционные системы могут работать с ней практически без изменений. Кроме того, многие драйверы устройств PCI Express совместимы с имеющейся периферией для PCI.

Строго говоря, PCI Express не является шиной в исходном смысле этого слова, поскольку она не позволяет напрямую подключать к системе более одного устройства. Обойти это ограничение можно с помощью коммутатора, благодаря которому несколько устройств могут одновременно подключаться к единственному каналу PCI Express, а также передавать данные друг другу, минуя процессор. С точки зрения пользователя установка и настройка плат расширения PCI Express почти не отличается от установки и конфигурирования традиционных плат расширения стандарта PCI-адаптеров, хотя размеры и цоколевка гнезд PCI существенно отличается от параметров гнезд PCI Express.

Первая версия PCI Express обеспечивает скорость передачи данных до 256 Мбайт/с, затем этот показатель будет увеличен еще в два раза. В отличие от шины PCI, передающей информацию лишь в одном направлении, каналы приема и передачи данных PCI Express функционируют параллельно и независимо друг от друга.

Видеоадаптеры подключаются к специальному гнезду PCI Express X16, которое объединяет 16 одноканальных линий передачи шины, вследствие чего его пропускная способность достигает 4 Гбайт/с в дуплексном режиме. Стандарт AGP 8X обеспечивает максимальную скорость передачи данных до 2,1 Гбайт/с от системы к видеоадаптеру. Если же данные передаются в обратном направлении, то скорость их передачи, как и для стандарта AGP 1X, не превышает 264 Мбайт/с. Подобная несимметричность существенно ограничивает возможности видеоадаптера.

Рис. 5.3. Плата расширения стандарта PC Card

Помимо шин PCI в портативных компьютерах применяется так называемая шина PCMCIA (Personal Computer Memory Card International Association, Международная ассоциация производителей карт памяти для персональных компьютеров). Этимология этого названия связана с тем, что изначально под этим названием выпускались только карты памяти. Теперь же так называются все

платы расширения, предназначенные для портативных компьютеров (альтернативное название — PC Card). На рис. 5.3 показана плата расширения формата PC Card.

Основные характеристики сетевых адаптеров

Помимо поддерживаемой шины, важнейшее значение имеет такая характеристика сетевого адаптера, как быстродействие. В настоящее время уже практически не осталось сетевых адаптеров, поддерживающих скорость передачи данных 10 Мбит/с. Поэтому стоит ориентироваться на сетевые адаптеры стандарта Fast Ethernet (100 Мбит/с). Для большинства практических целей их возможностей будет достаточно.

Если же необходимо модернизировать существующую сеть, поддерживающую скорость передачи данных 10 Мбит/с, стоит воспользоваться комбинированными сетевыми адаптерами стандарта 10/100 Мбит/с. Универсальность этих устройств заключается в том, что они автоматически определяют скорость передачи данных в локальной сети.

Также сетевые адаптеры классифицируются в зависимости от типа сетей, в которых они применяются, — Ethernet, FDDI, Token Ring и т. д.

Уникальной характеристикой сетевого адаптера является так называемый физический адрес (MAC-адрес), который жестко программируется на заводе-изготовителе. Этот адрес является 48-разрядным и однозначно идентифицирует компьютер, в котором установлен соответствующий сетевой адаптер.

ПРИМЕЧАНИЕ Производители сетевого оборудования не назначают MAC-адреса произвольным образом. Для этого используются блоки Ethernet-адресов, выделенные институтом IEEE. В этом важном деле волюнтаризм не допускается, поскольку последствия его в данном случае будут весьма неприятными. Одним из последствий может стать нарушение уникальности однородного пространства физических адресов Ethernet.

Поиск и устранение неисправностей

Иногда возникает ситуация, когда установленный сетевой адаптер отказывается работать. В чем же тут дело? На самом деле причин, провоцирующих подобную неприятную ситуацию, может быть несколько — неисправности в адаптере, в компьютере, в котором установлен адаптер, или повреждение кабеля, соединяющего адаптер с концентратором или коммутатором. А может случиться так, что проблема кроется во всех перечисленных устройствах сразу. И для ее устранения может быть достаточно изменить настройки соответствующего сетевого адаптера, а может быть придется выполнить серьезные ремонтные работы.

Если компьютер работает под управлением операционной системы Windows 2000, рекомендуется проверить журнал регистрации системных ошибок (Event Viewer). В нем регистрируются все события, происходящие в момент загрузки операционной системы.

ПРИМЕЧАНИЕ И самый главный совет в затруднительной ситуации — внимательно изучайте документацию, прилагаемую к сетевому адаптеру. Как правило, в ней можно найти ответы на все вопросы, связанные с настройкой этого устройства.

Проблема обнаруживается проще, если установленные в локальной сети адаптеры поддерживают стандарт Plug and Play. При этом конфликты, связанные с прерываниями и адресами ячеек памяти, исключены, поэтому причина неисправности кроется в кабеле, концентраторе, коммутаторе или в соединителях.

Диагностика неисправностей упрощается, если обращать внимание на светодиоды, установленные на сетевом адаптере. Обычно свечение светодиода означает активизацию сетевого адаптера и возможность обмена данными с другими аппаратными сетевыми компонентами. Если же светодиод мигает, это тревожный сигнал, который свидетельствует о наличии проблемы в сети. Следует обращать внимание на характер этого мигания, поскольку высокая его частота может обозначать передачу данных сетевым адаптером. Большинство сетевых адаптеров снабжено двумя светодиодами, один из которых сигнализирует о процессе обмена данными, а второй является индикатором стандартного или аномального режима функционирования сетевого адаптера.

В целях локализации и устранения проблемы, связанной с сетевым адаптером, рекомендуется воспользоваться достаточно простой последовательностью действий.

1. Проверить плотность соединения в разъемах сетевых устройств.
2. Вытащить и вставить повторно в разъем плату сетевого адаптера.
3. Протестировать идентичность типа канала передачи, используемого сетевым адаптером и такими устройствами, как концентраторы или коммутаторы или маршрутизаторы (дуплексный или полудуплексный режим передачи данных, идентичная скорость передачи данных).
4. Если сетевой адаптер обладает свойством авточувствительности, можно попробовать его активизировать или отключить. Именно это свойство может служить источником аппаратных конфликтов.
5. Подключить кабель, ведущий от сетевого адаптера, к другому порту концентратора или коммутатора.
6. Поменять сегмент кабеля, соединяющий сетевой адаптер с портом концентратора либо коммутатора.
7. Попробовать вставить плату сетевого адаптера в другое гнездо системной платы компьютера.
8. Обратить внимание на настройки BIOS для данного компьютера. При необходимости можно изменить те из них, которые относятся к сетевому адаптеру.
9. Если используется операционная система Windows XP, то нужно перейти в окно `Сетевые подключения` и проверить состояние подключения к локальной сети. Если отображается сообщение `Отключено`, достаточно в контекстном меню выполнить команду `Включить` (рис. 5.4). Обычно после этого отображается пиктограмма подключения к локальной сети.
10. Если ничего не помогает, то остается один радикальный метод — замена платы сетевого адаптера.

Рис. 5.4. Активизация платы сетевого адаптера

Как правило, в комплект поставки сетевого адаптера входят программные драйверы и диагностические программы. Обычно эти программы функционируют в среде MS-DOS, причем в операционную память не должны загружаться иные драйверы или какие-либо резидентные программы, поскольку это может привести к появлению конфликтов или искажению результатов тестирования.

Как правило, при загрузке диагностической программы отображается меню, в котором перечислены несколько видов тестов. Обычно предлагается диагностировать используемое оборудование или воспользоваться текстом, являющимся аналогом ping-теста на специальный кольцевой адрес. Результаты тестов вместе с информацией о выявленных ошибках отображаются на итоговом экране.

Если после успешного завершения тестов сетевой адаптер по-прежнему не работает, следует проверить его конфигурацию. Для этого можно воспользоваться приложением System Information (в Windows 2000) либо Сведения о системе (в Windows XP). При помощи этих приложений можно идентифицировать адреса ячеек памяти, выделенные для данного сетевого устройства, а также номера прерываний. На рис. 5.5 показано окно программы Сведения о системе.

Если же в сети функционируют компьютеры с установленными операционными системами Windows 98/NT 4.0, можно воспользоваться диагностической программой Microsoft Diagnostics (вкладка Resources).

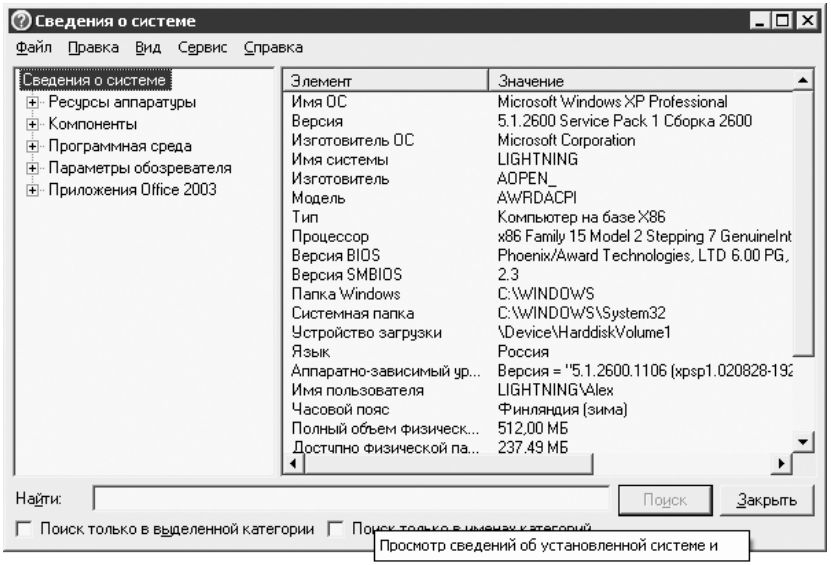


Рис. 5.5. Окно программы Сведения о системе

Если в сети используются устаревшие адаптеры стандарта ISA, скорее всего придется «покопаться во внутренностях» компьютера и подобрать правильную комбинацию перемычек, с помощью которых изменяются настройки прерывания.

Если же все выполненные ранее действия не привели к положительным результатам, причина неисправностей может заключаться в неправильном распределении IP-адресов. В этом случае надо проверить корректность самого IP-адреса и соответствующей маски подсети, руководствуясь правилами назначения IP-адресов различных классов.

Возможно, что причина появления проблем заключается в искажении сетевых фреймов, генерируемых сетевым адаптером. Подобная проблема может быть обнаружена только при помощи специальных сетевых пробников, речь о которых пойдет в последней главе книги.

ПРИМЕЧАНИЕ

Иногда неисправный концентратор позволяет выявить соединение двух сетевых компьютеров «напрямую». В этом случае изменяется распайка соединителя на кабеле витой пары («крест-накрест»). Подробнее о распайке сетевых кабелей рассказывается в последней главе книги.

Концентраторы

Сеть, построенная на базе витой пары, обязательно использует один или несколько *концентраторов*, при помощи которых реализуется физическое соединение между сетевыми компьютерами. Это устройство может иметь несколько названий, каждое из которых обозначает одно и то же: повторитель (repeater), хаб (hub) иди концентратор (concentrator). В зависимости от модификации этого

устройства изменяются его характеристики и набор выполняемых функций, хотя в основе оперирования устройств этого типа лежит передача сигналов между портами без их изменения. Любой концентратор снабжен несколькими *портами*, при помощи которых объединяются несколько физических сегментов локальной сети. Концентраторы используются в сетях, характеризующихся различными топологиями, — FDDI, Ethernet, Token Ring.

Так, например, в сетях, реализованных на базе коаксиального кабеля, концентраторы изначально именуются *повторителями* и применяются для объединения двух отрезков кабеля. Здесь прослеживается аналогия со *сплиттером*, применяемым для соединения коаксиальных кабелей. В подобных сетях повторители являлись необязательным компонентом, поскольку рабочие станции подключались к общей шине.

А вот в сетях, реализованных на основе витой пары, применение концентратора (хаба) стало обязательным. Количество портов типичного концентратора варьируется от 5 до 72, причем наравне с разъемами RJ-45, применяемыми для подключения сетевых компьютеров, эти устройства снабжены дополнительным разъемом, предназначенным для подключения к другому концентратору или магистральной линии связи. На рис. 5.6 показан типичный концентратор.

Рис. 5.6. Вот такие бывают концентраторы

Концентраторы могут объединяться между собой каскадным образом, причем для этого даже не требуется специально выделенный порт, достаточно обычного RJ-45. Но в этом случае в кабеле витой пары, соединяющем два концентратора, потребуется соединить жилы перекрестным образом. Обычно для подключения другого концентратора выделяется отдельный порт RJ-45, в котором реализована *инверсная* распайка жил.

ПРИМЕЧАНИЕ

В настоящее время концентраторы практически вышли из употребления, поскольку им на смену пришли более «интеллектуальные» собратья — коммутаторы, позволяющие реализовать более гибкое управление сетью. Еще пять лет назад коммутаторы стоили достаточно дорого, сейчас же их цена находится в разумных пределах, поэтому эти замечательные устройства привели к «вымиранию» концентраторов как вида. Подробнее коммутаторы рассматриваются в следующем разделе главы.

Нельзя не упомянуть об одном замечательном свойстве концентраторов, вносящем некий элемент автоматизации в процесс управления локальной сетью. Это свойство именуется *автоматической сегментацией*, и на практике означает автоматическое отключение неработоспособных портов. Каким же образом определяется неработоспособность? Очень просто. Например, в концентраторах Ethernet каждому порту периодически посылается последовательность импульсов проверки канала связи. Если ответный сигнал отсутствует, этот порт отключается, причем импульсы продолжают посылаться, чтобы в случае устранения неисправности порт можно было снова активировать. Причины, приводящие к отключению портов концентраторов, могут быть разделены на три категории.

1. Слишком длинная передача. Если время передачи превышает интервал времени, выделенный для передачи фрейма максимальной длины.
2. Количество конфликтов превысило рубеж в 60 допустимых коллизий.
3. Появление чрезмерно большого количества ошибочных фреймов, проходящих через данный порт.

На практике применяются концентраторы трех типов: с фиксированным количеством портов (устройство в виде отдельного блока, количество портов которого варьируется от 4 до 24), стековые концентраторы (несколько отдельных устройств объединяются в единое целое), а также модульные концентраторы (на одном шасси устанавливаются несколько независимых модулей).

Несмотря на ограниченный набор функций концентраторов, администратор локальной сети может даже реализовать некоторый уровень защиты данных, циркулирующих в этой сети. Для этого достаточно в ручном режиме назначить каждому порту концентратора MAC-адрес, который уникальным образом идентифицирует рабочую станцию, подключающуюся к данному концентратору. После этого все потуги злоумышленников, пытающихся несанкционированным образом подключиться к локальной сети и перехватить ценную информацию, будут тщетными.

ПРИМЕЧАНИЕ Подробнее о проблемах, связанных с обеспечением безопасности в локальных сетях, будет рассказано в десятой главе.

Концентраторы с большим количеством портов обычно служат для формирования локальной сети, состоящей из нескольких независимых сегментов. Это бывает полезным, когда с помощью одного концентратора формируется несколько независимых локальных сетей.

Многопортовые концентраторы обычно могут управляться посредством протокола SNMP, который позволяет выполнять дистанционное включение/отключение портов и отслеживание состояния работающего устройства.

Мосты и коммутаторы

Необходимость в этих устройствах возникла после того, как размеры локальных сетей Ethernet превысили некоторый порог, в результате чего потребовалось разбить одну большую сеть на отдельные сегменты. При этом повышается степень

гибкости, а также упрощается процесс управления сетью в целом. Разбиение сети на отдельные сегменты осуществляется с помощью *мостов* и *коммутаторов*, которые иногда называют свитчами. Несмотря на различие в наименовании, на самом деле мост и маршрутизатор выполняют одни и те же функции. Оба эти устройства в своей работе применяют два типа алгоритмов — *алгоритм прозрачного моста* (стандарт IEEE 802.1D) и *алгоритм моста с маршрутизацией от источника* (сети Token Ring компании IBM).

Основное различие между этими двумя устройствами заключается в методе обработки сетевых фреймов. Поскольку мост появился намного раньше коммутатора и использовался чаще всего для соединения между собой двух подсетей, в нем применяется последовательный метод обработки фреймов. В коммутаторе же реализован параллельный метод обработки сетевых фреймов, способный справиться со значительно большим трафиком между несколькими десятками сетевых сегментов. Благодаря тому, что скорость работы коммутаторов, снабженных несколькими параллельно функционирующими процессорами, в десятки раз превышает скорость работы однопроцессорного моста, последние практически не используются в современных локальных сетях. Единственная область их применения — соединение удаленных сетей, реализуемое посредством относительно медленных глобальных каналов связи.

Применение мостов сопряжено с рядом недостатков, основным из которых является абсолютная беспомощность в случае возникновения так называемого *широковещательного шторма*.

ПРИМЕЧАНИЕ Широковещательный шторм возникает в том случае, когда какое-либо сетевое устройство начинает генерировать фреймы, в которых в качестве адресов компьютеров-получателей применяются широковещательные адреса, то есть адреса всех сетевых компьютеров. В случае возникновения этого опасного явления сеть буквально «затапливается» вследствие резкого увеличения объема трафика.

Мосты абсолютно неприменимы в тех случаях, когда сеть обладает сложной структурой, с большим количеством петель и сегментов. Непригодность моста в подобных случаях объясняется особенностями его алгоритма, рассчитанного на использование в простых сетях Ethernet, состоящих максимум из двух сегментов, в каждом из которых подключено не более 20–30 рабочих станций.

Если же сеть обладает сложной петлеобразной структурой и включает несколько десятков рабочих станций, стоит воспользоваться коммутатором. Коммутатор может моделироваться совокупностью мостов, образующих одно устройство, наделенное возможностями контроля и передаваемых в сети фреймов данных. Коммутаторы полностью заменяют применяемые ранее мосты, но при этом обладают множеством дополнительных возможностей.

Беспроводные мосты

Несмотря на сходство названия, между обычными сетевыми мостами и *беспроводными мостами* не так уж и много общего. Разве что назначение — как и обыч-

ный сетевой мост, беспроводный мост предназначается для объединения между собой сетей, но при этом используется беспроводный канал связи (радиоканал).

До 2000 года стоимость беспроводных мостов, предназначенных для объединения обычных сетей через канал радиосвязи, составляла более пятисот долларов, в связи с чем они были совершенно недоступны для использования в небольших сетях.

Но в конце 2001 года производители сетевого оборудования решили расширить набор функциональных свойств точек доступа, поддерживающих стандарт IEEE 802.11b, придав им более универсальный характер. И первым шагом на пути к этому стало то, что точки доступа получили функцию беспроводных мостов. Но модернизированные устройства часто сохраняли прежнее название (точки доступа, access points), что часто приводило к путанице. Наиболее отрадным явлением стало то, что цены на подобные устройства достигли «магического порога» 100 долларов, в результате чего оживилась активность покупателей в этом секторе рынка.

В конце лета 2002 года появилась еще одна категория оборудования, способная выполнять функции беспроводного моста. Примером таких устройств может служить Linksys WET11, при помощи которого практически любое сетевое устройство стандарта Ethernet могло получать доступ к беспроводному каналу связи. Причем одновременно можно было подключить более двадцати устройств.

В следующий перечень сведены важные моменты, на которые следует обратить внимание в случае неработоспособности беспроводных мостов.

- Выбирать оборудование следует в соответствии с выполняемыми задачами. Необходимо удостовериться, что приобретаемое оборудование поддерживает требуемые режимы работы. Например, беспроводные маршрутизаторы сами по себе не могут работать в режиме моста, но эта проблема решается при помощи дополнительных модулей. С другой стороны, клиентский режим точки доступа различен у всех производителей, поэтому лучше приобретать все устройства у одной фирмы.
- Нужно убедиться, что все оборудование работает на небольшом расстоянии. Стоит установить оборудование в одной комнате и протестировать его в рабочем режиме. После этого можно устанавливать его на рабочем расстоянии.
- Будьте внимательны! Если настраиваются два одинаковых устройства, диалоговые окна обычно выглядят одинаково. На самом деле разница может быть существенной, поэтому стоит обращать внимание на подобные мелочи.
- Использовать открытой идентификации (Open System Authentication). Как правило, в процессе настройки оборудования доступны типы идентификации Open System, Shared Key и Closed System. Меньше всего ограничений влечет за собой режим Open System, именно его следует выбрать в целях тестирования. Затем можно будет его изменить, выбрав более серьезный режим.
- В тестовом режиме нужно отключить установку WEP и не активизировать ее до тех пор, пока не станет ясно, что оборудование использует совместимые режимы работы.
- Выбрать режим Long Preamble (длинная преамбула) для сетевых пакетов.
- Установить MAC-адреса в режимах «точка-точка» и «точка-многоточечное соединение» для точек доступа. Еще раз проверить их корректность.

Коммутаторы

Первый коммутатор появился в 1990 году (EtherSwitch, разработанный фирмой Kalpana). Этот коммутатор был оборудован 8 портами и предназначался для использования в сетях 10BASE-T. Передача данных между портами осуществлялась при помощи так называемой *коммутационной матрицы*. Работа подобной матрицы осуществляется на основе принципов, заложенных в основу технологии *коммутации каналов*. В соответствии с применяемым рабочим алгоритмом коммутаторы делятся на две разновидности — с полной буферизацией фреймов и с конвейерной обработкой фреймов.

Принцип работы *коммутатора с конвейерной обработкой* заключается в том, что полученный фрейм переадресовывается выходному порту сразу же после того, как будет получен его заголовок. То есть достаточно коммутатору получить адрес назначения, находящийся в заголовке фрейма, как происходит передача всего фрейма данных. Преимущество подобного режима работы заключается в резком повышении быстродействия. До тех пор, пока не происходят какие-либо серьезные сбои, скорость передачи данных коммутатором сопоставима со скоростью их распространения по сетевому кабелю.

Но за все нужно платить, поэтому использование этого метода влечет за собой некоторые проблемы. Цикл передачи данных начинается до того, как коммутатор осуществит проверку целостности фрейма данных. Если окажется, что фрейм не соответствует стандартам, он будет интерпретирован в качестве широковещательного со всеми вытекающими отсюда последствиями, среди которых будет и чрезмерный рост сетевого трафика.

Коммутаторы с полной буферизацией фреймов организуют накопление байтов данных в памяти до тех пор, пока не будет получен весь фрейм. Если выходной порт освобождается, а сам фрейм не относится к категории широковещательных и не поврежден в процессе передачи, то выполняется его доставка по назначению. В противном же случае коммутатор выполняет фильтрацию поврежденных или широковещательных фреймов, блокируя их дальнейшее распространение. Обычно задержка, связанная с накоплением байтов фрейма в буферной памяти, не превышает 30–40 мкс.

Коммутаторы могут работать в полудуплексном и дуплексном режиме. В последнем случае скорость передачи данных увеличивается примерно в два раза.

Как и мосты, коммутаторы по мере получения фреймов данных заносят в *адресную таблицу* адреса сетевых компьютеров, являющихся отправителями фреймов. При этом проявляется эффект обучения, когда эффективность работы коммутаторов растет с течением времени. В соответствии со своим внутренним устройством коммутаторы делятся на три класса.

- коммутаторы, использующие коммутационную матрицу;
- коммутаторы, оборудованные совместно используемой шиной;
- коммутаторы, применяющие разделяемую память.

Существуют также комбинированные устройства, сочетающие описанные выше технические подходы. Как и концентраторы, коммутаторы бывают автономные с фиксированным количеством портов, стековые и модульные. Любой коммута-

тор также характеризуется показателем производительности, который зависит от следующих факторов:

- величина внутренней адресной таблицы;
- быстродействие применяемого процессора;
- быстродействие внутренней шины;
- величина буфера, в котором хранятся сетевые фреймы;
- способ коммутации фреймов (конвейерная коммутация или полная буферизация);
- скорость фильтрации фреймов;
- величина задержки фреймов;
- скорость передачи фреймов.

Показатель скорости передачи фреймов существенно зависит от скорости, с которой принимаются фреймы во внутренний буфер коммутатора, скорости просмотра адресной таблицы в целях обнаружения порта, соответствующего указанному адресу назначения, а также скорости передачи фрейма в локальную сеть в соответствии с обнаруженным в адресной таблице портом назначения.

Скорость фильтрации фреймов определяется скоростью, с которой фреймы принимаются буфером концентратора, скоростью просмотра адресной таблицы, а также скоростью удаления фрейма, если его исходный адрес и адрес назначения относятся к одному и тому же логическому сегменту.

Величина задержки фреймов оценивается как интервал между получением первого байта фрейма входным портом коммутатора и его появлением на выходном порту коммутатора. Как правило, величина задержки не превышает 40 мкс (при конвейерной обработке фреймов) или 200 мкс (в случае обработки фреймов с полной буферизацией).

Советы по выбору коммутаторов

В процессе выбора коммутатора следует уделять внимание таким его характеристикам, как величина адресной таблицы и объем буферной памяти, предназначенной для промежуточного хранения фреймов. Показатель величины адресной таблицы определяет максимальное количество физических адресов (MAC-адресов), которые могут поддерживаться одновременно. Следует сразу определить область применения коммутатора. Если это устройство предназначено для небольших рабочих групп, вполне достаточно поддержки минимальной по объему адресной таблицы, обрабатывающей несколько десятков адресов. Если же коммутатор будет применяться в огромной локальной сети масштаба предприятия, объем адресной таблицы должен быть таким, чтобы поместить несколько тысяч MAC-адресов.

ПРИМЕЧАНИЕ На самом деле ничего страшного не произойдет, если количество физических MAC-адресов превышает возможности адресной таблицы. Коммутатор продолжит функционировать в обычном режиме, просто увеличится время задержки из-за обновления адресной таблицы.

Еще одной важной характеристикой коммутатора является емкость буферной памяти, предназначенной для временного хранения фреймов. Естественно, чем больше объем этой памяти, тем лучше. Но следует выбрать разумный компромисс, исходя из соображений стоимости устройства. Если коммутатор предназначен для использования в больших локальных сетях масштаба предприятия, объем буферной памяти должен быть не менее нескольких сотен килобайтов.

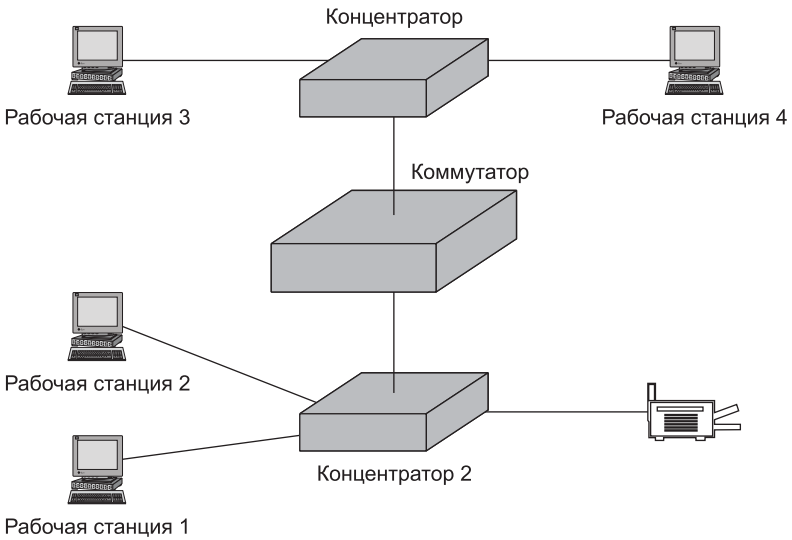


Рис. 5.7. Комбинированная сеть на базе концентраторов и коммутаторов

Помимо соображений производительности, при выборе коммутатора следует учитывать такие параметры, как количество портов и дополнительных сервисных возможностей.

Возможно создание комбинированных сетей на основе концентраторов и маршрутизаторов. Пример подобной сети приводится на рис. 5.7.

Маршрутизаторы

Под *маршрутизацией* понимается процесс доставки сетевых пакетов между конечными сетевыми узлами в сети. Этот процесс осуществляется на сетевом уровне модели OSI (3-й уровень) посредством *протоколов маршрутизации*. На этом уровне производится распределение единого логического пространства адресов, которое упрощает структурирование сетей и помогает осуществлять маршрутизацию трафика между сетями. *Маршрутизаторы* обычно снабжены несколькими сетевыми интерфейсами, предназначенными для подсоединения к локальным и глобальным сетям.

Как правило, маршрутизаторы предназначены для маршрутизации IP-пакетов, хотя могут использоваться для передачи фрагментов данных при помощи других протоколов, например IPX/SPX и AppleTalk.

Благодаря маршрутизаторам производится объединение отдельных сегментов локальной сети, в результате чего создаются более крупные (*объединенные*) сети. Эти устройства позволяют создавать гетерогенные сети, состоящие из отдельных локальных сегментов сетей Token Ring, Ethernet и т. д. Примером глобальной сети подобного рода служит Интернет, являющийся грандиозным объединением отдельных локальных сетей и персональных компьютеров, связанных между собой при помощи так называемых магистральных маршрутизаторов Интернета.

ВНИМАНИЕ Для каждого сетевого пакета устанавливается предельное количество переходов (hop), осуществляемых в процессе его прохождения через маршрутизатор. Обычно значение этого показателя равно 15, причем в результате прохождения через маршрутизатор это значение уменьшается на единицу.

Алгоритмы и протоколы маршрутизации

Выбор *маршрутов* для доставки сетевых пакетов осуществляется на основе *таблиц маршрутизации*, в которых хранятся адреса локальных сетей, обслуживаемых данным маршрутизатором. Причем в отличие от мостов, концентраторов и коммутаторов, в адресных таблицах которых хранятся физические MAC-адреса, в таблицах маршрутизации указываются адреса сетей, образующих единую объединенную сеть. Содержимое таблиц маршрутизации может пополняться за счет других маршрутизаторов, обменивающихся специальными служебными пакетами.

Алгоритмы маршрутизации, применяемые маршрутизаторами, делятся на три категории:

- алгоритмы простой маршрутизации;
- алгоритмы статической (фиксированной) маршрутизации;
- алгоритмы динамической (подстраиваемой маршрутизации).

Алгоритмы простой маршрутизации обычно не предусматривают использование таблицы маршрутизации. Маршрутизация пакетов осуществляется случайным образом по всем адресам, либо по образцу предыдущей маршрутизации.

В алгоритмах статической маршрутизации, как и следует из их названия, таблицы маршрутизации являются неизменными и загружаются при включении самого маршрутизатора. Разумеется, администратор сети может вручную добавлять или изменять записи в таблице маршрутизации.

На практике чаще всего применяются алгоритмы динамической маршрутизации. В этом случае таблица маршрутизации динамически изменяется в соответствии с измененной конфигурацией сети. Эти алгоритмы применяются специализированными протоколами маршрутизации. К их числу относятся протокол первоочередного открытия кратчайших маршрутов (OSPF, Open Shortest Path First) и протокол маршрутной информации (RIP, Routing Internet Protocol).

В протоколе RIP реализован *дистанционно-векторный алгоритм маршрутизации*, являющийся разновидностью алгоритма динамической маршрутизации. Этот алгоритм подразумевает широковещательную рассылку каждым маршрутизатором вектора, в качестве элементов которого используются значения количества пере-

ходов, отделяющего данный маршрутизатор от всех известных ему сетей. Если подобный вектор принимается другим маршрутизатором, он добавляет туда информацию, описывающую известные ему сети. Недостатки этого алгоритма связаны с его широковещательным характером и возможными неточностями в работе в больших и сложных сетях, поэтому его применение ограничивается небольшими локальными сетями.

Протокол OSPF представляет собой пример практической реализации *алгоритма состояния соединений*. Этот алгоритм предусматривает передачу каждому маршрутизатору сведений о количестве и топологии сетевых соединений. Широковещательная рассылка возникает только если меняется конфигурация сетевых соединений, поэтому объем служебного трафика будет существенно меньшим.

Обеспечение безопасности в сетях

Помимо своих непосредственных «обязанностей», связанных с обеспечением маршрутизации пакетов данных, маршрутизаторы выполняют множество дополнительных функций, к которым относится обеспечение безопасности в сети. Поскольку маршрутизатор анализирует заголовок сетевого пакета в процессе маршрутизации, можно реализовать фильтрацию «нежелательных» пакетов. Так, например, можно блокировать обмен данными через определенные порты TCP, запрещая доступ хакерам к локальной сети. Возможен также запрет доступа через Telnet, который является излюбленным инструментом компьютерных злоумышленников. Это означает, что на основе маршрутизатора может быть реализован брандмауэр.

ВНИМАНИЕ Дополнительные сведения о брандмауэрах можно найти в десятой главе.

Маршрутизаторы также могут регистрировать происходящие процессы, благодаря чему можно обнаруживать попытки незаконного проникновения в сеть.

А теперь подведем итоги и кратко опишем функции, выполняемые маршрутизаторами.

- На физическом уровне модели OSI маршрутизаторы обеспечивают физический интерфейс со средой передачи данных (кабельные и беспроводные сети), причем единственный маршрутизатор может поддерживать несколько сетей различной топологии.
- На сетевом уровне модели OSI осуществляется фильтрация маршрутизатором сетевого трафика. На основе анализа сетевых адресов принимается решение относительно корректности тех или иных пакетов данных.
- Машрутизатор может передавать пакеты данных из сетевого уровня на канальный, используя при этом протокол преобразования адресов (ARP, Address Resolution Protocol).

Нужен ли вам маршрутизатор?

Прежде, чем решиться на такой ответственный шаг, как приобретение маршрутизатора, следует задуматься над тем, нужен ли он вообще.

Несмотря на обилие замечательных качеств, присущих маршрутизаторам, необходимость в них возникает далеко не в каждой локальной сети. В частности, эти устройства не требуются, если предстоит управлять небольшой по размерам офисной локальной сетью, поскольку в этом случае можно ограничиться обычными коммутаторами. Необходимость же в маршрутизаторах появляется в том случае, когда вы имеете дело с большой сетью, состоящей из разнородных сегментов, которая к тому же подключена к Интернету. К примеру, при наличии маршрутизатора можно воспользоваться возможностями трансляции сетевых адресов (NAT, Network Address Translation). В этом случае «внешние» IP-адреса, видимые в Интернете, не совпадают с «внутренними» IP-адресами в локальной сети. Это способствует значительному повышению безопасности. Чаще всего маршрутизаторы применяют, если возникла одна из ситуаций, приведенных в следующем списке.

- рост размеров локальной сети может привести к ее перегрузке. Для решения этой проблемы следует разделить сеть на несколько подсетей, объединенных в единое целое при помощи маршрутизатора;
- когда необходима установка связи с региональными отделениями компании через Интернет;
- Для фильтрации трафика. При этом маршрутизатор исполняет роль брандмауэра.

Успешное применение маршрутизатора зависит от того, будет ли он правильно настроен. Процесс настройки маршрутизатора сродни искусству, а его описание выходит за рамки этой книги.

Если же вы решитесь на приобретение маршрутизатора, стоит обратить внимание на модели фирмы Cisco. Эта компания обладает достойным послужным списком и производит исключительно качественную продукцию (рис. 5.8). При выборе маршрутизатора нужно обращать внимание на его функциональные возможности (количество портов и тип поддерживаемых интерфейсов, наличие возможностей контроля и мониторинга сетей, быстродействие).

Рис. 5.8. Маршрутизатор от Cisco никогда не подведет

В следующей главе будут рассмотрены принципы проектирования сетей Ethernet.

6 ГЛАВА Примеры проектирования сети Ethernet

Предметом рассмотрения этой главы являются некоторые эмпирические соображения, при помощи которых можно спроектировать устойчиво функционирующую локальную сеть.

ПРИМЕЧАНИЕ Если требуется освежить в памяти некоторые физические принципы, заложенные в основу сетей Ethernet, стоит еще раз обратиться к третьей главе. Эти принципы используются в процессе проектирования сетей.

Корректное функционирование гетерогенной сети Ethernet можно обеспечить, если соблюдать несколько несложных правил.

- Количество сетевых компьютеров, одновременно работающих в сети на витой паре, не может превышать 1024. В сетях на коаксиальном кабеле количество сетевых компьютеров не превышает 30 (10BASE-2) или 100 (10BASE-5).
- Максимальная длина сетевого сегмента не может превышать предельное значение, заданное стандартом (100 метров для 100BASE-T, 185 метров для 10BASE-2 и 500 метров для 10BASE-5).
- Длительность интервала задержки при передаче сигнала между двумя самыми удаленными сетевыми компьютерами не может более чем в 575 раз превышать время, требуемое для передачи одного бита сетевого фрейма.
- Интервал между фреймами в процессе их пропускания через повторители должен как минимум в 47 раз превышать время, требуемое для передачи одного бита сетевого фрейма.

Если придерживаться этих простых правил, корректное функционирование сети гарантируется, даже если превышены ограничения на общее количество повторителей и общую длину сети (2500 м).

В процессе проектирования сети Ethernet следует придерживаться так называемого *правила 5–4–3*. В сетях Ethernet, выполненных на основе коаксиального кабеля, это правило дешифруется очень просто:

- количество сегментов, включающих в себя сетевые компьютеры, не превышает трех;
- количество повторителей, соединяющих различные сетевые сегменты, не превышает четырех;
- общее количество сетевых сегментов не превышает пяти. Причем два сегмента не могут включать в себя сетевые компьютеры и применяются только в целях обеспечения связности сети в целом.

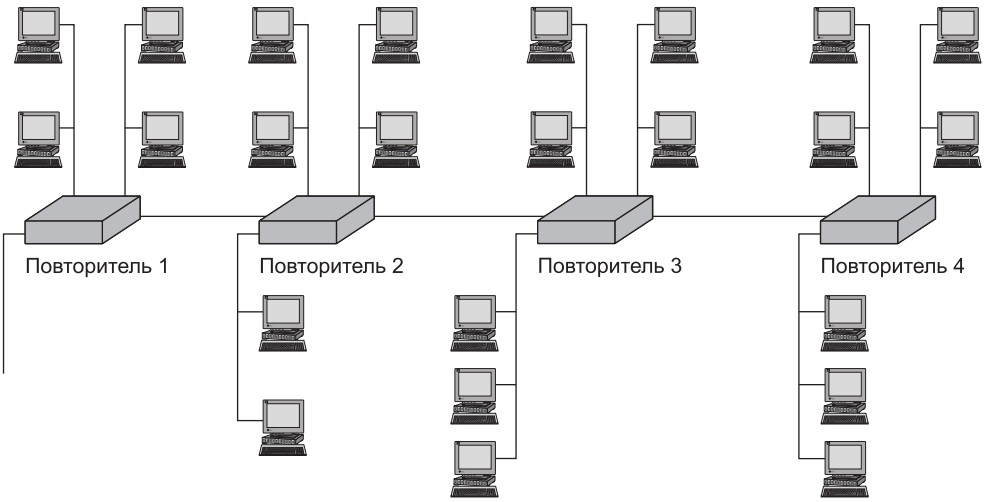


Рис. 6.1. Проектирование сети Ethernet на основе коаксиального кабеля

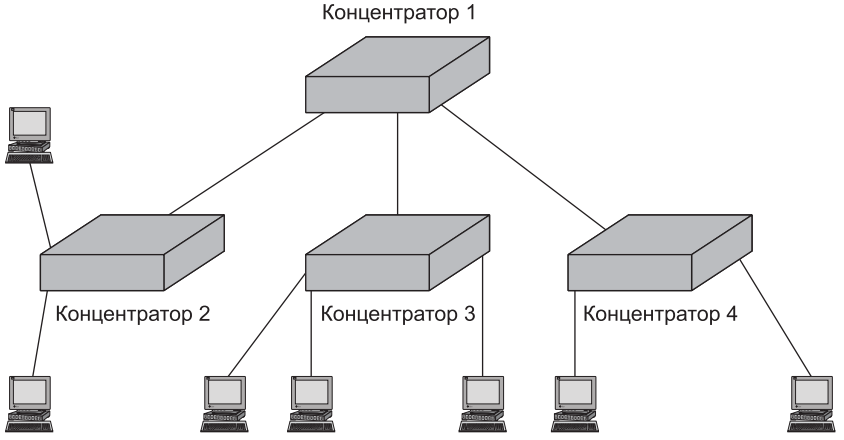


Рис. 6.2. Проектирование сети Ethernet на основе витой пары

В сетях Ethernet, реализованных на витой паре, это правило на практике означает ограничение на максимальное число каскадным образом соединенных концентраторов — не более четырех.

На рисунках 6.1 и 6.2 приводятся примеры сетей Ethernet, спроектированных на основе изложенных правил.

ВНИМАНИЕ Приведенные эмпирические правила позволяют проектировать сеть с определенным запасом прочности. На практике допускается их превышение в среднем на 10 %. Для более точного расчета сети следует воспользоваться параметрами времени задержки распространения сигнала между самыми удаленными сетевыми компьютерами и величиной задержки повторителей. Как правило, на практике необходимость в подобных точных расчетах не возникает, поэтому они здесь не приводятся.

На этом можно завершить рассмотрение основных аппаратных средств, применяемых в локальных сетях, и перейти к рассмотрению вопросов установки и настройки локальных сетей в среде Windows.

Установка и настройка локальных сетей

В главах этой части книги рассматриваются вопросы, возникающие в процессе установки и настройки локальных вычислительных сетей в среде Windows 2000/XP. Именно эти операционные системы установлены на большинстве современных персональных компьютеров, поэтому эта тема представляет наибольший интерес для пользователей.

7 ГЛАВА Установка и настройка сетей на платформе Windows 2000/XP

Важность поддержки локальных вычислительных сетей компания Microsoft осознала еще в далекие восьмидесятые годы прошлого века. Именно тогда появилась и начала триумфальное шествие по миру первая версия Windows — Windows 3.11 for Workgoups, обладающая поддержкой одноранговых локальных сетей. Одновременно с этим компания Microsoft начала разработку собственных сетевых операционных систем (Windows NT). С течением времени сетевые и обычные операционные системы неуклонно сближались, пока не появилась Windiws XP. Хотя уже Windows 2000 обладала многими «родовыми качествами» своих предшественников — Windows NT и Windows 95/98/Me.

В этой главе описываются основные инструментальные средства, применяемые для настройки и поддержки сетей, Active Directory, основные принципы управления пользователями и группами в Windows 2000/XP. Прежде чем перейти к описанию непосредственных процедур установки локальных вычислительных сетей в среде Windows XP/2000, будут рассмотрены основные проблемы, возникающие при установке или миграции в семействе операционных систем Windows 2000/XP. Здесь же можно будет найти описание типичных проблем, имеющих отношение к набору протоколов TCP/IP, и методов их устранения.

Естественно, столь сильный упор на системы Windows имеет свои причины. Несмотря на волну критики, которая обрушивается на творение Билла Гейтса, оно по-прежнему остается суперпопулярным среди домашних и корпоративных пользователей, и это вполне закономерно. Помимо всего прочего, операционные системы класса Windows 2000/XP обладают следующими поистине бесценными свойствами:

- повсеместная распространенность;
- сравнительная простота настройки и дальнейшего администрирования;

- совместимость с клиентскими компьютерами, на которых установлены операционные системы из семейства Windows 9x.

Предположим, что необходимо перевести свою сеть на платформу Windows 2000 Server или Windows XP. (До этого довольствовались системами Windows NT или даже Windows 95/98.) В таком случае возникнет ряд организационных вопросов, связанных с установкой новой операционной системы.

ПРИМЕЧАНИЕ Здесь не будут рассматриваться проблемы, связанные с установкой Windows XP, поскольку они не слишком отличаются от проблем, возникающих в процессе инсталляции Windows 2000 Server.

Организационные вопросы

Прежде чем приступить к установке операционной системы, следует тщательно все продумать. После того как вы ответите на вопрос о том, зачем нужна новая операционная система вообще, наступает время для ответа на очередной вопрос о порядке установки и дальнейшей эксплуатации сети на основе Windows 2000/XP.

Ситуация, когда подобная сеть создается впервые, — весьма типична. Это упрощает и усложняет работу одновременно.

Менее распространенной является ситуация, когда уже установлена локальная сеть на базе Windows NT 3.5/4 или Novell NetWare. При этом чаще всего возникает проблема, связанная с сохранением прежних сетевых настроек, а также пользовательских данных и приложений. В процессе инсталляции новой операционной системы могут возникать проблемы совместимости.

Ниже представлен схематичный план установки ОС, который, впрочем, не претендует на звание «истины в последней инстанции».

1. Предварительный анализ и подготовка к процессу установки.
2. Имитация полномасштабной сети на лабораторном стенде.
3. Развертывание и обкатка первых проектов.
4. Миграция на новую ОС.

Стоит несколько подробнее описать эти шаги.

Предварительный анализ и подготовка к процессу установки

На предварительном «аналитическом» этапе следует оценить время, которое потребуется для миграции к новой операционной системе. При этом нужно иметь в виду, что перед установкой новой сетевой ОС следует деинсталлировать все сетевые приложения, заархивировать наработанные непосильным трудом данные, а также выполнить ряд других неотложных работ. Исходя из этих соображений, можно смело заявить, что установка локальной сети в «чистой среде» — благо. В этом случае не требуется архивировать нужные данные. Причем перед этой процедурой потребуется «отделить зерна от плевел», что тоже весьма непросто.

ПРИМЕЧАНИЕ Имейте в виду, что внедрение локальной сети в крупной организации может занять несколько месяцев, так что к этому вопросу стоит подходить со всей ответственностью.

В процессе отбора специалистов по установке и настройке сети следует обращать внимание на то, что все они обязаны обладать знаниями и опытом работы с сетевыми протоколами Windows (TCP/IP, DHCP, SMNP, DNS, WINS), аппаратными сетевыми средствами, а также с хранилищами данных. Совсем неплохо, если бы они умели администрировать и развертывать сетевые операционные системы Windows, обладали опытом поддержки рабочих станций Windows, а также в идеале могли конфигурировать такие устройства, как коммутаторы и маршрутизаторы.

Естественно, перед осуществлением самой установки потребуется оценить текущую ситуацию на самой фирме, а также подготовить перечень убедительных аргументов для руководства компании, способных убедить последнее в необходимости и целесообразности осуществления всего комплекса работ. Безусловно, любые изменения могут привести к совершенно непредсказуемым осложнениям, поэтому руководство обычно страдает «здоровым консерватизмом». Придется призвать на помощь все свое красноречие и пробудить в себе дар убеждения, поскольку все это вам понадобится для «выбивания» средств, необходимых для осуществления проекта. Все будет гораздо проще, если руководство компании знает и ценит вас как грамотного специалиста, мнение которого является определяющим.

Предположим, что этап «психологической обработки» руководства завершился вашей убедительной победой. В этом случае важно не «почивать на лаврах», а незамедлительно перейти к следующему этапу. Нужно проанализировать потребности компании в разрезе тех или иных технологий и решений. От результатов практической реализации этого этапа будет зависеть успех всего проекта в дальнейшем. При этом следует учитывать не только актуальные потребности, но и те из них, которые могут возникнуть в ближайшие годы. Нужно тщательно проанализировать конкурентные преимущества вашей компании, ее «сильные» и «слабые» стороны, поскольку все это вместе взятое влияет на эффективность развертывания и эксплуатации сети в дальнейшем. Обратите внимание на ключевые моменты, имеющие отношение к любой компании и влияющие на решения, касающиеся внедрения новых технологий:

- факт поддержки со стороны руководящего и управляющего звена компании;
- величину наличных денежных средств;
- резерв времени, требуемого для перехода на использование новой системы;
- наличие материальных ресурсов;
- наличие и специфика трудовых ресурсов;
- наличие необходимых технических специалистов;
- инфраструктуру будущей сети;
- существующие технологии и системы;
- цели и задачи компании;
- деятельность конкурентов.

Имитация полномасштабной сети на лабораторном стенде

После получения необходимых материальных и трудовых ресурсов самое время задуматься о лабораторных испытаниях. Необходимость такого шага мотивируется тем, что перед установкой полномасштабной сети Windows 2000/XP следует произвести рабочую проверку всех используемых сетевых компонентов (маршрутизаторов, концентраторов, шлюзов), а также программного обеспечения, устанавливаемого на рабочих станциях и серверах.

Для лаборатории следует выделить отдельное помещение, снабженное надежным замком. Размеры помещения должны быть достаточными для того, чтобы в нем разместились десятки серверов, принтеров, а также другие компоненты. Иногда в реальной сети можно обойтись небольшим количеством серверов (даже одним), а бывают такие ситуации, когда локальная сеть становится настолько громоздкой, что требует установки 20–30 серверов.

На этом этапе также следует приступать к проектированию логической и физической структуры сетевого домена. Это подразумевает также настройку ключевых ролевых серверов (контроллеры доменов, серверы сертификатов, серверы лицензирования, серверы DHCP и т. д.).

Не следует также забывать о необходимости соблюдения безопасности при работе над проектом. Нужно применять различные уровни шифрования и средства обеспечения безопасности (например, идентификация пользователей на основе их биометрических характеристик).

После завершения проектирования логической и физической структуры сети, а также определения основных свойств подсистемы безопасности наступает этап испытаний на лабораторном стенде. При этом тестируются основные политики, службы DNS, WINS, DHCP, хранилища данных, порядок организации доступа к файлам и принтерам, а также некоторые другие параметры.

Нужно оценить преимущества и недостатки, связанные с переходом компании на использование ОС Windows 2000/XP. В любом случае придется составить перечень проблемных ситуаций, которые могут возникнуть в процессе перехода на новую сетевую операционную систему. Одна из подобных весьма неприятных ситуаций связана с невозможностью доступа к локальным сетевым ресурсам, являющимся местом хранения жизненно необходимых данных. Переход на новые технологии может быть также связан с временным блокированием доступа к Интернету. Неприятность этой ситуации усугубляется тем, что останавливается деловая электронная переписка, а также становится невозможным доступ к корпоративному веб-сайту.

Перед тем как приступить к полномасштабному тестированию, следует смоделировать возможные ситуации. Нужно создать схему, которая будет адекватно отображать инфраструктуру и топологию сети, тестируемой в лаборатории. На этой схеме будут изображены домены, рабочие станции и серверы (входящие в состав доменов), а также сетевые компоненты, обеспечивающие передачи данных.

Если тестовая лаборатория создается впервые, выберите для ее размещения изолированное, достаточно просторное помещение. Назначьте сотрудника, отвечающего

за лабораторию, следует также позаботиться о наличии надежного электроснабжения, средств пожаротушения и надежной двери с хорошими замками.

На следующем этапе потребуется выполнить работы по установке сети. Руководствуясь ранее разработанным планом, следует разместить концентраторы, маршрутизаторы, а также другое необходимое сетевое оборудование.

Составьте список серверов, которые планируется установить в лаборатории, а также определите необходимое количество клиентских станций. При выборе концентраторов ориентируйтесь на максимально возможное количество подключаемых к сети клиентов. Так, если в сети будет установлено не более 10 клиентов, вряд ли стоит приобретать 24-портовый концентратор.

В лаборатории следует использовать средства эмуляции сети, которые полностью имитируют топологию реальной сети, а также отображают взаимодействие между ее узлами. Репликация данных, осуществляемая между контроллерами доменов либо серверами DNS и WINS, выполняется следующим образом. Просто настройте обе сети, затем объедините их с помощью серверов удаленного доступа. При этом можно воспользоваться двумя модемами, обеспечивающими скорость передачи данных в 56 Кбит/с, а еще лучше — широкополосным соединением.

Серверы в сети Windows 2000 Server могут исполнять различные роли. И весьма желательно опробовать их в каждой из этих ролей для того, чтобы не возникало проблем в процессе реальной установки и эксплуатации локальной сети. В табл. 7.1 приводится краткое описание различных ролей серверов.

Таблица 7.1. Перечень серверов и выполняемых ими ролей (в среде Windows 2000)

Роль сервера	Описание
Контроллер домена	Этот сервер является основным для службы каталогов Active Directory. Следует обеспечить зеркальное копирование данных для этого сервера, воспользовавшись партнерами репликации. В этом случае обеспечивается поддержка избыточности
Сервер DNS	Сервер, на котором выполняется служба доменных имен DNS. Эти службы следует запускать на выделенных серверах (если домен имеет небольшие размеры, этой рекомендации можно не придерживаться). В больших сетях серверы DNS обычно взаимодействуют с другими серверами
Сервер DHCP	В обязанности сервера DHCP входит назначение IP-адресов. Эта служба может устанавливаться на сервере, где уже выполняются службы DNS и WINS, но лучше для этого использовать выделенный сервер. Особенно этот совет актуален, когда сеть перегружена, в результате чего возникают заторы
Сервер WINS	Этот сервер применяется для определения имен NetBIOS на основе заданного IP-адреса. В больших корпоративных сетях в этом случае используется выделенный сервер
Сервер IIS	Сервер IIS (Internet Information Services, информационные службы Интернета) входит в комплект поставки Windows 2000 Server, а также Windows XP. Этот компонент реализует поддержку служб FTP и Web в локальной сети, а также выполняет функции сервера Интернета. Для его установки рекомендуется использовать выделенный сервер (даже в условиях тестовой лаборатории)

Роль сервера	Описание
Сервер печати	Специальный сервер, обеспечивающий поддержку логических сетевых принтеров, а также выполняющий обработку запросов на печать
Файл-сервер	Этот сервер обеспечивает функционирование файловых служб и хранилищ. Обычно на файл-сервере устанавливаются отказоустойчивые дисковые массивы RAID-0–RAID-5, а сами серверы объединяются в кластеры для обеспечения дополнительной отказоустойчивости
Телефонный сервер	Этот сервер обеспечивает поддержку телефонных служб, использующих интерфейс телефонных приложений (TAPI, Telephony Application Programming Interface). Данный сервер обеспечивает функционирование служб обмена сообщениями, факсами, а также реализует IP-телефонию
Кластерный сервер	Данный сервер поддерживается только в версии Windows 2000 Advanced Server. Если же ваша цель заключается в изучении различных методов выравнивания нагрузки в сети, тогда имеет смысл установить и опробовать кластеры серверов в испытательной лаборатории
Сервер базы данных	Этот сервер обеспечивает поддержку баз данных, таких как SQL Server 2000, а также некоторых других
Почтовый сервер	Данный сервер выполняет задачи по маршрутизации и пересылке электронной почты
Сервер RAS	Служба удаленного доступа (Remote Access Service) предназначена для удаленного доступа к серверу Windows 2000 Server
Сервер резервного копирования	Этот сервер предназначается для резервного копирования данных с других серверов и рабочих станций
Сервер приложений	Серверы приложений обычно устанавливаются на выделенных рядовых серверах. К ним относятся терминальные службы, серверы компонентов и службы индексирования
Сервер сертификатов	Сервер сертификатов обеспечивает поддержку цифровых сертификатов стандарта X.509, отвечающих за проверку подлинности отправителя сообщения
Сервер лицензий	Сервер лицензий предназначен для определения факта соответствия лицензионным требованиям, которые выдвигает Microsoft

Естественно, столь обширный список вовсе не обязательно реализовывать на практике в полном объеме. Не следует устанавливать несколько служб (особенно если они выполняют различные функции) на одном и том же выделенном сервере.

ПРИМЕЧАНИЕ Обратите внимание на то, что в сетях Windows Server 2003 серверы выполняют аналогичные роли.

Имейте в виду, что в тестовой лаборатории изначально следует тестировать контроллер корневого домена. Служба каталогов Active Directory должна устанавливаться только в том случае, если были инсталлированы все необходимые компоненты системы (в том числе и сетевые компоненты), а также произведена проверка их стабильного функционирования.

После того как будет завершена установка контроллера домена и службы каталогов Active Directory, следует приступать к настройке учетных записей групп. Следующим этапом является установка сервером DNS, DHCP, WINS, а также других серверов и сетевых служб.

Развертывание и обкатка первых проектов

А теперь пришло время оценки первых результатов, полученных на этапах подготовки к процессу установки. На данном этапе необходимо контролировать процесс выполнения тех или иных задач, а также производить анализ возникающих в рабочем процессе проблем. При этом не следует терять связь с руководством, постоянно согласовывая с ним установку серверов и сетевой рабочей среды.

Затем начинается осуществление первых проектов. В качестве подобных проектов может выступать установка ролевого сервера (DHS, DHCP и т. д.), развертывание службы каталогов Active Directory, а также некоторые другие проекты. Необходимо проверить функционирование службы безопасности (установка и использование доверительных отношений, протокол Kerberos, служба NTLM, различные файловые системы, удаленный доступ пользователей, протоколы IPSec и RAS).

Миграция на новую ОС

После успешного внедрения первых проектов можно переходить к выполнению главной задачи — переводу корпоративной информационной системы на новую операционную систему. При этом следует фиксировать каждый выполняемый шаг для того, чтобы в случае возникновения каких-либо проблем можно было бы совершить откат назад и разобраться в причинах создавшейся ситуации.

Определение метода установки и настройки системы

Итак, вы завершили анализ предварительных условий и готовы приступать непосредственно к самому процессу установки. Закончены предварительные испытания, выбраны роли, которые будут играть серверы вашей будущей сети. Далее все зависит от того, с какой целью производится установка Windows 2000 Server или Windows XP. Некоторые разновидности систем будут рассмотрены далее.

Базовая система

В данном случае предъявляются минимальные требования к аппаратному обеспечению, призванному поддерживать функционирование сервера. Можно воспользоваться простейшей однопроцессорной материнской платой и ограничиться минимальным количеством оперативной памяти (128 Мбайт). Этот «джентльменский набор» дополняется одним жестким диском с интерфейсом EIDE (или SATA), дисководом компакт-дисков, стандартным флоппи-дисководом, сетевым адаптером (отдельным или интегрированным в состав системной платы), монитором, клавиатурой и мышью.

В этой комплектации могут использоваться процессоры Pentium с тактовой частотой 233 МГц, поэтому компьютеры, приобретенные 7–8 лет назад, смогут послужить вам верой и правдой еще не один год.

Маломощный выделенный сервер

Службы файлов и печати выполняются на специализированных серверах, именуемых *файл-серверами* и *серверами печати*, соответственно. В этом случае потребуется второй жесткий диск большего объема, как минимум 40 Гбайт, а также стандартные периферийные устройства, используемые для подключения принтеров и иного дополнительного оборудования. Объем оперативной памяти в этом случае должен составлять как минимум 128 Мбайт. Хотя можно воспользоваться памятью объемом в 256 Мбайт, исходя из экономических соображений. В роли центрального процессора в этом случае лучше использовать Pentium II с тактовой частотой 300 МГц (можно также применить Celeron с тактовой частотой 366 МГц или большей).

Сервер приложений

Под *сервером приложений* подразумевается сервер, выполняющий прикладные программы (в данном случае имеются в виду службы терминалов). Сюда входят системы управления базами данных, коммуникационные программы, а также приложения, реализующие управление сетью.

Службы терминалов

Сервер терминалов впервые появился в составе операционной системы Windows NT еще в 1997 году (TSE, Windows NT 4 Terminal Server Edition).

В состав Windows 2000 Server (Windows XP) служба терминалов входит в качестве неотъемлемой части. Результатом ее функционирования является то, что пользователи могут запускать свои приложения на сервере. При этом желательно ограничивать количество пользователей, работающих с сервером. Нужно следить, чтобы одновременно выполнялось не более четырех приложений. Настраивайте приложения таким образом, чтобы исключить использование громоздких рабочих столов, приводящих к чрезмерной перегрузке системы.

Если к серверу подключаются не более пяти пользователей, тогда достаточно использовать процессор Pentium II, который работает на тактовой частоте 300 МГц. На выполнение каждого приложения отводится 32 Мбайт оперативной памяти. Если максимальное количество одновременно выполняемых приложений на сервере не превышает пяти, общий объем памяти равняется 288 Мбайт (128 Мбайт (операционная система) + 160 Мбайт (пять приложений, каждое из которых занимает до 32 Мбайт оперативной памяти)). Конечно, можно обойтись и меньшим объемом оперативной памяти, но могут возникать определенные проблемы, если к серверу одновременно подключаются до пяти пользователей и каждый из них открывает больше двух приложений.

Ролевой сервер

Ролевые серверы предназначены для выполнения различных служб (например, Active Directory, DNS, DHCP или WINS). Если подобные службы используются достаточно интенсивно, следует выбирать центральный процессор Pentium II, работающий на тактовой частоте начиная с 300 МГц.

Сервер, рассчитанный на большие нагрузки

Если планируется установка сервера, предназначенного для решения критически важных задач, которые требуют значительного объема вычислительных системных ресурсов, рекомендуется воспользоваться процессором Pentium II (или даже Pentium III) с тактовой частотой не менее 400 МГц. Можно также рассмотреть вариант использования двухпроцессорной (или даже четырехпроцессорной) системы.

Объем жесткого диска (одного или нескольких) может доходить до 250 Гбайт, причем рекомендуется использовать винчестер, поддерживающий технологию RAID-5. Возможностями по поддержке этой технологии обладают некоторые контроллеры жестких дисков (как правило, SCSI).

Еще больше повысить степень отказоустойчивости сервера можно с помощью применения технологии кластеризации, обеспечивающей поддержку нескольких серверов. Возможности кластеризации поддерживаются версиями Windows 2000 Advanced Server (Windows 2003 Server).

Оборудование

В процессе установки операционной системы Windows 2000 Server (Windows XP) следует обратить свое внимание на выбор следующих компонентов:

- системная плата;
- процессор;
- оперативная память;
- контроллер жесткого диска;
- жесткий диск;
- сетевой адаптер.

Сетевые адаптеры подробно рассматривались в главе 5.

Список совместимого аппаратного обеспечения

Прежде чем приступать к поиску и приобретению необходимого оборудования, нужно просмотреть содержимое папки \support, которая находится на компакт-диске с операционной системой Windows 2000 Server (Windows XP). Если устанавливаемый в системе аппаратный компонент отсутствует в списке, следует обратиться к веб-сайту фирмы Microsoft по адресу http://www.microsoft.com/whdc/hcl/default.mspx (рис. 7.1). Естественно, этот список не исчерпывает все возможные

варианты, но все же лучше его придерживаться. В этом случае при возникновении каких-либо проблем при установке легальной копии Windows 2000 Server (Windows XP) вы имеете полное право на поддержку компании Microsoft.

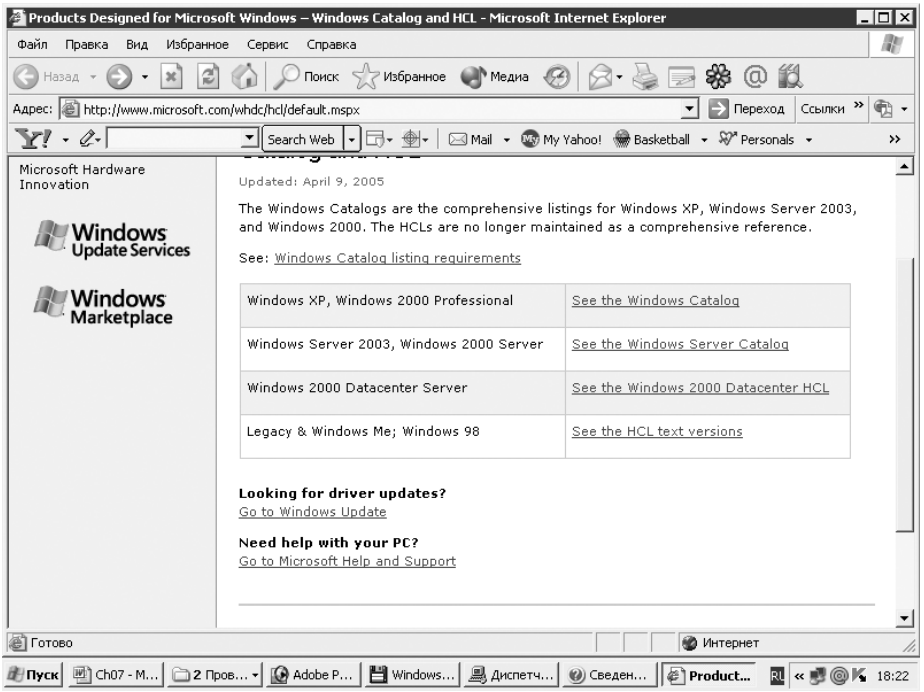


Рис. 7.1. Начальная страница веб-сайта, включающего список совместимого оборудования

Системные платы

Данные аппаратные компоненты характеризуются присущими им размерами и формой. Далее перечислены основные параметры системных плат, устанавливаемых в серверах.

- Форм-фактор системной платы. Этот признак позволяет отнести системную плату к одной из следующих категорий: AT (до сих пор немало серверных плат, особенно рассчитанных на различные варианты ОС Linux, поддерживают именно этот стандарт), ATX (наиболее популярный на сегодняшний день стандарт), BabyATX и MicroATX. Два последних стандарта предназначаются для использования в домашних ПК, поскольку им присуще меньшее количество разъемов, а также худшие условия для охлаждения и размещения таких серверных компонентов, как жесткие диски. Поэтому системные платы, предназначенные для использования на сервере, характеризуются форм-фактором AT и ATX.
- Слоты. На любой системной плате установлено несколько слотов (разъемов), количество которых может быть больше десяти. В настоящее время распространены материнские платы, на которых установлены разъемы PCI, PCI

Express или AGP. Стоит выбирать плату с 4-5 разъемами PCI. Для сервера наличие разъема AGP не является обязательным, поскольку монитор к нему обычно не подключается.

- Разъемы для установки модулей оперативной памяти. Оперативная память устанавливается в слоты SIMM (устаревший стандарт), DIMM (более новый стандарт), DDR и DDR II (современный стандарт, который не столь часто распространен в случае именно серверных системных плат). Ориентируйтесь на приобретение системных плат со слотами DIMM/DDR, обеспечивающими оптимальное соотношение цены и качества.
- Гнезда, предназначенные для установки центральных процессоров. В настоящее время доступны системные платы со следующими гнездами, предназначенными для установки центральных процессоров: Socket 7, Slot 1/Socket 370, Socket 478, Socket 775, Socket A, Socket 754 и Socket 939. Последние пять слотов предназначены для установки наиболее современных процессоров: Pentium 4 от Intel и Athlon от AMD. Слоты Socket 7 используются для установки процессоров Pentium 1, а слоты Slot 1/Socket 370 — Pentium II/III или Celeron.

Процессоры

При выборе процессора следует руководствоваться соображениями, связанными с требуемой производительностью и ценой этого устройства. Следует выбирать процессоры известных производителей: Intel или AMD. Попробуйте также поискать процессор в списке совместимости аппаратного обеспечения от фирмы Microsoft.

Жесткие диски

При выборе жесткого диска, предназначенного для сервера, следует исходить из предъявляемых к нему требований, связанных с областью применения, условиями эксплуатации, а также некоторыми другими факторами.

Существуют два основных стандарта жестких дисков, применяемых в настоящее время: IDE (EIDE), SATA/SATA II и SCSI (SCSI-2, SCSI-3 и Ultra SCSI). Имеет смысл использовать диск стандарта SCSI для поддержки большого количества пользователей, профессиональных ролевых серверов, а также терминальных служб и BackOffice.

Следует обратить внимание на параметры дисков SCSI, которые помогут сделать правильный выбор.

- Быстродействие. Жестким дискам SCSI присуще более длительное время передачи данных, а также время доступа, чем дискам с интерфейсом EIDE.
- Емкость. Наиболее распространенные диски SCSI обладают емкостями 9,1–30 Гбайт, тогда как диски EIDE выпускаются с объемом от 40 до 250 Гбайт.
- Адресация. Можно подключать до 15 дисков стандарта Ultra SCSI к одному сигнальному кабелю.
- Поддержка. Множество технологий поддержки ориентированы на жесткие диски стандарта SCSI: горячая замена дисков, хранилища данных и устройства для отключения, профессиональные контроллеры дисковых RAID-массивов.

СОВЕТ Обратите внимание на то, что диски SATA сочетают лучшие качества дисков EIDE и SCSI, поэтому имеет смысл остановиться именно на них.

Следует также отметить тот факт, что диски с интерфейсом SCSI отличаются большой степенью надежности, поэтому, несмотря на прочие их недостатки, иногда именно на них следует остановить свой выбор.

Как правило, стандартные контроллеры жестких дисков встроены в материнские платы. Для подключения жестких дисков стандарта SCSI потребуются специальные SCSI-адаптеры, хотя серверные материнские платы также снабжены контроллерами дисков SCSI.

Установка ОС Windows

Перед установкой операционной системы следует определить роль, возлагаемую на будущий сервер. В зависимости от этого изменяется перечень выполняемых действий.

Если устанавливается автономный сервер, следует определить следующие параметры:

- имя рабочей группы;
- пароль администратора;
- сетевой протокол;
- IP-адрес;
- IP-адрес сервера DNS.

В процессе установки рядового сервера потребуется определить следующие параметры:

- имя рабочей группы;
- пароль администратора;
- сетевой протокол;
- IP-адрес сервера DNS.

Установка ролевых серверов потребует определения следующих параметров:

- имя рабочей группы;
- пароль администратора;
- сетевой протокол;
- IP-адрес;
- IP-адрес сервера DNS;
- сведения о ролевой службе.

В процессе установки *контроллера доменов* можно настроить компьютер в качестве рядового сервера, а уже затем изменить его настройки по завершении установки. Можно также определить статус контроллера домена в процессе выполняемой установки. Рекомендуется воспользоваться последним способом, за исключением отдельных случаев, когда вам захочется поэкспериментировать.

Существует несколько причин, затрудняющих или даже полностью исключающих преобразование сервера в контроллер домена в процессе установки или непосредственно после ее завершения. Следует отметить, что операция преобразования контроллера домена является достаточно длительной. Может также потребоваться отключение контроллера домена, что нежелательно в силу ряда причин.

При установке контроллера домена потребуется определить следующие параметры:

- имя домена (в случае создания нового домена потребуется указание родительского домена; если же контроллер домена добавляется в существующий ранее домен, нужно точно указать имя данного домена);
- пароль администратора;
- сетевой протокол;
- IP-адрес;
- IP-адрес сервера DNS.

В следующих разделах описываются действия, выполняемые в процессе установки Windows 2000 Server. Установка Windows XP происходит аналогичным образом, поэтому отдельно не рассматривается.

Разбиение жесткого диска на разделы

В процессе установки операционной системы первый дисковый раздел отводится под размещение системных файлов. Именно он и будет называться *системным*.

Второй раздел именуется *загрузочным* и применяется для размещения загрузочных файлов, требуемых для выполнения загрузки основной части операционной системы.

Исходя из требований к безопасности, считается оптимальным использование двух жестких дисков (один диск в качестве системного, а второй — в качестве загрузочного). Далее приводится описание вариантов установки с использованием одного или двух жестких дисков.

При использовании одного жесткого диска загрузочные и системные файлы размещаются на различных логических дисках, но на одном физическом диске. В этом случае нужно выделить раздел для установки системных файлов размером, как минимум, в 2 Гбайт. Причем желательно отформатировать этот раздел с применением файловой системы NTFS. Если же используются два жестких диска, достаточно выбрать их объем, равный 2 Гбайт для каждого диска.

Один из дисков можно отформатировать с помощью файловой системы NTFS, а второй — с помощью файловой системы FAT16/FAT32. Таким образом появляется возможность реализации множественной загрузки, когда на одном и том же компьютере могут загружаться несколько операционных систем, использующих различные файловые системы (например, Windows 98 и Windows XP).

Иногда все же лучше использовать второй жесткий диск для хранения зеркальной копии данных, благодаря чему повышается отказоустойчивость системы в целом.

Базовый вариант установки

Установка, выполняемая с компакт-диска, включает четыре этапа:

1. запуск программы установки на выполнение;

2. применение мастера установки;
3. настройка сетевых компонентов;
4. выполнение финальной настройки.

Использование мастера установки

Мастер установки (в Windows 2000 Server/XP) автоматизирует прохождение шагов установочного процесса.

ПРИМЕЧАНИЕ Вполне естественно, что процесс установки Windows XP немного отличается от процесса установки Windows 2000 Server, но эти отличия не столь значительны, поэтому здесь рассматриваться не будут.

1. Региональные установки. На данном этапе администратор, производящий установку, должен выбрать язык, указать местонахождение, а также используемую раскладку клавиатуры. Можно также настроить сервер на применение нескольких языков и региональных настроек. При выборе нескольких языков Windows устанавливает таблицы символов для каждого из них.
2. Имя и организация. Здесь потребуется указать имя оператора данного компьютера, а также название организации, которая приобрела лицензию на данный программный продукт.
3. Способ лицензирования. В этом диалоговом окне можно выбрать лицензию из расчета на одно рабочее место или на один сервер. Если выбирается лицензия на один сервер, потребуется указать количество лицензий, приобретенных с целью обеспечения доступа клиентов.
4. Имя компьютера. На этом шаге потребуется указать имя компьютера. При этом Windows 2000 выбирает имя, которое изначально задано по умолчанию и может быть изменено пользователем. В данном случае проще воспользоваться каким-либо осмысленным именем.
5. Пароль, блокирующий учетную запись администратора. Используемый в этом случае пароль блокирует учетную запись администратора системы. Поэтому злоумышленник, не знающий тайны «золотого ключика», не сможет воспользоваться практически неограниченными административными правами доступа.
6. Компоненты Windows 2000. На данном этапе выполняется установка дополнительных компонентов и служб Windows 2000. Большинство из них может быть настроено позднее, поэтому не стоит тратить драгоценное время. Лучше перейти сразу к установке сетевых параметров. Здесь подразумевается ввод сведений, имеющих отношение к серверам DNS, DHCP, а также установка сетевых протоколов и служб. Установка некоторых служб (службы IIS и транзакций) предлагается по умолчанию. Поэтому если установка этих служб не требуется, следует отменить установки соответствующих флажков.
7. Службы терминалов. На этом шаге администратор может выбрать режим функционирования службы терминалов. В данном случае выбирается режим администрирования, который может быть изменен в дальнейшем.
8. Настройки отображения. На этом шаге указывается разрешение экрана, количество используемых цветов, настраивается способ вывода изображения

с помощью видеоадаптера (например, частота обновления видеоизображения). Многие настройки, определяющие отображение на экране, можно оставить заданными по умолчанию. Правда, придется изменить стандартное экранное разрешение 640 × 480 на 800 × 600 или даже на 1024 × 768 (для мониторов с размером по диагонали 17 дюймов или большим).

9. Время и дата. На этом шаге потребуется указать временной пояс, а также установить флажок, определяющий автоматический переход на летнее время. После завершения ввода всех необходимых данных происходит автоматический переход к третьей фазе процесса — установка сетевых компонентов.

Установка сетевых компонентов Windows

На этом этапе программа установки Windows начинает процесс установки сетевых компонентов. При этом предпринимаются попытки автоматического обнаружения сетевого адаптера. Если в системе установлен сетевой адаптер, выпущенный хорошо известным и зарекомендовавшим себя производителем, то особых проблем не возникнет. Ниже описаны соответствующие шаги, имеющие отношение к данному этапу.

1. Обнаружение сетевого адаптера. После того как было произведено обнаружение и установка драйверов для сетевого адаптера, установочная программа Windows 2000 Server предпринимает попытки по обнаружению местоположения сервера DHCP в сети. Для этого производится трансляция пакетов в направлении порта 75, а также прослушиваются ответы, генерируемые сервером DHCP. Если таким образом Windows 2000 не может получить значение IP-адреса, используются возможности протокола автоматического конфигурирования в целях автоматического выделения IP-адреса. После этого можно продолжить процесс установки сетевых компонентов, отложив установку необходимых рабочих групп и выполнение требуемых сетевых настроек.
2. Сетевые компоненты. На этом шаге производится выбор устанавливаемых сетевых компонентов. В их состав входят Client for Microsoft Networks (Клиент для сетей Microsoft), File and Print Sharing for Microsoft Networks (Совместное использование файлов и печати для сетей Microsoft), а также набор протоколов TCP/IP. Можно установить другие службы и компоненты в любое время после завершения процесса установки.
3. Рабочая группа или домен. Если производится установка в существующий домен, понадобится указать имя учетной записи администратора и пароль. Благодаря этим сведениям можно создать новую учетную запись в домене. Если в процессе установки внутри ранее существующего домена возникли какие-либо проблемы, установите рабочую группу. Если рабочей группы пока не существует, укажите ее имя.

Завершающая настройка

Эта стадия установки включает завершающее копирование файлов, настройку компонентов, построение списка ненужных файлов с их последующим удалением.

Сведения о новой конфигурации сохраняются в базе данных системного реестра, а также на жестком диске.

Установка через локальную сеть

Установка операционной системы Windows 2000 Server возможна с помощью так называемых *точек общего доступа*, которые также могут называться дисками или серверами распределения.

Если распределенный общий ресурс создать затруднительно, нужно скопировать содержимое папки i386 с компакт-диска на жесткий диск и открыть к нему общий доступ. Процесс установки в этом случае выглядит следующим образом.

1. На целевом компьютере нужно создать раздел FAT16. Если размер раздела не превышает 2,1 Гбайт, можно воспользоваться программой FDISK, входящей в комплект поставки MS-DOS. Если же величина создаваемого раздела превышает 2 Гбайт, придется воспользоваться файловой системой FAT32 и 32-разрядной версией программы FDISK.
2. Загрузите сетевую клиентскую программу. При этом можно использовать загрузочную дискету Windows 95/98, а также некоторые DOS-программы. Обычно клиенты MS-DOS содержат файлы, имеющие отношение к протоколу TCP/IP, системные файлы DOS-оболочки, обеспечивающие минимальное функционирование компьютера, а также драйверы сетевого адаптера.
3. Потребуется создать конфигурационные файлы, которые позволяют использовать распределенные точки общего доступа, загружаясь через сеть.

После подключения к точке общего доступа через сеть запустите программу установки winnt.exe, воспользовавшись компакт-диском с системой Windows 2000 Server. Эта программа начнет работу, распределив ее на несколько стадий:

- программа winnt.exe создаст четыре загрузочных дискеты Windows 2000 Server (дискеты должны быть предварительно отформатированы).
- на целевом компьютере будет создана временная папка win_nt.
- программа winnt.exe скопирует основные установочные файлы во временную папку на целевом сервере.

Проблемы на этапе установки и их устранение

Как правило, при установке Windows 2000 Server особых проблем не возникает, но всякое правило имеет свои исключения. То же самое можно сказать и в этом случае.

Иногда бывает так, что программа установки просто зависает, не выполнив и половины возлагаемых на нее задач. При этом на экране отображается сообщение об ошибке, либо просто появляется «синий экран смерти».

Если случилась подобная неприятность и компьютер не реагирует на нажатие каких-либо клавиш, просто выключите его и включите снова через 10–20 секунд. Если это не поможет, тогда попробуйте повторно запустить программу установки. В случае, когда «зависание» повторяется с удручающей периодичностью, придется перейти к методу последовательного выявления аппаратных компонентов, вызывающих сбои. Нужно по очереди удалять компоненты системы, заменяя их аналогами от других производителей, и смотреть на реакцию программы установки. Этот метод должен обязательно помочь в любой ситуации.

Завершение установки

После завершения установки системы и регистрации в ней с использованием учетной записи администратора, Windows 2000 Server автоматически отобразит экран Настройка сервера Windows 2000 (рис. 7.2). С помощью этого инструментального средства производится настройка таких компонентов, как Active Directory, службы DNS, DCHP и т. д. В принципе, все необходимые настройки можно выполнить позднее, поэтому данный инструмент можно не использовать.

А теперь рассмотрим основные инструментальные средства, с помощью которых обеспечивается установка и настройка локальных сетей (в среде Windows 2000/XP).

Консоль управления Microsoft

Консоль управления Microsoft (MMC, Microsoft Management Console) представляет собой некий центр, обеспечивающий единое управление административными апплетами, которые отвечают за настройку многих параметров системы. Консоль MMC является нововведением, появившимся в операционных системах семейства Windows 2000. Ранее настройка системы могла производиться исключительно с помощью апплетов системы управления.

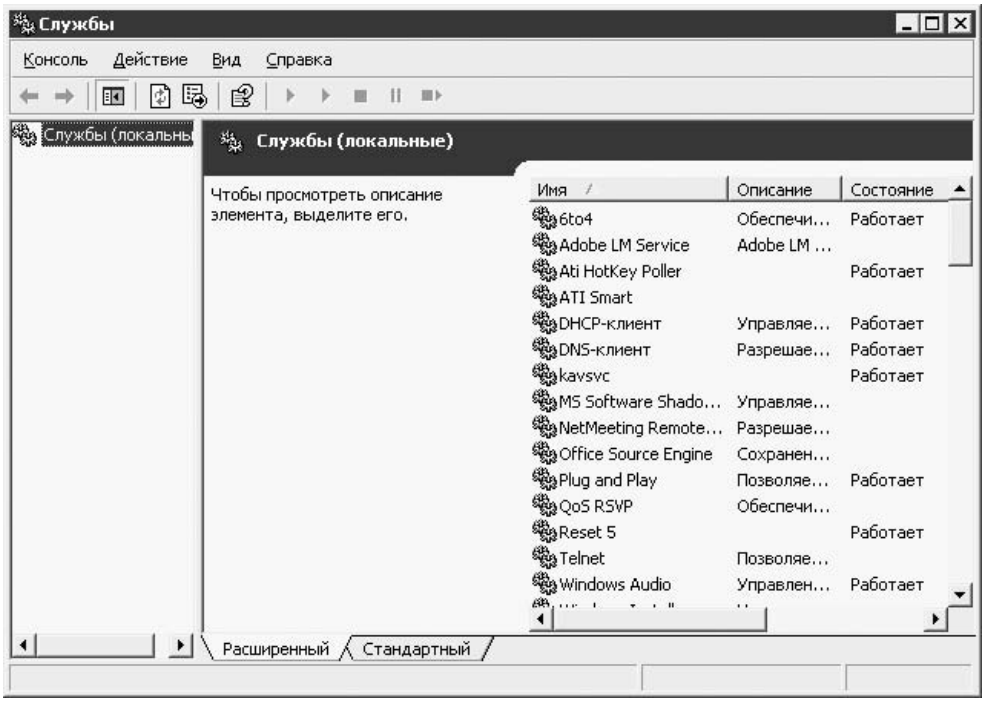


Рис. 7.2. Консоль управления Microsoft

Консоль управления Microsoft представляет собой некую оболочку, включающую инструменты администрирования системы, именуемые *оснастками*. На рис. 7.2 приводится пример консоли управления с загруженной оснасткой Управление компьютером. Именно эта оснастка позволяет устанавливать основные системные параметры.

ВНИМАНИЕ На рис. 7.2 изображена консоль управления Microsoft из Windows XP, которая весьма напоминает консоль MMC из Windows 2000 Server.

Консоль управления позволяет объединить инструменты администрирования в единое целое, в результате чего становится возможным формирование некоего «административного окна», содержащего весь набор применяемых данным пользователем инструментов.

Доступ к консоли MMC

Для того чтобы открыть консоль MMC, достаточно выбрать соответствующий ярлык в папке Администрирование, в меню — кнопку Пуск или дважды щелкнуть на значке в окне проводника. Можно также воспользоваться режимом командной строки, в которой следует указать следующий синтаксис:

```
MMC путь \имя_файла.msc /a /s
```

Обратите внимание на описание параметров команды:

- Путь \имя_файла.msc. Вместо параметра путь указывается путь к файлу консоли управления, определенному под именем имя_файла.msc. В этом случае можно указать полный путь или воспользоваться переменной %systemroot% в целях указания пути к папке, в которой находятся файлы Windows 2000 на локальном компьютере.
- /a. Этот переключатель определяет переход в авторский режим (в среде Windows 2000), а также разрешает изменения для консоли.
- /s. Этот переключатель позволяет отменить заставку, которая обычно появляется при запуске консоли MMC на платформах Windows 9x или Windows NT.

Можно выбрать авторский режим работы с консолью, если в контекстном меню оснастки в папке Администрирование выбрать команду Свойства. В отобразившемся окне свойств на вкладке Ярлык следует установить переключатель /a.

Например, для переключения в авторский режим консоли MMC сервера DNS следует ввести следующую команду:

```
%SystemRoot%\System32\dnsmgmt.msc /a
```

Добавление/удаление оснастки производится при помощи команды Консоль ▸ Добавить/удалить оснастку. Изменения вступают в силу после следующего запуска консоли.

Заранее настроенные консоли управления от фирмы Microsoft находятся в папке \systemroot\System32. Любую консоль можно открыть, выполнив двойной щелчок мыши на соответствующем файле.

Оснастки консоли MMC

Инструменты, реализующие выполнение административных задач в составе интегрированного интерфейса, называются *оснастками*. Например, оснастка DNS применяется для управления DNS-сервером.

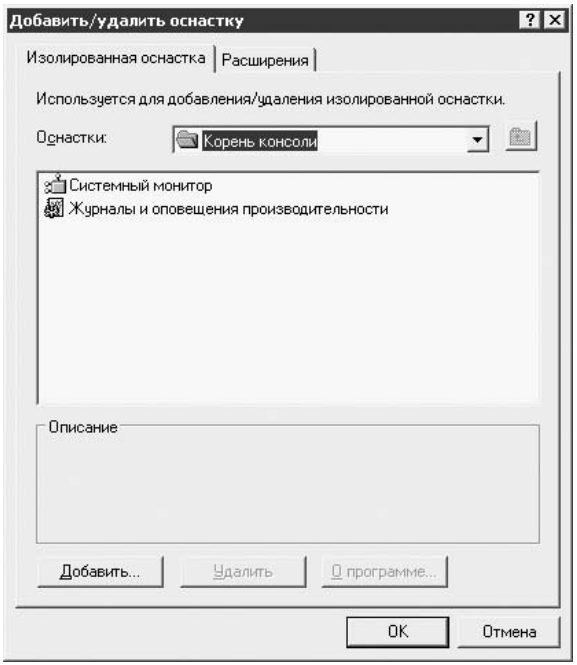


Рис. 7.3. Окно добавления изолированной оснастки

Сами оснастки делятся на две категории: *изолированные* и *расширения*. Изолированные оснастки выполняются сами по себе, а расширения связаны с какой-либо другой оснасткой.

Добавление оснасток производится в авторском режиме консоли MMC. Достаточно выбрать команду Добавить/Удалить оснастку, а затем в окне Добавить/Удалить оснастку нажать кнопку Добавить, после чего будет отображено окно Добавить изолированную оснастку, в котором перечислены все типы доступных оснасток (рис. 7.3).

Панель управления

Панель управления играет роль некоего пульта управления, обеспечивающего настройку аппаратного обеспечения. Чтобы открыть окно панели управления, нужно выполнить команду Пуск ▸ Настройка ▸ Панель управления. После этого на экране отобразится окно с многочисленными значками оснасток (рис. 7.4 и 7.5).

Как видите, между панелями управления Windows 2000 и Windows XP имеется много общего.

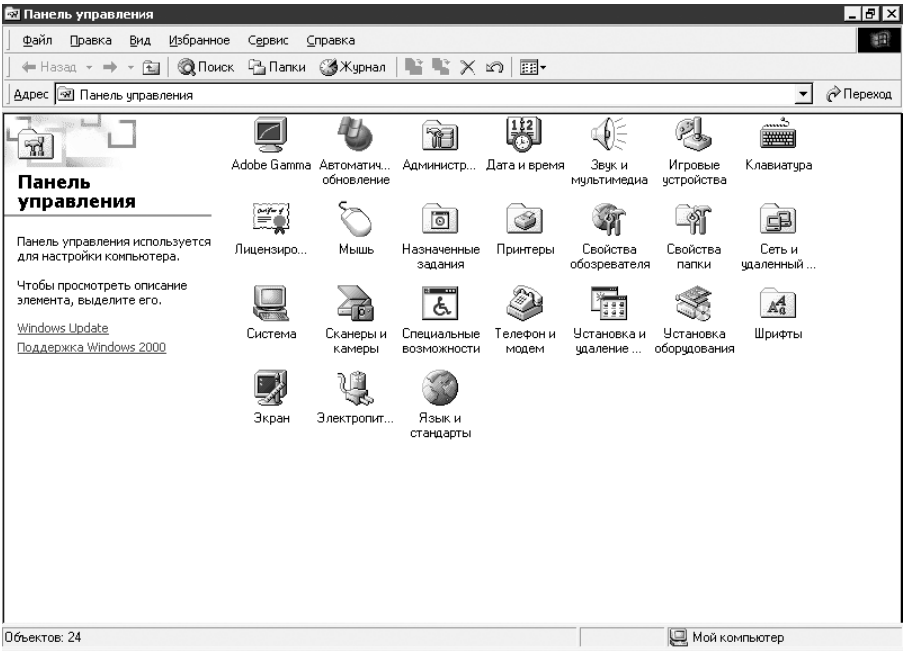


Рис. 7.4. Панель управления Windows 2000

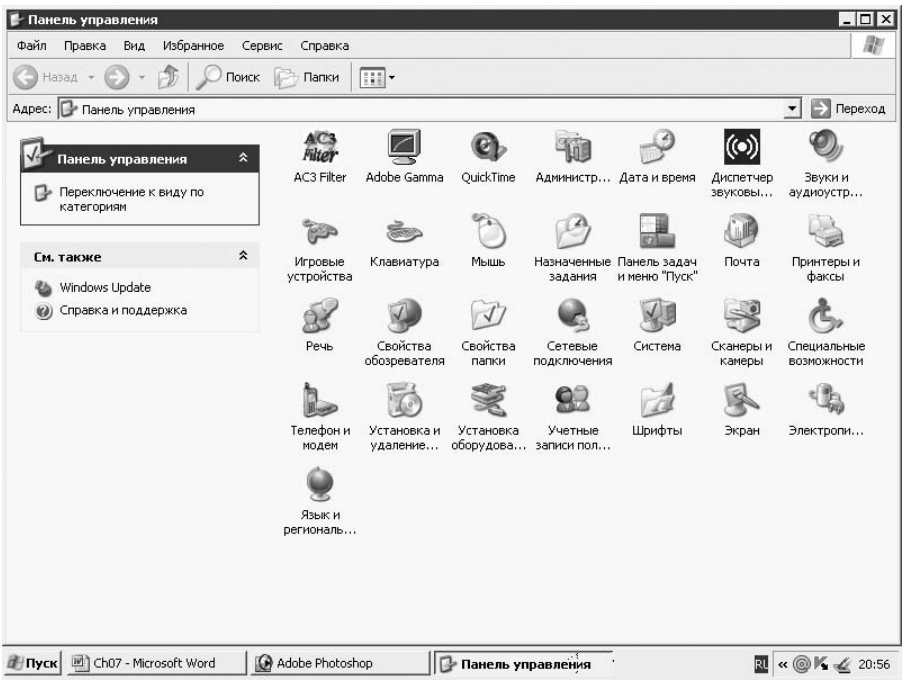


Рис. 7.5. Панель управления Windows XP

Установка оборудования

После щелчка на значке Установка оборудования запускается мастер установки и удаления оборудования. Эта программа позволяет установить новое устройство, подключить и отключить существующее устройство, а также устранить некоторые неполадки для установленного в системе оборудования. Рабочее окно мастера показано на рис. 7.6.

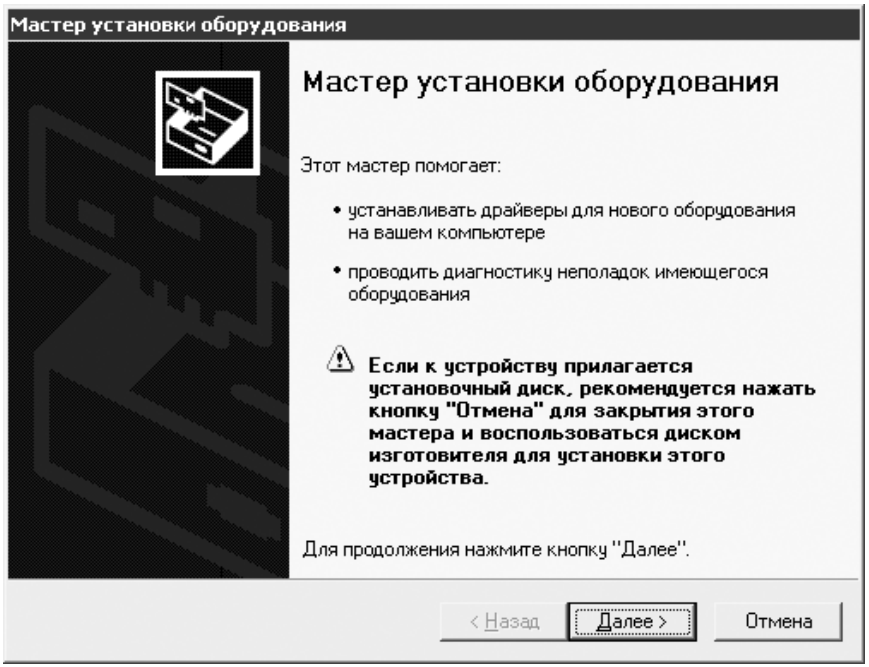


Рис. 7.6. Мастер установки оборудования

Установка и удаление программ

Апплет Установка и удаление программ позволяет изменять установку существующих программ или удалять их, добавлять или удалять компоненты Windows 2000 Server (Windows XP). Рабочее окно этого апплета показано на рис. 7.7.

Администрирование

Папка Администрирование включает в себя различные инструменты администрирования, в том числе и оснастки консоли MMC, реализующие функции по управлению компьютером и сервером (рис. 7.8).

Теперь после завершения рассмотрения основных инструментов, используемых для управления и настройки сетей Microsoft, остановимся на рассмотрении службы каталогов Active Directory.

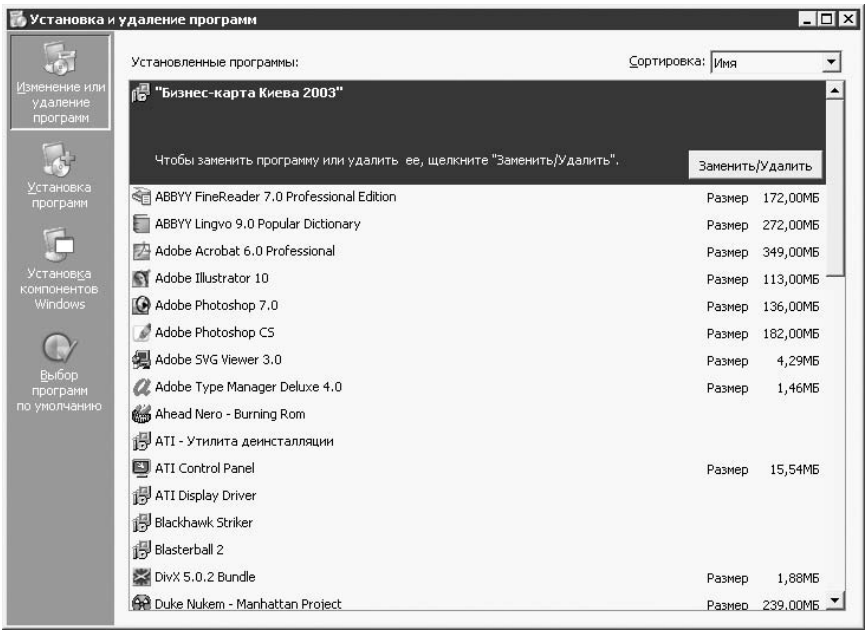


Рис. 7.7. Это приложение позволит установить или удалить программу

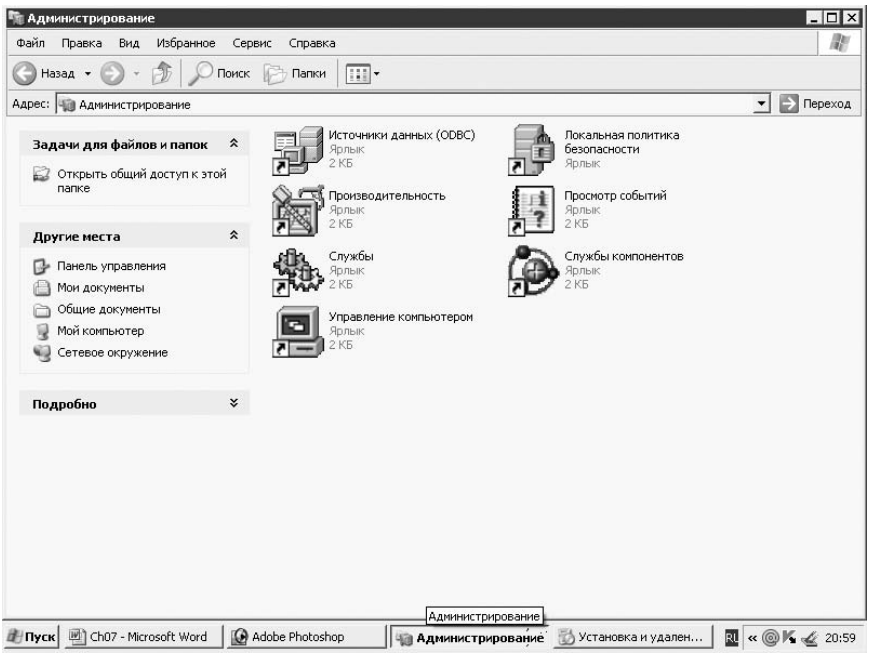


Рис. 7.8. Используя инструментальные средства, можно эффективно управлять сетевым компьютером и учетными записями пользователей

Служба каталогов Active Directory

Служба каталогов *Active Directory* обеспечивает функционирование универсального распределенного хранилища данных, доступ к объектам которого возможен из любой точки локальной сети и даже из Интернета.

Для службы каталогов Active Directory использовался ряд открытых международных стандартов, с помощью которых удалось создать нечто вроде всеобъемлющей иерархической базы данных, поддерживающей самые разнообразные объекты. При этом использовались спецификации, определенные в стандарте X.500 и протоколом LDAP.

Стандарт *X.500* использовал стандарты и интерфейсы, определяющие глобальную и распределенную службы каталогов. В основе всей структуры находится база данных каталогов (DIB, Directory Information Base). Эта база данных наполнена сведениями об объектах, хранящихся в каталогах.

Получение доступа к базе данных DIB, а также к пользователям и их компьютерам, осуществляется при помощи объектно-ориентированной иерархической структуры (рис. 7.9).

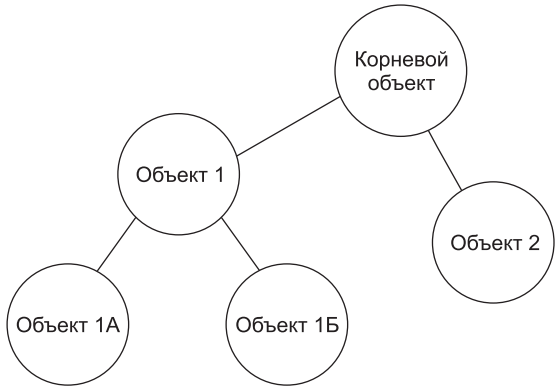


Рис. 7.9. Иерархическая структура, определяемая стандартом X.500

Еще одним предком службы каталогов Active Directory является протокол LDAP (Lightweight Directory Access, облегченный протокол доступа к каталогам). Этот протокол содержит целый ряд полезных функций, присущих любой службе каталогов. Одним из самых полезных свойств этого протокола является поддержка гиперпоиска. Это означает, что возможна установка ссылки с одного каталога на другой в процессе поиска необходимой информации. Яркий пример реализации на практике этого свойства — поиск в Интернете, основанный на системе гиперсвязей.

Далее перечислены компоненты протокола LDAP, которые в той или иной степени заложены в основу многих современных служб каталогов, включая также Active Directory.

- Модель данных. Именно модель данных, определяющая способ доступа к данным, которые хранятся в каталогах, определяется спецификацией X.500.

В этом случае данные добавляются к объектам путем определения их атрибутов. Каждый атрибут может содержать одно или несколько значений. Все объекты объединяются в группы классов, например организационные единицы (OU, organization unit).

- Организационная модель. Эта модель представляет собой «перевернутую» древовидную структуру, которая также берет свое начало в спецификации X.500. Подобная структура поддерживается большинством современных служб каталогов.
- Модель безопасности. Данная модель определяет способ осуществления безопасного и надежного доступа к информации. Протокол LDAP обеспечивает идентификацию пользователей с помощью *протокола Kerberos*. При этом реализуются несколько уровней проверки идентичности, а также *защищенный уровень простой проверки идентичности* (SASL, Secure Authentication Secure Level). Протокол LDAP 3.0 обеспечивает поддержку протокола безопасных сокетов (SSL, Secure Socket Level), входящего в стек протоколов TCP/IP.
- Функциональная модель. Эта модель определяет методы запросов и модификации объектов каталогов. Сюда включены операции добавления элементов, редактирования и распространения полей атрибутов, а также действия по удалению и запросу объектов каталога.
- Технологическая модель. Данная модель определяет методики интеграции и взаимодействия службы каталогов с другими совместимыми службами. Способность образования гиперсвязей, присущая протоколу LDAP, проистекает именно из этой модели.

Протокол LDAP поддерживается подавляющим большинством приложений и серверных технологий, особенно приложениями Интернета.

Итак, служба каталогов Active Directory позаимствовала лучшие характеристики, присущие протоколу LDAP, а также определяемые спецификацией X.500. Поэтому служба каталогов Active Directory может выполнять обмен данными с любой другой службой, поддерживающей протокол LDAP, а таких служб очень много.

Ниже приводятся некоторые основные признаки, характеризующие службу каталогов Active Directory:

- вмонтирована в операционную систему Windows NT, которая является предшественницей Windows 2000. Это позволяет обеспечивать обратную совместимость;
- представляет собой подлинно распределенную архитектуру, благодаря чему администратор может распространять изменения по всей сети независимо от начальной точки;
- обеспечивает высокую степень масштабирования и саморепликации. Изначально реализованная на одном компьютере система может получить распространение на всю локальную сеть (или объединение сетей). В ближайшее время, вероятно, служба будет широко распространена благодаря простоте доступа к ресурсам.
- дает возможность расширения структурной модели службы каталогов Active Directory, что позволяет развивать ее схему без малейших ограничений. Для расширения схемы достаточно зарегистрировать идентификатор объекта (OID, Object Identifier).

Схемы именования

На основе службы каталогов Active Directory реализуется несколько схем именования, которые будут рассмотрены чуть позже.

Соглашения о наименовании, принятые в стандартах LDAP и X.500, называются *схемой именования с атрибутами*. В данном случае имя состоит из названия сервера, на котором размещается каталог, имени пользователя, имени подразделения и т. д.

Например, подобное имя может иметь следующий формат:

```
LDAP://my_server.my.com/cn=epson, ou=autosales,
dc=smallcom, dc=com
```

Логическая структура домена

При использовании службы каталогов Active Directory применяется корневая иерархическая структура, в которой допускается существование единственного *родительского домена*. С этим доменом связаны *дочерние домены*. Например, у воображаемой компании WIM может быть корневой домен wim.com. Поддомен или дочерний домен, выделенный для бухгалтерии, может называться accounting.wim.com. При этом следует обращать внимание на то обстоятельство, что в качестве имени корневого домена организации не может указываться .com, поскольку это имя зарегистрировано комитетом InterNIC для выдачи ведущим коммерческим организациям. Поскольку в данном случае осуществляется работа с Active Directory, все компоненты, образующие домен, являются объектами. А точнее, объектами-контейнерами, атрибуты имен которых легко управляемы. Однозначная идентификация в службе каталогов Active Directory производится с помощью так называемых *глобально уникальных идентификаторов* (GUID). Поэтому корневой домен является корневым объектом-контейнером, который, в свою очередь, может содержать другие объекты. Пример логической структуры домена приводится на рис. 7.10.

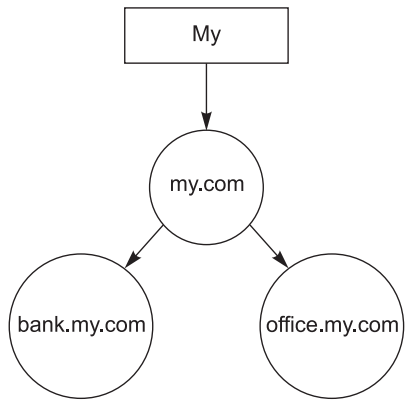


Рис. 7.10. Пример логической структуры домена

Организационные единицы

Классы объектов содержатся в одном из основных объектов-контейнеров, называемых *организационными единицами* (OU, Organization Unit). Подразделения могут включать в себя такие объекты, как учетные записи пользователей, принтеры, компьютеры, общие ресурсы, а также другие подразделения.

Деревья

Рассмотренная в предыдущих разделах доменная структура представляется в виде так называемых *деревьев доменов*. Все объекты, которые расположены от объекта до корневого домена, образуют дерево домена. Дерево является уникальным в службе каталогов Active Directory, поскольку существование нескольких одинаковых родительских доменов просто невозможно.

Вообще говоря, дерево домена — это некий систематический набор объектов домена в структуре службы каталогов Active Directory, который относится к одному непрерывному пространству имен. Следует иметь в виду, что корневой домен может расширяться или разделяться с образованием нескольких поддоменов. Имена поддоменов уникальны, поскольку все они совместно используют стандартную схему каталогов, которая включает формальное определение для всех объектов в дереве домена.

В службе каталогов Active Directory применяются соглашения о назначении имен DNS в случае присвоения имен иерархической структуре доменов и соответствующим устройствам. Поэтому домены и устройства Active Directory следует уникальным образом идентифицировать в Active Directory и системе имен DNS.

Леса доменов

Можно создать еще один родительский домен в Active Directory, затем создавать в нем объекты, которые полностью идентичны объектам из соседних доменов. В этом случае создаются наборы деревьев домена, которые именуются *лесом*. В службе каталогов Active Directory одно дерево домена рассматривается как лес, который состоит всего лишь из одного дерева. Между деревьями могут устанавливаться доверительные отношения, которые обеспечивают пользователям одного дерева леса получение доступа к ресурсам другого дерева.

Доверительные отношения

Взаимодействие между доменами Windows 2000 организуется при помощи установления между ними *доверительных отношений*. На рис. 7.11 показана схема установления доверительных отношений между тремя доменами, подчиняющихся закону транзитивности. Благодаря заранее установленным доверительным отношениям исключается необходимость повторных проверок взаимодействующих доменов при установлении каждого сеанса связи.

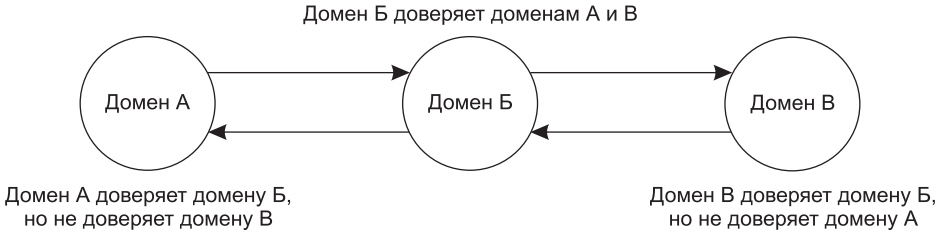


Рис. 7.11. Доверительные отношения, установленные между тремя доменами

Установка службы каталогов Active Directory

Если служба каталогов Active Directory не была установлена во время инсталляции Windows 2000 Server, ее можно установить и позже. Для этого нужно перейти в панель управления (команда Пуск ▸ Настройка ▸ Панель управления) и выбрать апплет Настройка сервера. После этого на экране отобразится диалоговое окно Настройка сервера Windows 2000 (рис. 7.12).

ВНИМАНИЕ Служба каталогов Active Directory может устанавливаться только в томе NTFS, поэтому в локальной системе должен присутствовать хотя бы один том, на котором установлена эта файловая система.

Рис. 7.12. Окно настройки параметров Windows 2000 Server

После завершения необходимых подготовительных действий выберите вкладку Active Directory и щелкните на вкладке Запустить мастер установки Active Directory. На экране будет отображено окно мастера установки службы каталогов Active Directory (рис. 7.13).

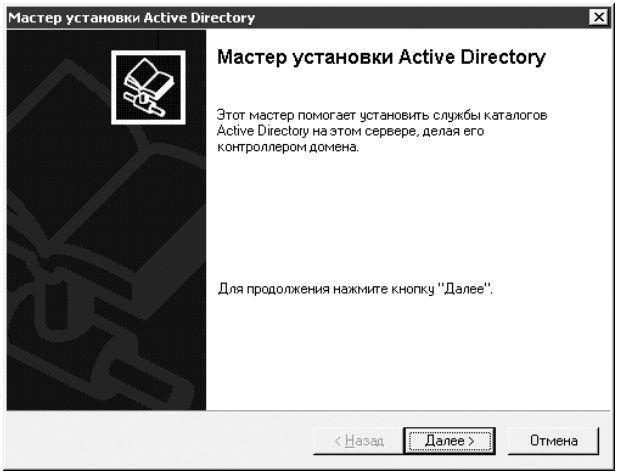


Рис. 7.13. Окно мастера установки службы каталогов Active Directory в Windows 2000

1. Находясь в окне мастера, нужно нажать кнопку Далее. После этого будет отображено диалоговое окно Тип контроллера домена (рис. 7.14), в котором следует выбрать роль, исполняемую данным сервером (контроллер домена в новом домене или дополнительный контроллер домена в существующем домене).

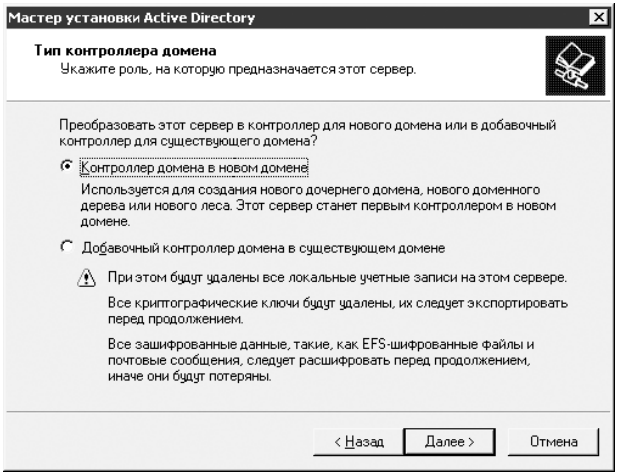


Рис. 7.14. Выбор типа контроллера домена

ВНИМАНИЕ Обратите внимание на то, что в процессе установки контроллера домена будут утеряны все локальные учетные записи, хранящиеся на данном компьютере. Помимо этого будут утеряны все зашифрованные данные (если применяется файловая система EFS), а также все ключи шифрования. Во избежание возможных потерь следует предварительно экспортировать все ключи шифрования, а также дешифровать все ранее зашифрованные файлы.

2. В этом диалоговом окне выберите создание нового доменного дерева или дочернего домена в существующем доменном дереве (рис. 7.15). Затем нужно нажать кнопку Далее.

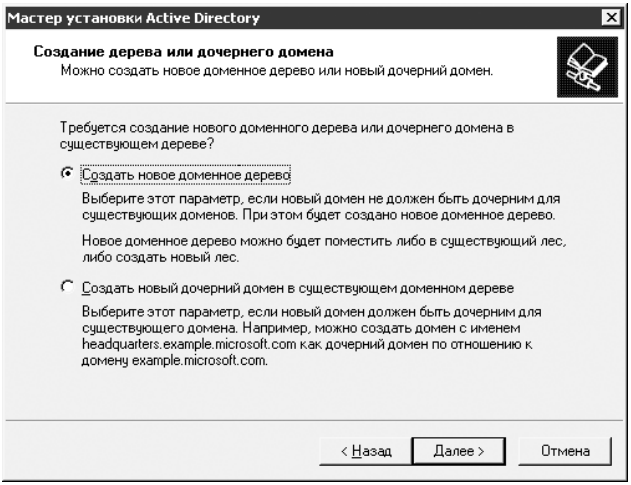


Рис. 7.15. Осуществите выбор между созданием нового доменного дерева или дочернего домена

3. Теперь следует выбрать создание нового леса доменов или присоединение к уже существующему ранее лесу (рис. 7.16). Установите соответствующий переключатель и нажмите кнопку Далее.

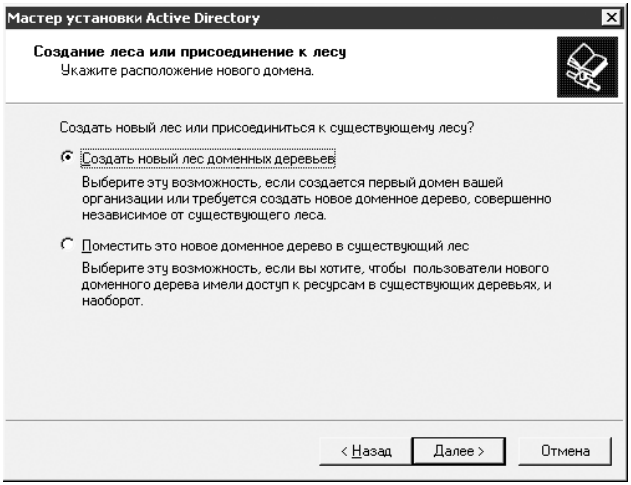


Рис. 7.16. А теперь можно указать создание нового леса из доменов или присоединение к ранее созданному лесу

4. В следующем диалоговом окне следует ввести DNS-имя домена (рис. 7.17). При этом следует руководствоваться правилами создания иерархических доменных имен (например, my_server.com). Затем нажмите кнопку Далее.

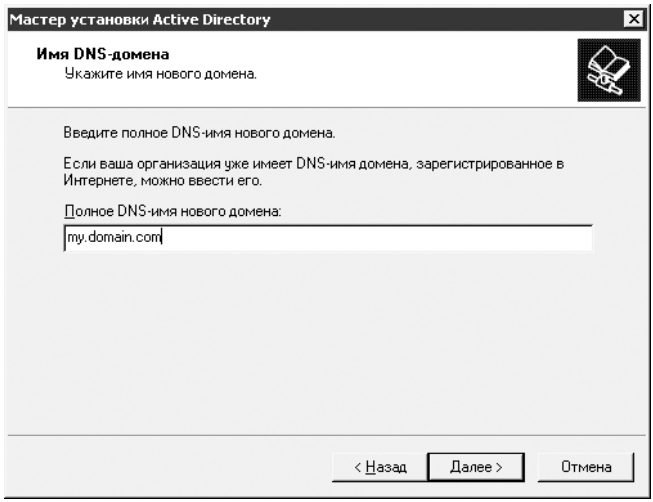


Рис. 7.17. Ввод DNS-имени в соответствии с правилами именования

5. В следующем диалоговом окне (рис. 7.18) пользователю предлагается указать имя NetBIOS домена, распознаваемое внутри локальной сети. После ввода соответствующего имени нажмите кнопку Далее.

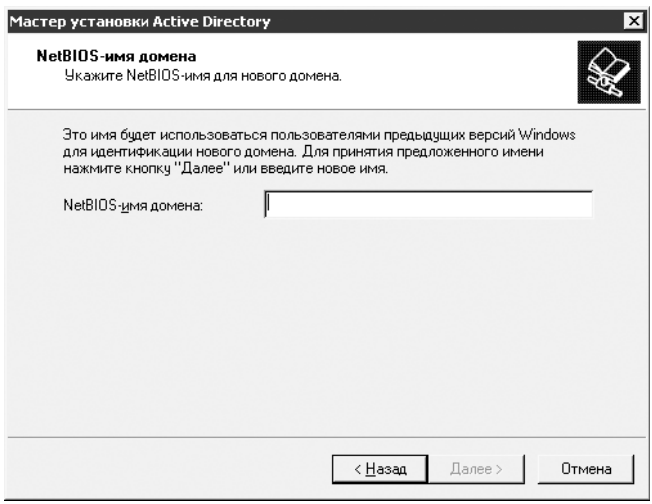


Рис. 7.18. Имя NetBIOS для домена

6. В следующем диалоговом окне (рис. 7.19) нужно указать расположение базы данных и журнала службы каталогов Active Directory. Для увеличения быстродействия системы в целом эти компоненты следует размещать на различных дисках (или хотя бы в различных разделах одного диска). Затем нажмите кнопку Далее.

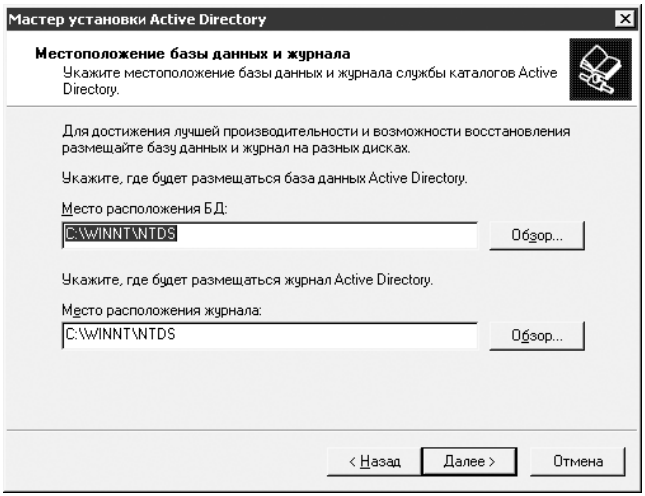


Рис. 7.19. База данных и журнал службы каталогов Active Directory

7. В следующем диалоговом окне (рис. 7.20) укажите местоположение папки Sysvol, в которой находится серверная копия общих файлов домена. Содержимое этой папки реплицируется на все контроллеры домена. После того как было выбрано местоположение для папки, нажмите кнопку Далее.

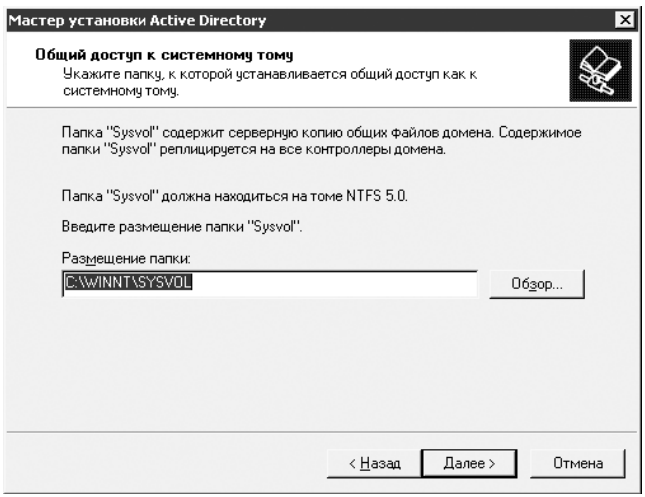


Рис. 7.20. Здесь находятся общие файлы, входящие в состав домена

8. В следующем диалоговом окне (рис. 7.21) выбираются разрешения, заданные по умолчанию, для объектов, которые являются пользователями или группами. Здесь можно выбрать разрешения, поддерживаемые серверами, предшествующими Windows 2000. Эта возможность полезна в том случае, если имеются серверные программы, которые выполняются на серверах, предшествую-

щих Windows 2000. Если же такие программы отсутствуют, лучше выбрать опцию установки разрешений, совместимых исключительно с серверами Windows 2000 — в этом случае значительно повышается уровень безопасности локальной сети в целом. Затем нажмите кнопку Далее.

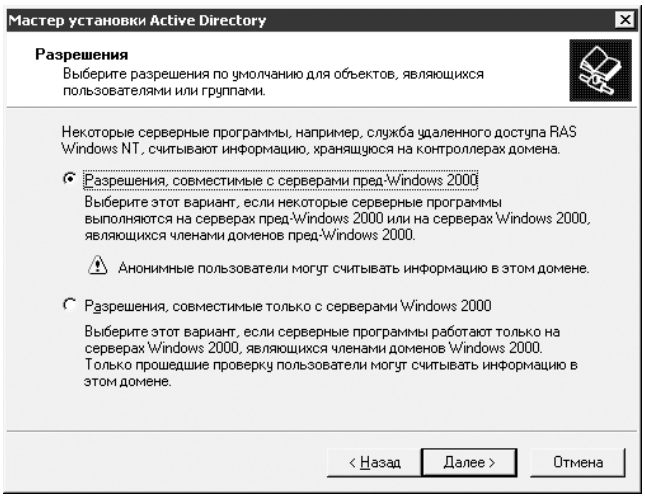


Рис. 7.21. Указание совместимости для разрешений

9. В следующем диалоговом окне (рис. 7.22) указывается пароль администратора данного сервера, который будет использоваться при запуске компьютера в режиме восстановления службы каталогов Active Directory. Обратите внимание на тот факт, что этот пароль не совпадает с паролем учетной записи администратора. Нажмите кнопку Далее.

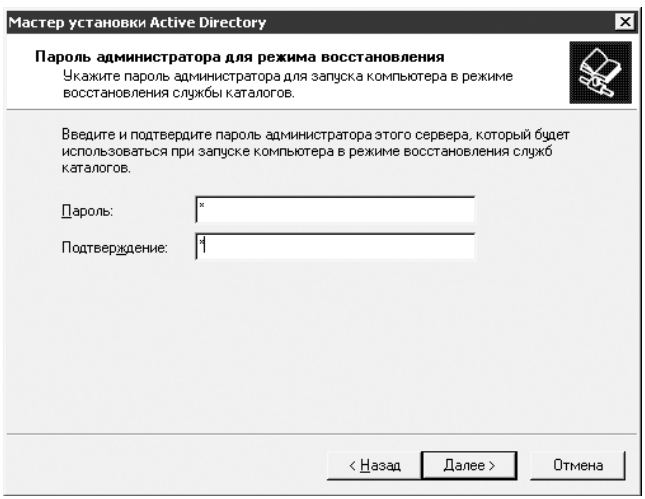


Рис. 7.22. Пароль администратора, применяемый в режиме восстановления для службы каталогов Active Directory

10. В этом диалоговом окне отображается итоговая информация (рис. 7.23), соответствующая выбранным ранее параметрам. На этой стадии еще не поздно все изменить. Если же вас все устраивает, нажмите кнопку Далее.

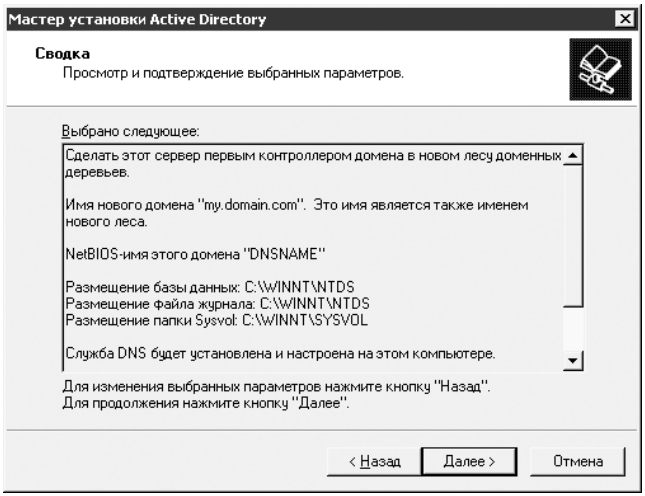


Рис. 7.23. Итоговые сведения, соответствующие введенным пользователем данным

11. Теперь запускается процесс установки службы каталогов Active Directory. Если при этом не произойдут какие-либо сбои, после перезагрузки компьютера служба каталогов будет активизирована. Обратите внимание на то, что корректная установка Active Directory возможна только в том случае, если предварительно был установлен и правильно настроен DNS-сервер.

Управление учетными записями

Все пользователи, которые периодически подключаются к локальной сети, считаются *локальными пользователями*. В данном контексте допускается двоякая трактовка термина «локальный». В частности, пользователи могут быть локальными по отношению к компьютеру или рабочей станции, к которым они подключаются локальным образом. Также можно рассматривать локальных пользователей домена в отличие от удаленных пользователей, работающих со службами удаленного доступа.

Совокупность пользователей (а также других объектов) образует *группу*. Служба каталогов Active Directory способна поддерживать группы в качестве управляемого объекта.

Каждому пользователю сети Windows 2000 Server (а также Windows XP) соответствует *учетная запись*. В локальной сети все действия производятся именно по отношению к учетным записям, а не к пользователям, выступающим в качестве автономных объектов. Все учетные записи делятся на две большие категории: *доменные* и *локальные*.

После завершения установки сетевой ОС Windows 2000 Server создаются несколько доменных и локальных учетных записей. Если же устанавливается служба каталогов Active Directory, локальные учетные записи попросту отключаются и остаются только доменные учетные записи. Конечно, следует подробнее рассмотреть различные типы учетных записей.

Доменные учетные записи хранятся в базе данных Active Directory и доступны в любом месте локальной сети. Этот тип учетных записей применяется для регистрации в сети, и они могут создаваться пользователями, обладающими соответствующими правами доступа. Непосредственно после создания доменные учетные записи становятся доступными во всей локальной сети.

Локальные учетные записи связаны с одним компьютером или рабочей станцией и хранятся локально, то есть не в базе данных Active Directory, а в локальной базе данных SAM. В связи с этим локальные учетные записи носят ограниченный характер и могут предоставлять доступ только к ресурсам конкретного локального компьютера.

Встроенные учетные записи

После установки Windows 2000 Server на автономном сервере или на контроллере домена, который совместим со службой каталогов Active Directory, создаются несколько *встроенных учетных записей*.

Если операционная система устанавливается на автономном сервере или рабочей станции, то стандартные учетные записи являются локальными по отношению к домену, в состав которого входит данный компьютер, и относятся к локальной базе данных SAM.

Если же установка ОС производилась на сервере, который играет роль контроллера домена, то создаются доменные учетные записи, которые носят универсальный характер и доступны во всей локальной сети.

Непосредственно после установки системы по умолчанию создается два типа встроенных учетных записей: *администратора* и *гостя*. Причем это справедливо как для Windows 2000 Server, так и для Windows XP.

Учетная запись администратора находится в локальной базе данных SAM, а также в глобальной базе данных Active Directory. Именно эта учетная запись часто становится объектом преступных посягательств со стороны разного рода хакеров. Если пароль этой учетной записи станет известным посторонним лицам, а такие случаи неоднократно происходили на практике, под угрозой будет само существование локальной сети.

Каким же образом можно защитить эту важнейшую учетную запись от преступных посягательств? Первый и наиболее простой способ заключается в переименовании учетной записи, благодаря чему потенциальный взломщик сети будет должен сначала отыскать ту самую учетную запись, которая предоставит ему права доступа администратора. Следует внимательно отнестись к выбору пароля для этой учетной записи. Нельзя использовать слишком простые пароли, а также слова, которые могут стать легкой добычей хакеров, взламывающих сеть методом *атаки со словарем*. Можно также создать фиктивную учетную запись,

назвать ее «Администратор», а затем предоставить ей гостевые права доступа. Злоумышленник потратит массу времени на взлом пароля именно этой учетной записи, а результат будет практически нулевым. Можно просто прекратить пользоваться учетной записью администратора, заблокировав ее пароль. Вряд ли эта учетная запись понадобится после того, как была завершена настройка сети.

ПРИМЕЧАНИЕ Подробное рассмотрение вопросов обеспечения безопасности сети будет проведено в десятой главе.

Гостевая учетная запись создается по умолчанию после завершения установки Windows 2000 Server (Windows XP) или после создания контроллера домена и установки службы каталогов Active Directory. Эта учетная запись не требует ввода пароля, а ее владельцу можно предоставить права доступа к тем или иным ресурсам компьютера. Иногда может создаваться впечатление, что эта учетная запись не очень-то и нужна. Каждому постоянному пользователю соответствует своя учетная запись, а всякого рода посетители лишь негативно влияют на безопасность всей системы в целом. Ниже приведены некоторые аргументы в пользу сохранения гостевых учетных записей.

1. Благодаря гостевой учетной записи принятый на работу сотрудник фирмы может приступать к работе, не дожидаясь выделения собственной учетной записи.
2. Если многие сорудники фирмы не входят в штат, наличие гостевой учетной записи приводит к существенному росту безопасности системы в целом.
3. Если учетная запись пользователя сети в силу каких-либо причин заблокирована, при наличии гостевой учетной записи у него остается возможность регистрации в домене, а также получения доступа (как правило, только в режиме чтения) к внутренней локальной сети компании.

Идентификаторы безопасности

Процесс идентификации учетной записи пользователя подсистемой безопасности производится с помощью так называемого *идентификатора безопасности* (SID, security identifier). Благодаря этому обеспечивается уникальность учетной записи, а также всех связанных с ней прав доступа и разрешений. Поэтому при удалении учетной записи и последующем ее восстановлении пропадут все связанные с ней права доступа и разрешения.

Идентификатор безопасности, хранящийся в базе данных, создается непосредственно после формирования учетной записи. Сам объект идентификатора делится на два раздела. Первый раздел определяет домен, а второй задает учетную запись внутри этого домена и называется *относительным идентификатором* (RID, Relative Identifier).

Если пользователь регистрируется в домене или на компьютере, то происходит поиск в базе данных идентификатора SID, а также добавляется маркер, соответствующий данному пользователю. Маркер доступа используется для идентификации пользователя в процессе выполнения любых действий, связанных с безопасностью системы.

Идентификаторы SID также применяются для идентификации владельца объекта, соответствующей ему группы, а также пользовательской учетной записи в случае обращения к определенным ресурсам системы.

Групповые учетные записи

Благодаря наличию групп пользователей возможно одновременное назначение прав доступа всем пользователям, которые нуждаются именно в этих правах доступа.

Группы Windows 2000 делятся на категории *безопасности* и *распределения*. Группа безопасности является стандартным участником политики безопасности Windows 2000, а также элементом *списка контроля доступа* (ACL). Возможна централизованная рассылка электронных сообщений всем членам группы безопасности, для которых выделен единый адрес электронной почты.

Группа распределения не является участником политики безопасности Windows 2000, а ее применение ограничивается списком распределения. В этой группе можно сохранять сведения, имеющие отношение к контактам и учетным записям пользователей.

Группы также имеют различные представления. В частности, группы бывают универсальными, глобальными и локальными.

Универсальные группы могут включать в себя любые домены Windows 2000, имеющие отношение к рассматриваемому лесу доменов. В качестве членов этой группы могут также выступать элементы любого другого представления. Группы этого типа могут создаваться для всех пользователей, которые нуждаются в предоставлении доступа к ресурсам, находящимся в других доменах. Члены универсальной группы могут получать права доступа к произвольным ресурсам в любом домене.

Глобальные группы включают в себя только ресурсы исходного домена. Сюда же могут входить и другие глобальные группы, а также группы контактов. Члены глобальных групп получают доступ к ресурсам из любого домена в лесу. Они могут относиться к любой группе из рассматриваемого леса доменов. Глобальные группы могут включать в себя другие глобальные, универсальные и локальные группы.

Локальные группы домена могут иметь отношение к любому домену леса. В группу подобного рода могут включаться пользователи и локальные группы, имеющие отношение к этому же домену. Члены локальной группы не могут входить в глобальные и универсальные группы.

Ниже описан набор свойств, присущих группам:

- группы представляют собой набор пользовательских учетных записей;
- пользователи или члены групп наследуют все права доступа, определенные для той или иной группы;
- пользователи могут быть членами нескольких групп;
- группы могут включаться в состав подразделений, которые, в свою очередь, могут быть элементами других подразделений.

Встроенные группы

В процессе установки Windows 2000 Server (Windows XP) создается несколько встроенных групп, хотя некоторые из них можно создавать только в ручном режиме. Так, например, группа администраторов домена не будет создана до тех пор, пока не будет сформирована первая учетная запись компьютера.

Далее перечислены встроенные группы, автоматически создаваемые в процессе установки Windows 2000 Server.

- Администраторы (Administrators). В процессе установки операционной системы в эту группу автоматически помещается одна учетная запись администратора, который обладает наивысшим уровнем приоритета. В эту группу можно добавлять учетные записи других пользователей, которые получат расширенный набор прав доступа. Интересно отметить тот факт, что администраторы, несмотря на весь присущий им набор полномочий, не могут получить доступ к файлам и папкам тех пользователей, которые наложили соответствующие ограничения. Это позволяет обеспечивать полноценную защиту сетевых ресурсов.
- Пользователи (Users). К этой группе по умолчанию относятся все пользовательские учетные записи, созданные в Windows 2000 (Users). Следует отличать эту группу от папки Users, в которой помещаются анонимные и гостевые учетные записи.
- Опытные пользователи (Power Users). Члены этой группы обладают теми же правами, что и члены группы Users, а также некоторыми дополнительными административными привилегиями.
- Операторы учетных записей (Account Operators). Члены этой группы обладают расширенным набором административных прав доступа. Операторы имеют право создавать учетные записи пользователей и групп, они также могут изменять и удалять эти записи в рамках всего домена. Операторы учетных записей могут регистрироваться на серверах, отключать их, а также добавлять компьютеры в состав доменов. Операторы учетных записей не могут удалять локальные группы администраторов, администраторов домена, операторов архива, операторов печати, операторов сервера, а также любые другие группы, входящие в состав перечисленных выше групп. Они также не могут модифицировать свойства учетных записей членов групп более высокого уровня.
- Операторы архива (Backup Operators). Члены этой группы могут создавать резервные копии системы, а также восстанавливать ранее зарезервированные данные. При этом они могут пользоваться только специальными программами резервного копирования. Операторы архива также могут регистрироваться в системе на контроллерах доменов и резервных серверах.
- Операторы печати (Print Operators). Члены этой группы могут создавать, удалять и управлять общими точками печати, которые расположены на серверах печати. В область их компетенции также входит отключение серверов печати.
- Операторы сервера (Server Operators). Члены этой группы могут управлять различными серверами.

- Репликатор (Replicator). Эта группа содержит пользовательскую учетную запись, применяемую для обеспечения доступа к службе репликации.
- Гости (Guests). Эта группа содержит учетные записи пользователей-гостей или тех пользователей, которые не располагают учетными записями в домене. Как правило, члены этой группы могут регистрироваться без паролей, причем допускается выполнение весьма ограниченного набора действий.

ВНИМАНИЕ В среде Windows XP создаются присущие только ей встренные группы Пользователи удаленного рабочего стола и HelpServicesGroup (Группа технической поддержки).

Следует обратить особое внимание на глобальные группы, которые автоматически включаются в состав локальных групп.

- Администраторы домена. Эта группа предоставляет пользователям административные права, без которых нельзя управлять контроллерами доменов, непосредственно доменами, рядовыми серверами и рабочими станциями. Если эта группа будет удалена из группы администраторов рядового сервера, то доступ к любому рядовому серверу будет заблокирован. Данная группа в силу своей глобальной природы может входить в состав любой локальной группы, имеющей отношение к произвольному домену, а также может быть добавлена в состав универсальных групп.
- Пользователи домена. В состав данной группы включаются все пользователи домена независимо от их принадлежности к другим группам. Эту группу можно также включить в состав локальной группы Users.

Также существуют фиксированные группы, которые создаются после завершения установки операционной системы Windows 2000 Server. Эти группы нельзя изменять, удалять или деактивировать.

- Все (All). К этой группе можно отнести всех пользователей компьютера и сети в целом. Вообще говоря, если данная группа будет включена в состав какой-либо локальной группы, то ресурсы, предоставленные в распоряжение пользователей этой локальной группы, будут выставлены на всеобщее обозрение. Этот момент представляет определенную опасность, поэтому следует учитывать это обстоятельство в своих дальнейших действиях.
- Интерактивные (Interactive). В состав этой группы включаются все пользователи, которые работают на данном компьютере.
- Сеть (Network). К этой группе можно отнести всех пользователей, которые подключаются к данному компьютеру через сеть.
- Система (System). Членами этой группы являются специализированные группы, учетные записи и ресурсы, требуемые для обеспечения нормального функционирования операционной системы.
- Создатель-владелец (Creator-Owner). В состав этой группы входят владельцы или создатели папок, файлов и заданий печати.

Пример создания группы в среде Windows 2000 Server

В этом разделе будет рассмотрен пример создания группы в среде Windows 2000 Server.

Прежде всего, необходимо запустить оснастку ActiveDirectory – пользователи и компьютеры. Затем нужно выбрать подразделение, в котором будет создана новая группа, и выполнить команду Действие ▸ Создать ▸ Group. После этого отобразится диалоговое окно Новый объект — Group (рис. 7.24), в котором определяются необходимые параметры, перечисленные в списке.

- Имя новой группы. Здесь указывается уникальное имя, присваиваемое данной группе.
- Имя новой группы, относящееся к нижнему уровню. Это имя добавляется в автоматическом режиме после определения имени новой группы.
- Представление группы. В данном случае можно обозначить группу как локальную в домене, глобальную или универсальную.
- Тип группы. Здесь группу можно объявить как группу безопасности или группу распространения. Не следует забывать о том, что в случае выбора группы безопасности затрудняется применение универсальных групп с недостаточно жесткими параметрами безопасности, если домен функционирует в смешанном режиме.

Рис. 7.24. В этом диалоговом окне создается новая группа

Указав тип группы, достаточно нажать кнопку OK, после чего создание группы будет завершено.

Для ранее созданной группы можно определять различные свойства, задающие общие параметры, а также членство указанной группы в других группах.

Пример создания группы в среде Windows XP

Методика создания группы в среде Windows XP не слишком сильно отличается от рассмотренной ранее процедуры для Windows 2000 Server.

1. Выполнить команду Пуск ▸ Панель управления. На экране будет отображена панель управления Windows XP.
2. В панели управления перейти в раздел Администрирование, после чего щелкнуть мышью на значке Управление компьютером.
3. Щелчком на знаке плюса нужно раскрыть ветвь Локальные пользователи и группы, после чего потребуется перейти в правую панель и в контекстном меню выполнить команду Создать группу.
4. В диалоговом окне Новая группа ввести информацию в поля Имя группы, Описание, Члены группы (рис. 7.25).
5. Нажать кнопку Создать, после чего новая группа будет сохранена.

Рис. 7.25. В этом диалоговом окне определяются параметры новой группы

Свойства ранее созданных групп могут изменяться. Для этого достаточно выделить требуемую группу, а затем в контекстном меню выбрать пункт Свойства.

Управление пользователями и группами

Подсистема безопасности контролирует доступ к локальной сети, а также обеспечивает защиту сетевых и вычислительных ресурсов с помощью двух методов — права и системы разрешений.

Права предоставляются отдельным пользователям или группам пользователей. В качестве пользователей могут выступать не только люди, но и отдельные процессы, управляющие памятью или задействующие время центрального процессора.

Разрешения применются в тех случаях, когда доступ к определенному объекту строго регламентируется. Разрешения могут предоставляться файловой системой или службой каталогов Active Directory.

Права делятся на две больших категории: *привилегии* и *права доступа*. Если права предоставляются отдельным пользователям и группам для выполнения заранее определенных операций в вычислительной среде, то они получают название привилегий. При этом следует иметь в виду, что приоритет привилегий будет выше, чем приоритет разрешений. В качестве примера можно рассмотреть право на архивирование файлов и каталогов, которое обладает более высоким приоритетом по сравнению с любым разрешением, запрещающим доступ.

С помощью *прав регистрации* устанавливается порядок регистрации пользователя в системе. Права регистрации также могут определяться при помощи групповой политики, о которой подробнее будет сказано в следующем разделе. Эти права устанавливаются на уровне объектов групповой политики (GPO), после чего могут связываться с отдельными группами и пользователями.

Групповые политики

Контроль изменений, имеющих место в среде Windows 2000 Server, осуществляется с помощью оснастки Групповая политика. Эта оснастка используется в следующих случаях:

- администрирование и конфигурирование оборудования;
- администрирование и конфигурирование клиентов;
- параметры и политика, связанные с операционной системой;
- параметры и политика подсистемы обеспечения безопасности;
- обеспечение доступа к сети.

Этот перечень может уточняться и модифицироваться, но суть дела от этого не меняется.

То или иное свойство *групповой политики* в среде Windows 2000 Server может применяться к объекту, который отвечает за осуществление контроля над доступом пользователя или компьютера к определенным системным ресурсам. Этот объект именуется объектом групповой политики (GPO, Group Policy Object).

Групповая политика может применяться по отношению к узлу, домену или подразделению, которые играют роль контейнеров для субъектов групповых политик. Благодаря использованию групповых политик пользователю будут доступны многие возможности.

- Объекты групповых политик могут настраиваться и сохраняться в базе данных Active Directory либо определяться в качестве объектов локальной политики. Защита и блокирование автономных компьютеров осуществляются с помощью локальных объектов групповых политик.
- Сами объекты групповой политики могут применяться по отношению к пользователям и компьютерам, которые находятся в контейнерах Active Directory.

- Всем объектам групповой политики присуща определенная степень защиты. Подобно любым другим объектам Windows 2000, любой объект групповой политики может быть заблокирован.
- Возможны фильтрация или контроль объектов групповой политики на основе их принадлежности к тем или иным группам безопасности.
- Сценарии регистрации в системе, завершения сеанса работы и автозагрузки также используют объекты групповой политики.

Групповые политики способны оказывать влияние практически на любой процесс, приложение или службу, выполняемые в системе Windows 2000 Server (Windows XP).

Ниже перечислены категории групповых политик.

- Развертывание приложений. Политики из этой категории применяются для управления доступом пользователя к отдельным приложениям.
- Развертывание файлов. Эти политики призваны размещать файлы в заранее указанных на компьютерах пользователей папках.
- Создание сценариев. Эти политики обеспечивают выбор сценариев, которые будут запускаться на выполнение в заранее указанное время.
- Программы. Политики из этой категории обеспечивают настройку программ, установленных на пользовательских компьютерах, которые подключены к локальным и глобальным сетям.
- Безопасность. Одна из наиболее важных областей применения групповых политик.

ПРИМЕЧАНИЕ В среде Windows XP создание и настройка политик осуществляется с помощью апплета Локальная политика безопасности, который находится в разделе Администрирование в панели управления. Подробное рассмотрение возможностей этого инструментального средства производится в десятой главе.

Установка и настройка сетевых протоколов

В этом разделе будет рассматриваться установка и настройка сетевых протоколов в среде Windows 2000 Server. Начать рассмотрение следует, конечно, с набора протоколов TCP/IP.

ВНИМАНИЕ В среде Windows XP настройка протокола практически ничем не отличается, о некоторых особенностях будет упомянуто чуть позже.

Для установки набора протоколов TCP/IP в контекстном меню приложения Мое сетевое окружение нужно выбрать пункт Свойства. Можно также воспользоваться командой Пуск ▸ Настройка ▸ Сеть и удаленный доступ к сети. После этого в контекстном меню сетевого подключения, использующего набор протоколов TCP/IP, нужно выполнить команду Свойства. После этого будет отображено диалоговое окно свойств выбранного соединения (рис. 7.26). Если в перечне установленных компонентов

протокол TCP/IP отсутствует, нужно нажать кнопку Установить, а после этого выполнить команду Протокол ▸ Добавить. В отобразившемся на экране списке нужно выбрать компонент TCP/IP (Протокол Интернета (TCP/IP)) и нажать кнопку OK.

ПРИМЕЧАНИЕ

В среде Windows XP доступ к окну установки и конфигурирования набора протоколов TCP/IP производится при помощи команды Пуск ▸ Сетевое окружение. В окне Сетевое окружение нужно активировать ярлык Сетевые подключения. После этого в контекстном меню требуемого сетевого подключения останется выбрать пункт Свойства. В результате выполнения этих действий отобразится диалоговое окно свойств данного подключения (рис. 7.27).

Рис. 7.26. На этой странице производится установка и настройка различных сетевых компонентов

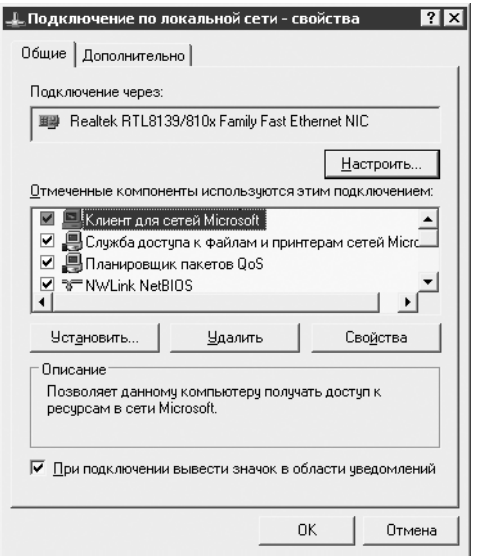


Рис. 7.27. Установка и настройка сетевых программных компонентов в среде Windows XP

Настройка набора протоколов TCP/IP

Для настройки свойств набора протоколов TCP/IP нужно использовать упомянутое ранее окно свойств сетевого соединения. Достаточно дважды щелкнуть на записи, соответствующей протоколу TCP/IP, после чего будет отображена вкладка Общие окна свойств этого протокола. На ней располагаются основные настраиваемые параметры этого окна (рис. 7.28).

Конечно, нужно описать параметры, отображаемые в этом диалоговом окне.

- Получить IP-адрес автоматически. Этот флажок применяется в том случае, если автоматическое получение IP-адреса и некоторых других параметров выполняется с помощью службы DHCP.
- Использовать следующий IP-адрес. Этот флажок применяется для определения постоянного IP-адреса.

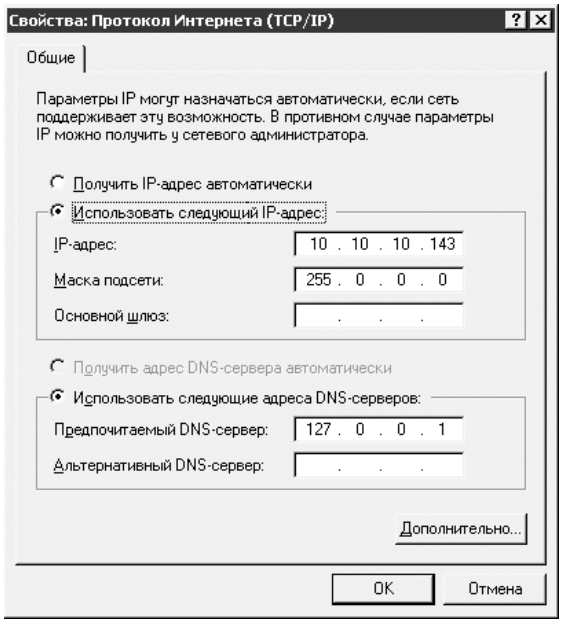


Рис. 7.28. Диалоговое окно настройки параметров набора протоколов TCP/IP

- IP-адрес. В этом поле указывается статический IP-адрес в виде последовательности октетов, разделенных точками.
- Маска подсети. Данное поле хранит маску подсети в виде набора октетов, разделенных точками.
- Основной шлюз. Это поле предназначено для указания основного шлюза, применяемого для маршрутизации IP-трафика, который не имеет отношения к локальной сети.
- Получить адрес DNS-сервера автоматически. Этот флажок позволяет в автоматическом режиме получать список DNS-серверов от DNS-сервера. Он доступен только в случае автоматического получения IP-адреса.
- Использовать следующие адреса DNS-серверов. В этом поле указываются постоянные IP-адреса, соответствующие установленным DNS-серверам.
- Предпочитаемый DNS-сервер. В поле указывается IP-адрес DNS-сервера, который используется по умолчанию для определения имен и IP-адресов узлов.
- Альтернативный DNS-сервер. Здесь можно указать IP-адрес DNS-сервера, который применяется для идентификации имен узлов и IP-адресов в том случае, если основной DNS-сервер окажется недоступным.

Если нажать кнопку Дополнительно, то будет отбражено диалоговое окно Дополнительные параметры TCP/IP (по умолчанию выбрана вкладка Параметры IP, как показано на рис. 7.29), в котором можно определить дополнительные IP-адреса компьютера, а также указать дополнительные адреса шлюзов. В поле Метрика интерфейса определяется показатель количества переходов, характеризующий

установленный шлюз. При осуществлении маршрутизации по умолчанию используется тот шлюз, которому присуще наименьшее значение этого показателя.

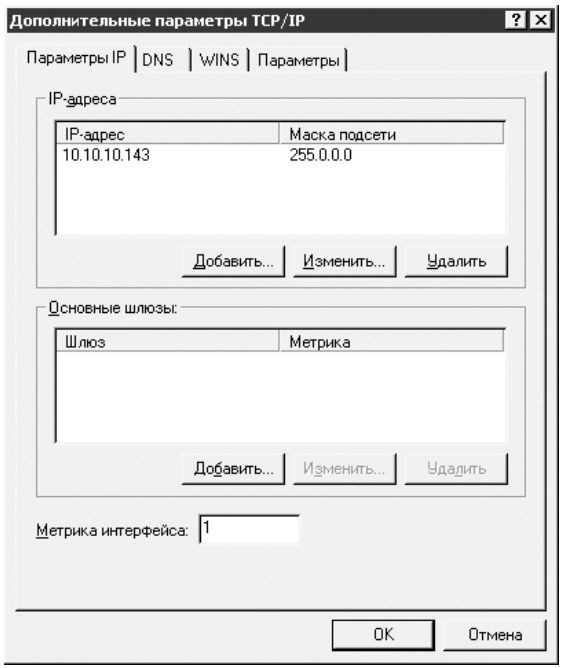


Рис. 7.29. Окно Дополнительные параметры TCP/IP, вкладка Параметры IP

В этом диалоговом окне также имеются вкладки DNS, WINS, Параметры. Следует рассмотреть назначение каждой вкладки.

Вкладка DNS (рис. 7.30) применяется для конфигурирования параметров сервера DNS. Здесь, помимо описания адресов DNS-серверов, можно узнать, каким образом сетевой клиент выполняет операции по определению имен и динамическому обновлению записей службы DNS.

Вкладка DNS позволяет задавать ряд важных параметров.

- Дописывать основной DNS-суффикс и суффикс подключения. Этот переключатель определяет добавление основного суффикса, а также суффикса подключения к именам узлов в процессе их определения. Основной DNS-суффикс может задаваться в диалоговом окне свойств Сетевая идентификация. Его можно применять по отношению ко всей системе либо заменять DNS-суффиксом, который определяется для конкретного используемого подключения.
- Дописывать родительские суффиксы основного DNS-суффикса. Этот флажок указывает на то, будут ли предприниматься попытки нахождения неопределенного имени на уровне родительского домена компьютера. Предположим, что для данного компьютера в качестве основного DNS-суффикса используется support.microsoft.com. В этом случае для определения имени Bill будут перебираться названия bill.support.microsoft.com и bill.microsoft.com.

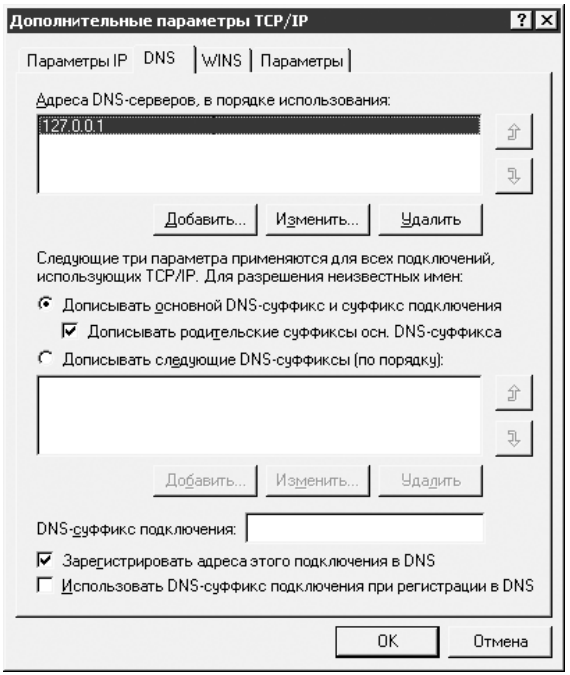


Рис. 7.30. На этой вкладке настраиваются параметры сервера DNS

- Дописывать следующие DNS-суффиксы (по порядку). Этот переключатель применяется только в том случае, если в процессе идентификации неопределенных имен используются лишь указанные суффиксы DNS.
- DNS-суффикс подключения. В этом поле подключению сопоставляется DNS-суффикс, который отличается от основного суффикса, определяемого в окне Сетевая идентификация.
- Зарегистрировать адреса этого подключения в DNS. В случае выбора этого переключателя клиенты будут отсылать DNS-серверу запросы на обновление записей при модификации имени узла или IP-адреса. При этом DNS-серверу отсылается полное имя компьютера вместе с соответствующим IP-адресом. Имя компьютера указывается на вкладке Сетевая идентификация, которая находится в диалоговом окне свойств Система.
- Использовать DNS-суффикс подключения при регистрации в DNS. Если установлен этот переключатель, сетевой клиент отсылает DNS-серверу запросы на обновление записей в случае изменения имени узла или IP-адреса. В отличие от предыдущего переключателя, в процессе регистрации клиента используется первая часть имени компьютера, которая указана на вкладке Сетевая идентификация диалогового окна свойств Система наравне с DNS-суффиксом, определенным в текстовом поле DNS-суффикс подключения.

На вкладке WINS (рис. 7.31) настраиваются параметры служб WINS. Далее приводится краткое описание параметров, настраиваемых в этом диалоговом окне.

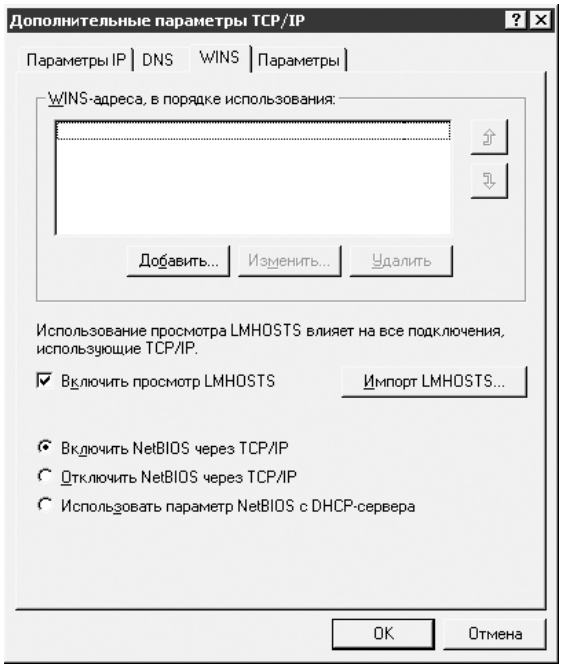


Рис. 7.31. На этой вкладке настраиваются параметры служб WINS

- Включить просмотр LMHOSTS. Этот флажок определяет использование локального файла LMHOSTS для имен NetBIOS на основе указанных IP-адресов.
- Импорт LMHOSTS. Эта кнопка обеспечивает импорт данных, направляемых в локальный файл LMHOSTS из какого-либо другого файла LMHOSTS.
- Включить NetBIOS через TCP/IP. Этот переключатель активизирует протокол NetBIOS через TCP/IP (NetBT и WINS). Его необходимо использовать в том случае, если в сети имеются компьютеры, на которых установлены ранние версии Windows 9x или Windows NT. Необходимость в этом протоколе отсутствует, если используется однородная вычислительная среда Windows 2000 или производится подключение к другим компьютерам в Интернете с помощью службы DNS.
- Отключить NetBIOS через TCP/IP. Этот переключатель позволяет отключить протокол NetBT, когда он не нужен.
- Использовать параметр NetBIOS с DHCP-сервера. Этот переключатель позволяет DHCP-серверу автоматически определять настройки службы WINS.

Вкладка Параметры (рис. 7.32) позволяет выполнять настройку параметров протокола IP Security (IPSec), а также задавать параметры фильтрации IP-пакетов. После нажатия на кнопку Свойства отображается диалоговое окно IP-безопасность. Здесь можно использовать флажки Не использовать IPSec или Использовать следующую политику IP-безопасности. В последнем случае потребуется в списке указать необходимую политику, а затем нажать кнопку OK.

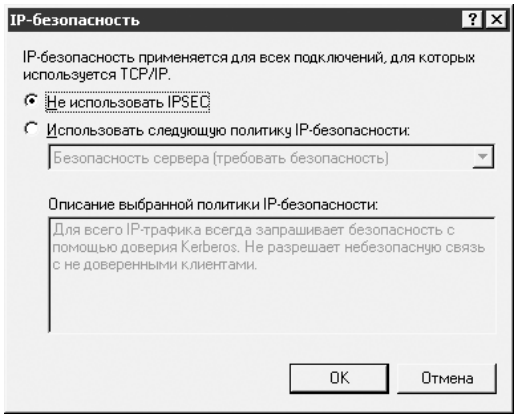


Рис. 7.32. В этом окне производится настройка параметров протокола IPSec

Если нажать кнопку Свойства при выбранной вкладке Фильтрация TCP/IP, то будет отображено диалоговое окно Фильтрация TCP/IP (рис. 7.33). Этот параметр обеспечивает менее строгий метод контроля по сравнению с протоколом IPSec. Здесь можно настраивать трафик для определенных портов TCP/IP, UDP и протокола IP.

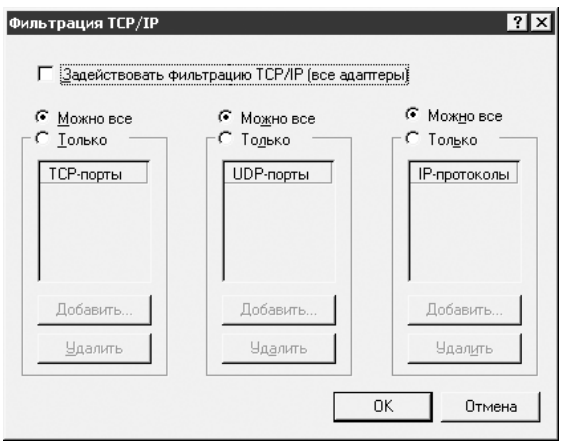


Рис. 7.33. В этом окне задается контроль трафика для портов TCP, UDP и протокола IP

ПРИМЕЧАНИЕ В Windows XP вкладка IPSec отсутствует, поэтому можно настраивать только фильтрацию пакетов.

Теперь настало время обсудить настройку программной маршрутизации в Windows 2000 Server.

ВНИМАНИЕ В среде Windows XP программный маршрутизатор отсутствует. Если вам требуется этот компонент, нужно использовать программы независимых разработчиков.

Установка и настройка службы DHCP

Служба DHCP, входящая в комплект поставки Windows 2000 Server, используется для назначения адресов и управления ими. Причем в этом случае реализуется динамическое присвоение адресов.

Установка службы DHCP осуществляется при помощи апплета панели управления Установка и удаление программ. Для получения доступа к параметрам этой службы после установки достаточно выполнить команду Пуск ▸ Программы ▸ Администрирование ▸ DHCP. В результате выполнения этой команды на экране будет отображено окно консоли DHCP (рис. 7.34).

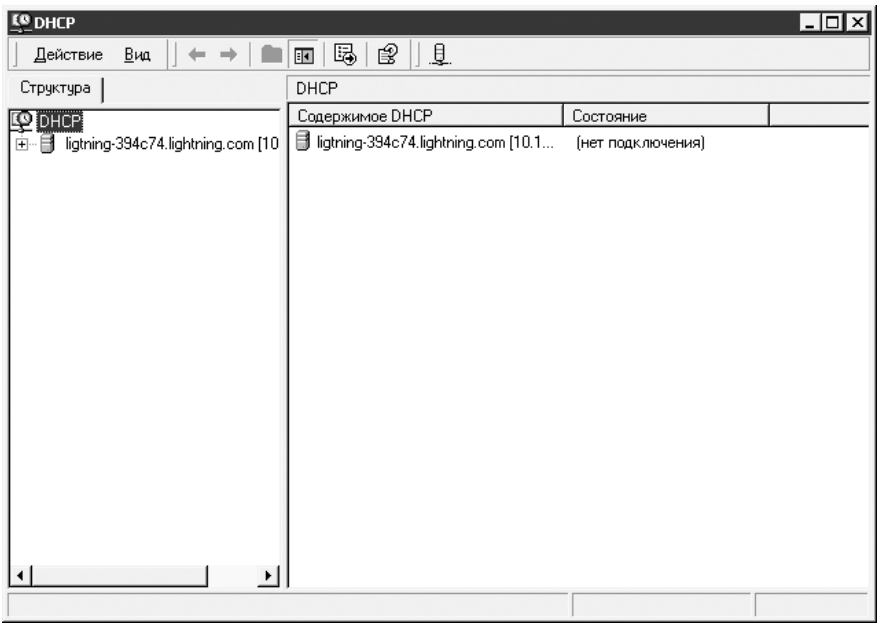


Рис. 7.34. Консоль DHCP в среде Windows 2000 Server

Набор свойств перечня IP-адресов определяется с помощью так называемых *областей DHCP*. Этим же механизмом предоставляются сведения о службе доменных имен и стандартном шлюзе. Чтобы начать работу со службой DHCP, потребуется создать хотя бы одну такую область. Для этого в контекстном меню дерева сервера DHCP нужно выполнить команду Создать область. После этого на экране будет отображено окно мастера, в котором потребуется указать соответствующие сведения.

- Имя. В этом поле определяется имя, отображаемое в консоли DCHP области. Например, «Область „Бухгалтерия“».
- Описание. Этот необязательный параметр отображается на вкладке области Общие диалогового окна свойств. В рассматриваемом случае было указано описание «Отдел бухгалтерии».

- Начальный IP-адрес. В этом поле вводится IP-адрес, определяющий начало области обзора.
- Конечный IP-адрес. В этом поле указывается IP-адрес, определяющий конец области обзора.
- Исключаемый диапазон адресов. Здесь указываются IP-адреса, которые исключаются из рассматриваемой области.
- Срок действия аренды. Интервал времени, определяющий срок действия IP-адреса.
- Настройка дополнительных параметров. Мастер может предложить настройку дополнительных параметров области.
- Активизация области. Этот параметр позволяет активизировать область в любой момент времени.

Служба DHCP также позволяет создавать несколько областей, выступающих в качестве единого целого, — *суперобласти*. Эти объекты могут применяться для выделения IP-адресов клиентам в многосегментных сетях.

Установка служб DNS и WINS

Служба DNS (Domain Name Service, служба доменных имен) позволяет выполнять операции преобразования имен компьютеров и узлов в IP-адреса (*разрешение имен*). При этом используется так называемый *прямой просмотр*. Если же на основе первоначального IP-адреса определяется имя компьютера, применяется операция обратного *просмотра*.

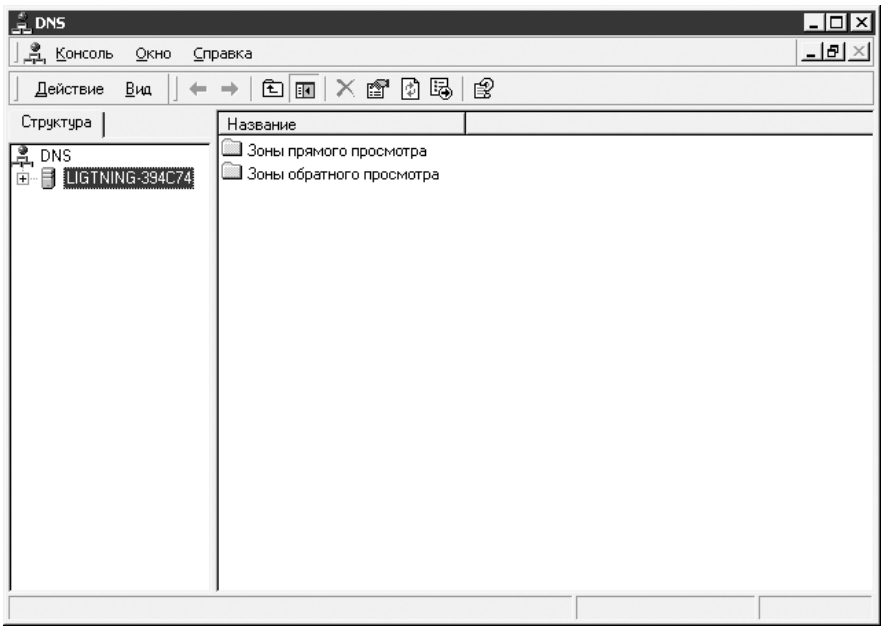


Рис. 7.35. Так выглядит консоль DNS в среде Windows 2000 Server

Служба WINS (Windows Internet Naming Sevice, служба имен Интернета для Windows) обеспечивает функционирование службы имен NetBIOS, которая связывает имена NetBIOS с IP-адресами. Она отвечает за централизованное управление данными из пространства имен NetBIOS и позволяет избежать удаленного администрирования несколькими файлами LMHOSTS. Служба WINS также обеспечивает совместимость со старыми сетями Windows (до Windows 2000).

Установка службы DNS производится при помощи апплета Установка и удаление программ в панели управления. После его запуска в диалоговом окне Установка и удаление программ нужно выбрать пункт Установка или удаление компонентов Windows. Затем потребуется выбрать компонент Сетевые службы и нажать кнопку Состав. В новом окне потребуется выбрать пункт DNS и нажать кнопку OK.

В окне консоли DNS (рис. 7.35) можно настраивать различные параметры, создавать зоны прямого и обратного просмотра, а также настраивать свойства зон.

Установка службы WINS подобна установке службы DNS. На рис. 7.36 показано окно консоли WINS.

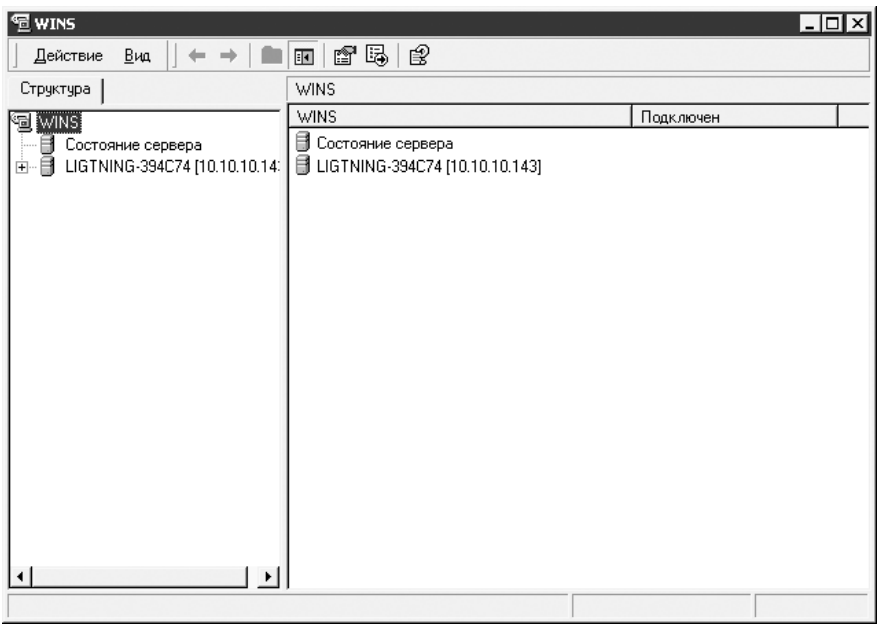


Рис. 7.36. Так выглядит консоль WINS в среде Windows 2000 Server

Настройка клиентов

Если нужно настроить клиентские системы Windows 2000 для работы со службами DNS и WINS, то особых проблем, как правило, не возникает. В этом случае следует определить IP-адреса для клиентов, используемые при работе с DNS- и WINS-серверами. С помощью службы DHCP можно реализовать настройки таким образом, чтобы сервер DHCP автоматически предоставлял клиентам сведения о серверах DNS и WINS.

Если же служба DHCP не применяется, то все настройки выполняются вручную. Для этого нужно выполнить команду Пуск ▸ Настройка ▸ Сеть и удаленный доступ к сети и перейти в диалоговое окно Сеть и удаленный доступ к сети. В контекстном меню требуемого подключения нужно выполнить команду Свойства и перейти на вкладку Общие. В общем списке потребуется выбрать протокол TCP/IP и нажать кнопку Свойства. В открывшемся диалоговом окне протокола можно будет выполнить необходимые настройки.

В процессе настройки клиентов Windows NT и Windows 9x для использования службы DNS нужно щелкнуть правой кнопкой мыши на значке Сетевое окружение и в контекстном меню выбрать пункт Свойства. В отобразившемся диалоговом окне свойств протокола TCP/IP можно будет произвести необходимые настройки.

Настройка программной маршрутизации в среде Windows 2000 Server

Служба *маршрутизации и удаленного доступа* (RRAS, Routing and Remote Access Service), действующая в системе Windows 2000 Server, обеспечивает возможность использования сервера Windows 2000 в качестве маршрутизатора постоянных подключений, а также маршрутизатора по требованию, который может устанавливать подключения в случае поступления соответствующего клиентского запроса.

ПРИМЕЧАНИЕ Для получения дополнительных сведений о маршрутизаторах и протоколах маршрутизации обратитесь к пятой главе.

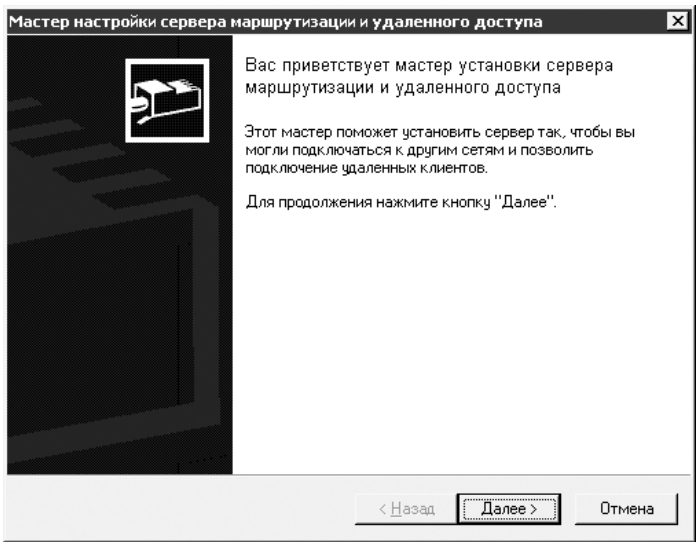


Рис. 7.37. При помощи этого мастера можно настроить и запустить на выполнение службу маршрутизации и удаленного доступа

Для запуска на выполнение службы маршрутизации и удаленного доступа нужно выполнить команду Пуск ▸ Программы ▸ Администрирование ▸ Маршрутизация и удаленный доступ. После этого в левой части окна нужно выбрать сервер и выполнить команду его контекстного меню Настроить и включить маршрутизацию и удаленный доступ (рис. 7.37).

После щелчка на кнопке Далее будет отображено следующее окно, в котором нужно выбрать переключатель Сетевой маршрутизатор (рис. 7.38).

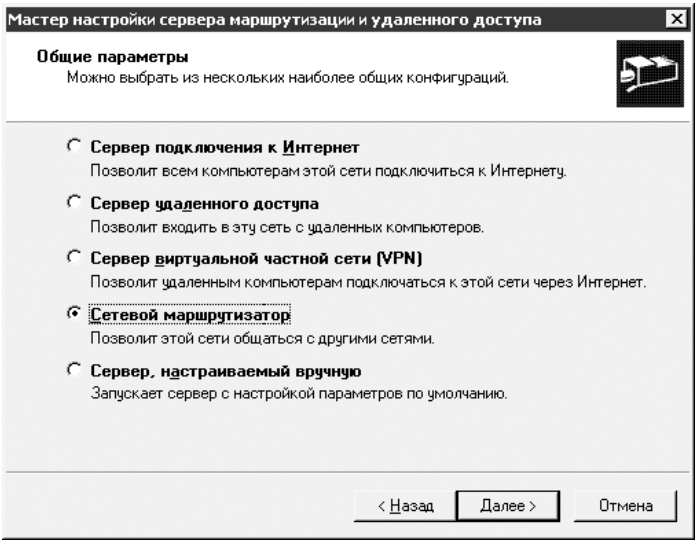


Рис. 7.38. Здесь определяется область применения службы маршрутизации и удаленного доступа

После щелчка на кнопке Далее отображается диалоговое окно, в котором нужно выбрать один из двух переключателей режимов работы.

- Установить общий доступ к подключению Интернета (ICS). Этот режим используется для подключения к Интернету небольших домашних или офисных сетей.
- Установить маршрутизатор с протоколом преобразования сетевых адресов (NAT). Этот режим устанавливается в том случае, если имеется несколько подключений или если требуются протоколы маршрутизации.

Затем производится настройка следующего набора параметров.

- Протоколы. В этом диалоговом окне следует выбрать поддерживаемые протоколы. Они должны быть заранее установлены, так как служба RRAS лишь разрешает их использование по умолчанию.
- Использовать подключения по требованию. Пользователь должен установить соответствующий переключатель в зависимости от того, будут ли выбраны подключения по требованию.
- Назначение IP-адресов. Можно выбрать способ назначения IP-адресов с помощью службы DHCP либо задать пул статических IP-адресов.

Настройка маршрутизатора

После запуска службы маршрутизации и удаленного доступа потребуется выполнить настройку самого маршрутизатора. Сначала будет рассмотрен вариант с использованием статических маршрутов.

Для добавления очередного статического маршрута следует открыть окно консоли RRAS и раскрыть ветвь IP-маршрутизация. В ней нужно выбрать пункт Статические маршруты, а затем в контекстном меню правой панели выполнить команду Новый статический маршрут. После этого на экране отобразится диалоговое окно Статический маршрут (рис. 7.39), параметры которого описаны в следующем списке.

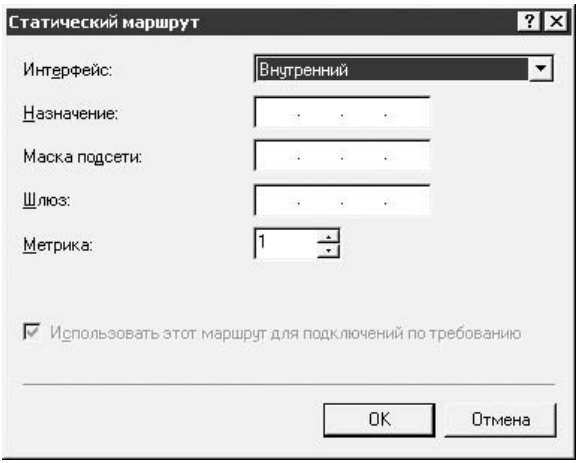


Рис. 7.39. Здесь определяется статический маршрут

- Интерфейс. Здесь указывается сетевой интерфейс, который будет применяться для пересылки соответствующих сетевых пакетов. Можно выбрать внутренний интерфейс или подключение по локальной сети.
- Назначение. Здесь указывается адрес, соответствующий адресу целевого пакета. После этого служба RRAS сравнивает указанный в заголовке пакета адрес назначения с целевым адресом, который был ранее внесен в это поле. Можно указывать адреса узлов, сетевые адреса, стандартный маршрут или просто 0.0.0.0.
- Маска подсети. В этом поле указывается маска сети назначения или узлов. В случае стандартного маршрута достаточно ввести маску 0.0.0.0.
- Шлюз. Указанный здесь адрес применяется для отсылки всех пакетов, имеющих отношение к определенному маршруту. Этот адрес должен быть доступным для внешнего сетевого сегмента маршрутизатора.
- Метрика. Выбранная здесь числовая величина определяет относительную стоимость маршрута. Причем меньшей цене соответствует меньшее значение метрики, что является вполне логичным.
- Использовать этот маршрут для подключений по требованию. Результатом установки этого флажка будет то, что маршрутизатор инициализирует подключение

по требованию после получения пакетов для указанного маршрута. Этот параметр будет доступным, только если для маршрутизатора определен как минимум один интерфейс по требованию.

Если нужно установить интерфейс для подключения по требованию, следует открыть окно консоли RRAS, а затем активировать узел сервера, для которого устанавливается интерфейс. В контекстном меню интерфейсов маршрутизации, перечисленных в левой панели окна, нужно выполнить команду Создать новый интерфейс вызова по требованию. После этого останется лишь указать соответствующие параметры, которые будут использованы мастером при создании нового интерфейса.

Динамическая маршрутизация

В случае построения очень сложных сетей придется от статических маршрутов перейти к использованию протоколов RIP или OSPF. Настройка этих двух основных протоколов маршрутизации описывается в следующих разделах главы.

Настройка протокола RIP

Перед тем как выполнять настройку протокола RIP, следует его установить. Для этого в окне консоли RRAS нужно открыть ветвь IP-маршрутизация. В контекстном меню пункта Общие следует выполнить команду Новый протокол маршрутизации. В отобразившемся окне останется лишь выбрать пункт RIP версии 2 для IP и нажать кнопку OK. После этого в ветви IP-маршрутизация отобразится новый узел RIP.

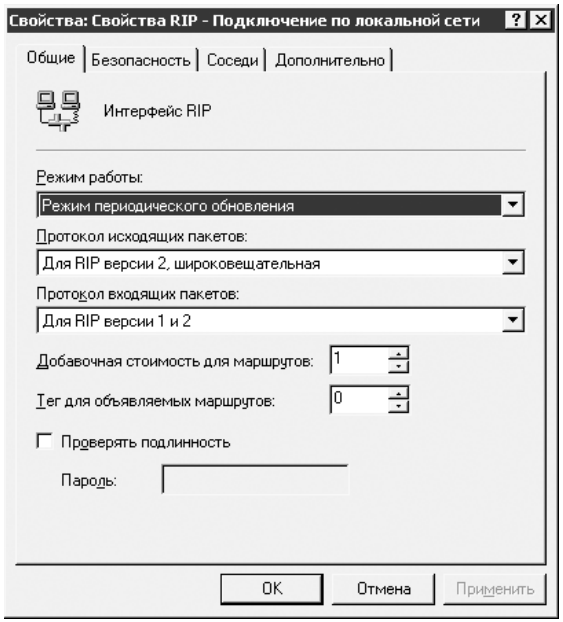


Рис. 7.40. Вкладка Общие окна свойств протокола RIP

Затем следует указать интерфейс, используемый при запуске и выполнении протокола. Для этого в контекстном меню узла RIP нужно выполнить команду Новый интерфейс. В диалоговом окне потребуется выбрать требуемый интерфейс и нажать кнопку OK.

После завершения выбора интерфейса потребуется настроить параметры протокола RIP. Ниже приводится соответствующий список, относящийся к вкладке Общие (рис. 7.40).

- Режим работы. В этом поле определяется режим обновления данных о маршрутах, используемый протоколом RIP. Режим автостатического обновления указывает на отсылку службой RRAS уведомлений только в том случае, если обновления запрашиваются другими маршрутизаторами. Если же выбран режим периодического обновления, уведомления RIP отсылаются автоматически через определенные интервалы времени, которые определяются параметром Интервал периодического обновления на вкладке Дополнительно.
- Протокол исходящих пакетов. Здесь указывается протокол, используемый исходящими уведомлениями протокола RIP.
- Протокол входящих пакетов. В этом поле указывается, каким образом маршрутизатор обрабатывает входящие уведомления протокола RIP. Если выбран параметр Игнорировать входящие пакеты, то маршрутизатор будет функционировать только в режиме отсылки уведомлений.
- Добавочная стоимость для маршрутов. Это значение добавляется к количеству переходов, в результате чего увеличивается относительная стоимость маршрута. Благодаря этому параметру обеспечивается блокирование избыточного трафика именно для данного маршрута.
- Тег для объявляемых маршрутов. Эта опция обеспечивает передачу номера тега вместе со всеми уведомлениями протокола RIP версии 2.
- Проверять подлинность/пароль. Этот параметр определяет включение незакодированного пароля во все входящие и исходящие уведомления протокола RIP версии 2. Сам пароль указывается в поле Пароль.

На вкладке Безопасность (рис. 7.41) определяется, какие маршруты будут приниматься/отклоняться в случае поступления RIP-сообщений от других маршрутизаторов.

На вкладке Соседи (рис. 7.42) определяется способ взаимодействия данного маршрутизатора с соседними маршрутизаторами. Ниже приводится описание соответствующих параметров.

- Только широковещательная или многоадресатная рассылка (не использует ресурсы соседних маршрутизаторов RIP). Этот переключатель позволяет пропускать только те уведомления протокола RIP, которые отсылаются с применением указанного на вкладке Общие протокола исходящих пакетов.
- Использует соседние маршрутизаторы в дополнение к широковещательной или многоадресатной рассылке. Этот переключатель позволяет определять те маршрутизаторы, которым служба RRAS отсылает уведомления протокола RIP, а также маршрутизаторы, которые сами отправляют уведомления протокола RIP с применением протокола исходящих пакетов.
- Использует ресурсы соседних маршрутизаторов вместо широковещательной или многоадресатной рассылки. В этом случае выбираются маршрутизаторы, которым

служба RRAS отсылает уведомления протокола RIP, но сами они в этом участия не принимают. Этот способ используется в сетях, которые не поддерживают рассылку широковещательных уведомлений протокола RIP.

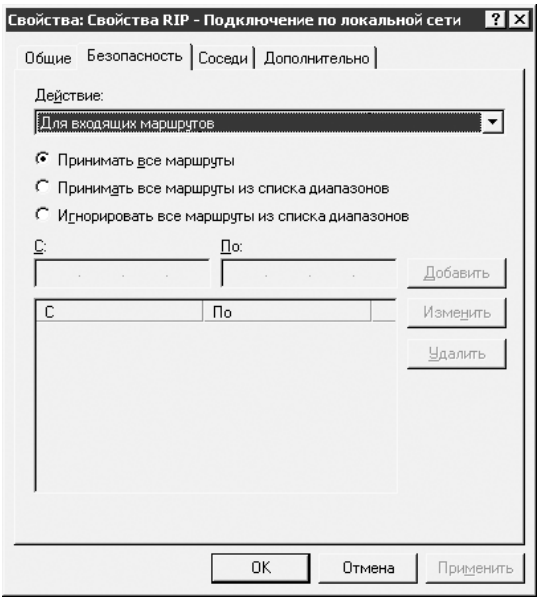


Рис. 7.41. Вкладка Безопасность окна свойств протокола RIP

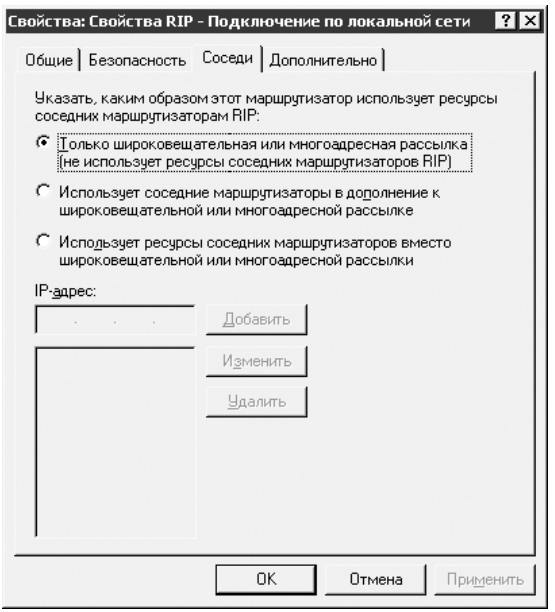


Рис. 7.42. Вкладка Соседи окна свойств протокола RIP

На вкладке Дополнительно определяется ряд дополнительных параметров протокола RIP (рис. 7.43).

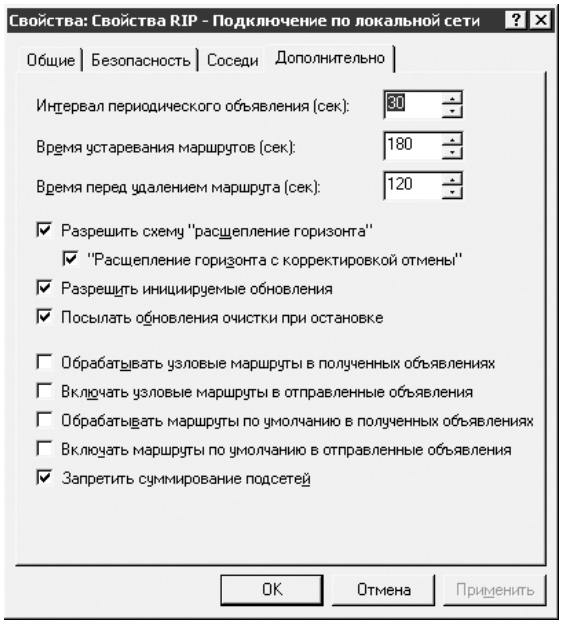


Рис. 7.43. Вкладка Дополнительно окна свойств протокола RIP

- Интервал периодического обновления (сек). Интервал, по прошествии которого поступают уведомления протокола RIP от локального маршрутизатора.
- Время устаревания маршрута (сек). Время существования маршрутов, используемых протоколом RIP. Если в течение этого времени маршруты не обновляются, они помечаются как недействительные.
- Время перед удалением маршрута (сек). Это время определяет период, в течение которого маршруты остаются в таблице маршрутизации до их окончательного удаления.
- Разрешить схему «расщепления» горизонта. При установке этого флажка предотвращается распространение в сети сведений о маршрутах, которые были созданы ранее.
- «Расщепление горизонта с корректировкой отмены». Этот флажок позволяет назначить метрику маршрутам, сведения о которых распространяются в той сети, в которой они были созданы. В результате эти маршруты станут недостижимыми.
- Разрешить инициируемые обновления. Этот флажок позволяет маршрутизатору генерировать периодические обновления в случае изменений таблицы маршрутизации.
- Посылать обновления очистки при остановке. Этот флажок позволяет протоколу RIP сообщать сведения обо всех маршрутах, длина которых равна 15, соседним

маршрутизаторам в случае отключения локального маршрутизатора, в результате чего эти маршруты будут недоступны.

- Обрабатывать узловые маршруты в полученных объявлениях. Этот параметр позволяет включать сведения о маршрутах узлов, содержащихся в уведомлениях протокола RIP.
- Включать узловые маршруты в отправленные объявления. Этот параметр позволяет включать сведения о маршрутах для узлов в исходящие уведомления.
- Обрабатывать маршруты по умолчанию в полученных объявлениях. Этот параметр позволяет включать сведения о стандартных маршрутах, содержащиеся в уведомлениях протокола RIP.
- Включать маршруты по умолчанию в отправленные объявления. Этот параметр обеспечивает включение сведений о стандартных маршрутах в исходящие уведомления протокола RIP.
- Запретить суммирование подсетей. При установке этого флажка обеспечивается определение параметров маршрутов в соответствии с идентификаторами сети.

ВНИМАНИЕ Если при подключении рабочей станции Windows XP не просматриваются «соседние» компьютеры, исправить ситуацию может установка службы Слушатель RIP. Эта служба просто необходима, если в вашей сети используется протокол RIPv1, и выполняется прием обновлений маршрутов, отправляемых маршрутизаторами. Для установки этой службы в панели управления нужно запустить апплет Установка и удаление программ, затем щелкнуть на ярлыке Установка компонентов Windows, перейти в раздел Сетевые службы и установить соответствующий флажок.

Настройка протокола OSPF

Для установки протокола OSPF нужно выбрать сервер в окне консоли RRAS и раскрыть ветвь IP-маршрутизация. В контекстном меню Общие потребуется выбрать пункт Новый протокол маршрутизации. Затем нужно выбрать пункт OSPF-открытие кратчайшего пути первым и нажать кнопку OK. Затем правой кнопкой мыши нужно щелкнуть на узле OSPF и в контекстном меню выполнить команду Новый интерфейс. После этого будет отображено диалоговое окно свойств интерфейса (рис. 7.44).

Диалоговое окно свойств протокола OSPF содержит три вкладки: Общие, Соседи NBMA и Дополнительно.

На вкладке Общие отображается адрес, на который отвечает интерфейс маршрутизатора, код области, а также некоторые другие свойства. На вкладке Соседи NBMA диалогового окна свойств протокола OSPF и определяются соседние маршрутизаторы, если тип сети — NBMA. На вкладке Дополнительно диалогового окна свойств протокола OSPF определяются интервалы времени задержки между передачами, а также параметры MTU для каждого выбранного интерфейса.

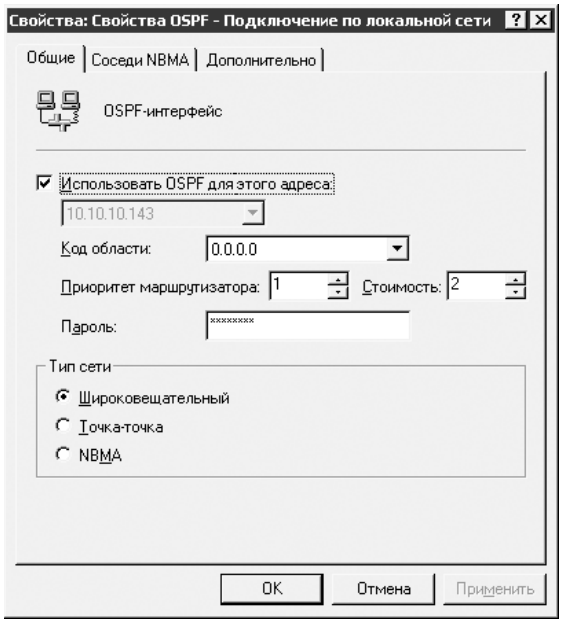


Рис. 7.44. Диалоговое окно настройки свойств протокола OSPF

Типичные проблемы и неполадки в локальной сети

В случае возникновения каких-либо проблем с сетями TCP/IP в первую очередь следует попытаться определить, не была ли случайным образом изменена конфигурация системы. Достаточно часто к неприятностям приводит неправильное указание IP-адреса, маски подсети или адреса шлюза. Для устранения проблем достаточно обратиться к диалоговому окну свойств набора протоколов TCP/IP.

Источником проблем может также служить некорректная настройка службы DNS или IP-маршрутизации.

Общее правило, которым следует руководствоваться в данном случае, состоит в применении метода «последовательного подхода». В следующем перечне кратко описаны шаги, присущие этому подходу, в формате «проблема-решение».

1. Не инициализируется набор протоколов TCP/IP или не запускается нужная служба. В этом случае причина обычно кроется в некорректной настройке. Для устранения этой ошибки нужно перейти в диалоговое окно свойств определенного интерфейса и внимательно просмотреть заданные параметры. Особенно это актуально для статических IP-адресов. Если в системе установлено несколько сетевых адаптеров, нужно проверить корректность назначенных им приоритетов. Для этого достаточно в диалоговом окне Сеть и удаленный доступ к сети выбрать команду Дополнительно ▸ Дополнительные параметры. Затем в диалоговом окне Адаптеры и привязки нужно переместить основной

адаптер в верхнюю часть списка. Требуется также убедиться в том, что протокол TCP/IP привязан к основному адаптеру.

2. Невозможно подключиться к другим компьютерам или другие компьютеры не отвечают. Причины появления этой проблемы часто связаны с конфликтом IP-адресов, ошибками сетевых аппаратных компонентов или с некорректной арендой адресов DHCP. Если используется система Windows 2000 Server, то команда ipconfig позволяет проверить IP-адрес, маску подсети и адрес шлюза.

ПРИМЕЧАНИЕ Чуть позже будет приведен краткий обзор наиболее полезных команд, используемых для просмотра конфигурации и настройки сети.

3. Что делать в том случае, если выполнение команды ping *локальный_узел* завершается успехом, но соединение с локальными или удаленными компьютерами не может быть установлено? В этом случае следует проверить корректность заданной маски подсети. Если устанавливается соединение с локальными компьютерами, а к удаленным компьютерам подключиться невозможно, то, скорее всего, неправильно настроен шлюз или маршрутизатор.

ВНИМАНИЕ Быстрый просмотр параметров рабочей станции (IP-адрес, маска подсети, основной шлюз) в среде Windows XP осуществляется при помощи выбора в контекстном меню сетевого подключения пункта Состояние. В этом же окне отображается физический адрес (MAC-адрес) рабочей станции. Обратите внимание на кнопку Исправить в окне Состояние подключения к локальной сети. Не следует нажимать эту кнопку, если параметры набора протоколов TCP/IP настроены вручную. Результат этого действия, скорее всего, будет негативным.

4. Команда ping имя_компьютера дает положительные результаты только при ее выполнении на локальном компьютере. Причиной возникновения подобной ошибки может служить некорректно работающая служба DNS. Нужно убедиться в корректности указания DNS-серверов, а также в их доступности.
5. Команда ping дает положительные результаты при ее запуске с рабочей станции, на которой выполняется операционная система, отличная от Windows 2000, но соединение этой станции со всей сетью при помощи консольной команды NET не выполняется. Эта проблема может быть связана с алгоритмом определения имен NetBIOS. Нужно проверить настройки службы WINS и убедиться в том, что протокол NetBIOS корректно функционирует. Эта проблема может также появляться в том случае, если заблокировано выполнение службы рабочей станции на локальном компьютере или на том компьютере, к которому требуется подключиться в данный момент.
6. Возможно установление связи с компьютером или веб-сайтом с использованием IP-адреса, а не имени узла. В этом случае проблемы надо искать в службе DNS. Нужно убедиться в том, что указаны правильные DNS-серверы, а также в том, что они доступны в настоящий момент.

Помимо описанных общих методик диагностики и устранения неисправностей, Windows 2000 (Windows XP) предлагает несколько диагностических утилит, выполняемых в режиме командной строки. Эти команды описаны далее.

Команда arp

Эта команда реализует вывод и изменение записей кэша протокола ARP, который содержит одну или несколько таблиц, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet или Token Ring. Для каждого сетевого адаптера Ethernet или Token Ring, установленного в компьютере, используется отдельная таблица. Запущенная без параметров, команда arp выводит справку.

Синтаксис

arp [-a [*IP-адрес*] [-N *IP-адрес интерфейса*]] [-g [*IP-адрес*] [-N *IP-адрес интерфейса*]] [-d *IP-адрес* [*IP-адрес интерфейса*]] [-*IP-адрес MAC-адрес* [*IP-адрес интерфейса*]]

Таблица 7.2. Параметры команды arp

Параметр	Описание
–a [IP-адрес] [–N IP-адрес интерфейса]	Вывод таблиц текущего протокола ARP для всех интерфейсов. Чтобы вывести записи ARP для определенного IP-адреса, нужно воспользоваться командой arp -a с параметром IP-адрес. Чтобы вывести таблицы кэша ARP для определенного интерфейса, нужно указать параметр -N IP-адрес интерфейса. Параметр -N вводится с учетом регистра символов
-g [IP-адрес] [-N IP-адрес интерфейса]	Эффект такой же, как и в случае применения параметра -a
-d IP-адрес [IP-адрес интерфейса]	Удаление записи с определенным IP-адресом. Чтобы удалить запись таблицы для определенного интерфейса, нужно указать IP-адрес интерфейса. Чтобы удалить все записи, нужно указать звездочку (*) вместо параметра IP-адрес
-s IP-адрес MAC-адрес [IP-адрес интерфейса]	Добавление статической записи, которая сопоставляет параметр IP-адрес с физическим адресом MAC-адрес, в кэш ARP. Чтобы добавить статическую запись кэша ARP в таблицу для определенного интерфейса, нужно указать параметр IP-адрес интерфейса
/?	Отображение справки в командной строке

- IP-адреса, указываемые в качестве параметров, записываются в точечно-десятичной нотации.
- Физический адрес для параметра MAC-адрес состоит из шести байтов, записанных в шестнадцатеричном формате и разделенных дефисами (например, 00-01-80-55-58-79).

- Записи, добавленные с параметром `-s`, являются статическими и не удаляются из кэша ARP после истечения заданного периода времени. Записи удаляются, если протокол TCP/IP был остановлен и снова запущен. Чтобы создать постоянные статические записи кэша ARP, достаточно выполнить соответствующие команды `arp` и воспользоваться планировщиком заданий для выполнения этого файла при запуске.
- Эта команда доступна, только если в свойствах сетевого адаптера в окне Сетевые подключения в качестве компонента установлен Протокол Интернета (TCP/IP).

Примеры применения

Чтобы вывести таблицы кэша ARP для всех интерфейсов, нужно ввести следующую команду:

```
arp -a
```

Чтобы вывести таблицу кэша ARP для интерфейса, которому назначен IP-адрес 10.1.24.9, достаточно выполнить следующую команду:

```
arp -a -N 10.1.24.9
```

Чтобы добавить статическую запись кэша ARP, которая сопоставляет IP-адрес 10.1.24.9 с физическим адресом 00-01-80-55-58-79, требуется выполнить следующую команду:

```
arp - 10.1.24.9 00-01-80-55-58-79
```

Команда ipconfig

Эта команда отображает все текущие параметры сети TCP/IP и обновления параметров DHCP и DNS. При вызове команды `ipconfig` без параметров выводится только IP-адрес, маска подсети и основной шлюз для каждого сетевого адаптера.

Синтаксис

`ipconfig [/all] [/renew [`*адаптер*`]] [/release [`*адаптер*`]] [/flushdns] [/displaydns] [/registerdns] [/showclassid адаптер] [/setclassid адаптер [`*код_класса*`]]`

Таблица 7.3. Параметры команды ipconfig

Параметр	Описание
/all	Отображение полной конфигурации набора протоколов TCP/IP для всех адаптеров. Если этот параметр не будет указан, то команда ipconfig отображает лишь IP-адреса, маску подсети и основной шлюз для каждого адаптера. Адаптеры могут представлять собой физические интерфейсы, такие как установленные сетевые адаптеры, или логические интерфейсы, такие как подключения удаленного доступа
/renew [адаптер]	Обновление конфигурации DHCP для всех адаптеров или только для явно указанного адаптера. Этот параметр может использоваться только на компьютерах с адаптерами, настроенными для автоматического получения IP-адресов

Продолжение ⇩

Таблица 7.3 (*продолжение*)

Параметр	Описание
/release [адаптер]	Отправка сообщения DHCPRELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаление настроек IP-адресов для всех адаптеров (если параметр адаптера не задан) или для заданного адаптера. Этот параметр отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов
/flushdns	Сброс и очистка содержимого кэша разрешения имен DNS клиента. Во время устранения неполадок DNS эту процедуру используют для удаления из кэша записей отрицательных попыток сопоставления и других динамически добавляемых записей
/displaydns	Отображение содержимого кэша разрешения имен DNS клиента, включающего записи, предварительно загруженные из локального файла Hosts, а также последние полученные записи ресурсов для запросов разрешения имен. Эта информация используется службой DNS клиента для быстрого разрешения часто встречаемых имен без обращения к указанным в конфигурации DNS-серверам
/registerdns	Динамическая регистрация вручную имен DNS и IP-адресов, настроенных на компьютере. Этот параметр полезен при устранении неполадок в случае отказа в регистрации имени DNS или при выяснении причин неполадок динамического обновления между клиентом и DNS-сервером без перезагрузки клиента. Имена, зарегистрированные в DNS, определяются параметрами DNS в дополнительных свойствах протокола TCP/IP
/showclassid адаптер	Отображение кода класса DHCP для указанного адаптера. Чтобы просмотреть код класса DHCP для всех адаптеров, вместо этого параметра нужно ввести символ звездочки (*). Данный параметр доступен только на компьютерах с адаптерами, настроенными для автоматического получения IP-адресов
/setclassid адаптер [код_класса]	Задание кода класса DHCP для указанного адаптера. Чтобы задать код класса DHCP для всех адаптеров, вместо параметра адаптер укажите звездочку (*). Данный параметр доступен только на компьютерах с адаптерами, настроенными для автоматического получения IP-адресов. Если код класса DHCP не задан, текущий код класса удаляется
/?	Отображение справки в командной строке

- Команда ipconfig является эквивалентом командной строки команды winipcfg, входящей в состав Windows Millennium Edition, Windows 98 и Windows 95. Хотя Windows XP не имеет графического эквивалента команде winipcfg, для просмотра и обновления IP-адреса можно воспользоваться окном Сетевые подключения. Для этого нужно открыть окно Сетевые подключения, щелкнуть правой кнопкой мыши на сетевом подключении, выбрать команду Состояние, а затем открыть вкладку Поддержка.
- Данная команда доступна только на компьютерах с адаптерами, настроенными для автоматического получения IP-адресов. Это позволяет пользователям определять, какие значения конфигурации были получены с помощью DHCP, APIPA или другого способа автоматического конфигурирования.

- Если значение параметра *адаптер* содержит пробелы, его следует заключать в кавычки.
- В именах адаптеров, задаваемых для команды ipconfig, поддерживается использование знака звездочки (*) для задания имен, начинающихся с указанной строки или содержащих определенную последовательность символов.
- Эта команда доступна, только если в свойствах сетевого адаптера в объекте Сетевые подключения в качестве компонента установлен протокол Интернета (TCP/IP).

Примеры применения

Чтобы вывести основную конфигурацию TCP/IP для всех адаптеров, нужно ввести команду:

```
ipconfig
```

Чтобы вывести полную конфигурацию TCP/IP для всех адаптеров, требуется ввести команду:

```
ipconfig /all
```

Чтобы обновить конфигурацию IP-адреса, определенную DHCP-сервером только для адаптера Подключение по локальной сети, следует ввести команду:

```
ipconfig /renew «Подключение по локальной сети»
```

Чтобы сбросить кэш разрешения имен DNS при наличии проблем в процессе разрешения имен, нужно ввести команду:

```
ipconfig /flushdns
```

Чтобы отобразить код класса DHCP для всех адаптеров с именами, начинающимися со слова Подключение, достаточно ввести команду:

```
ipconfig /showclassid Подключение*
```

Чтобы задать код класса DHCP My_server для адаптера Подключение по локальной сети требуется ввести команду:

```
ipconfig /setclassid «Подключение по локальной сети» My_server
```

Команда hostname

Эта команда отображает имя узла, входящего в состав полного имени компьютера.

Синтаксис

```
hostname
```

Для этой команды используется единственный параметр /?, при указании которого в командной строке отображается справка по команде.

Доступ к команде возможен только в том случае, если в свойствах сетевого адаптера объекта Сетевые подключения в качестве компонента установлен протокол Интернета (TCP/IP).

Примеры применения

Для отображения на экране имени компьютера нужно выполнить следующую команду:

```
hostname
```

Команда msconfig

В отличие от всех остальных утилит командной строки, при вызове этой утилиты отображается диалоговое окно Настройка системы (рис. 7.45), состоящее из шести вкладок.

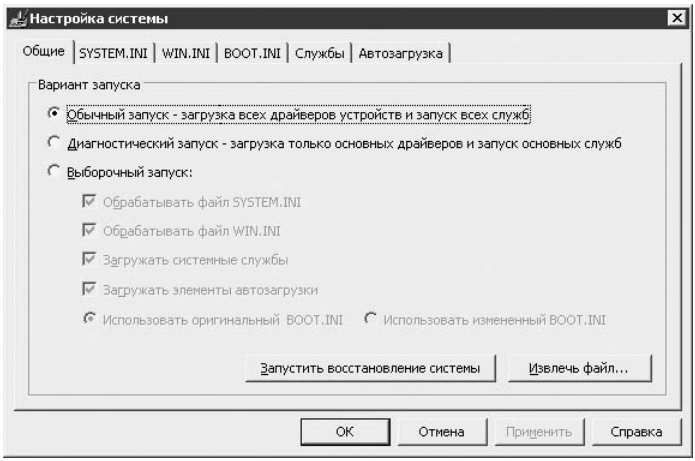


Рис. 7.45. Доступные в этом диалоговом окне вкладки позволяют настраивать различные аспекты загрузки системы

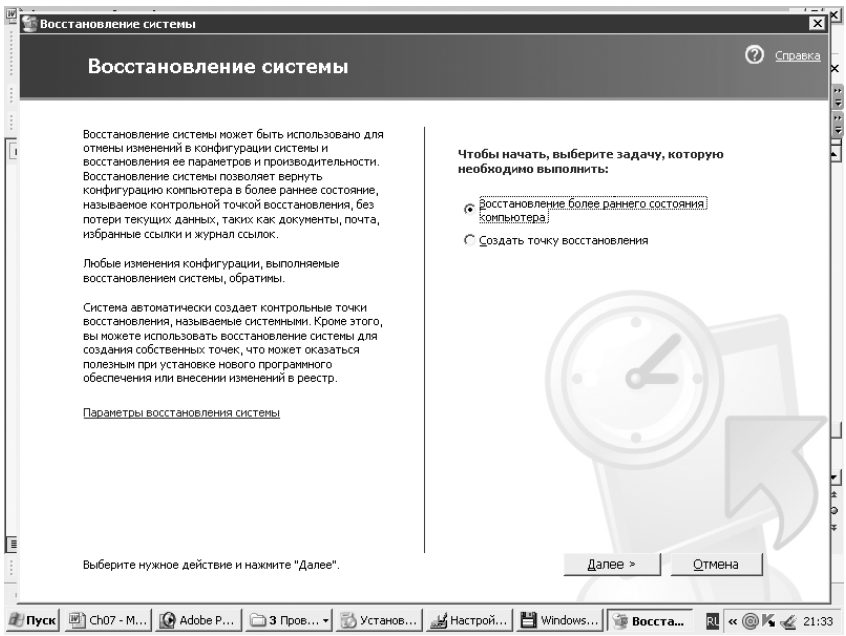


Рис. 7.46. Параметры этого диалогового окна позволяют управлять общими аспектами загрузки операционной системы

- Общие. Здесь можно выбирать вариант запуска системы. Кроме того, в распоряжении пользователя находятся две дополнительных возможности: Запустить восстановление системы и Извлечь файл. Первая команда запускает мастер восстановления системы из более раннего состояния (рис. 7.46). Эту возможность часто используют в том случае, когда происходит критический системный сбой и альтернативные методы не помогают. Вторая команда позволяет извлечь файл из установочных файлов системы.
- SYSTEM.INI. Как и следует из ее названия, эта вкладка позволяет легко и быстро редактировать различные разделы этого важного системного файла конфигурации, доставшегося Windows XP в наследство от более старых версий Windows.
- WIN.INI. Эта вкладка позволяет редактировать данные еще одного важного системного файла — WIN.INI. Этот файл также относится к категории унаследованных способов конфигурирования системы.
- BOOT.INI. Еще один важный системный файл, перешедший по наследству из Windows 2000, при помощи которого можно выбирать различные варианты загрузки одной или нескольких операционных систем. После выбора этой вкладки открывается соответствующее диалоговое окно, в котором пользователь может выбрать различные варианты загрузки (и соответствующие ключи, рис. 7.47).

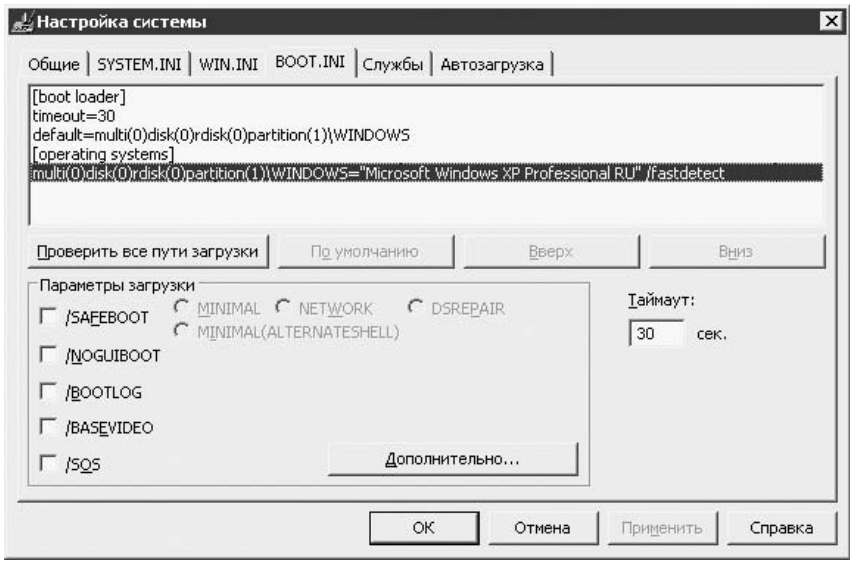


Рис. 7.47. Файл BOOT.INI позволяет легко и просто организовать мультисистемную загрузку

- Службы. После выбора этой вкладки открывается диалоговое окно, в котором отображены службы, выполняющиеся в данный момент на компьютере (рис. 7.48). Пользователь может остановить выполнение любой службы или всех служб одновременно, хотя последнее делать крайне не рекомендуется.

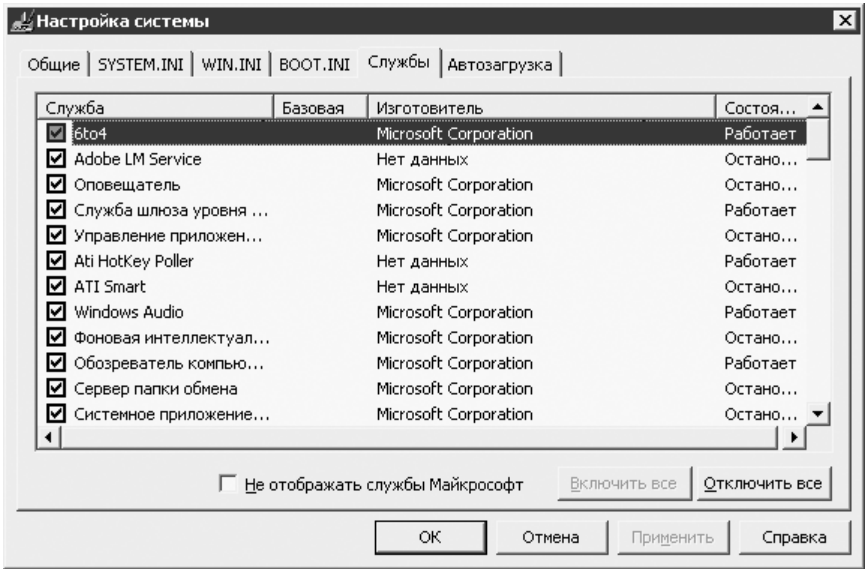


Рис. 7.48. Вкладка Службы позволяет отслеживать запущенные службы

- Автозагрузка. Эта вкладка позволяет изменять набор программ, автоматически загружаемых в процессе загрузки операционной системы (рис. 7.49). При этом пользователю доступны сведения относительно расположения соответствующего загружаемого файла, а также название ключа системного реестра.

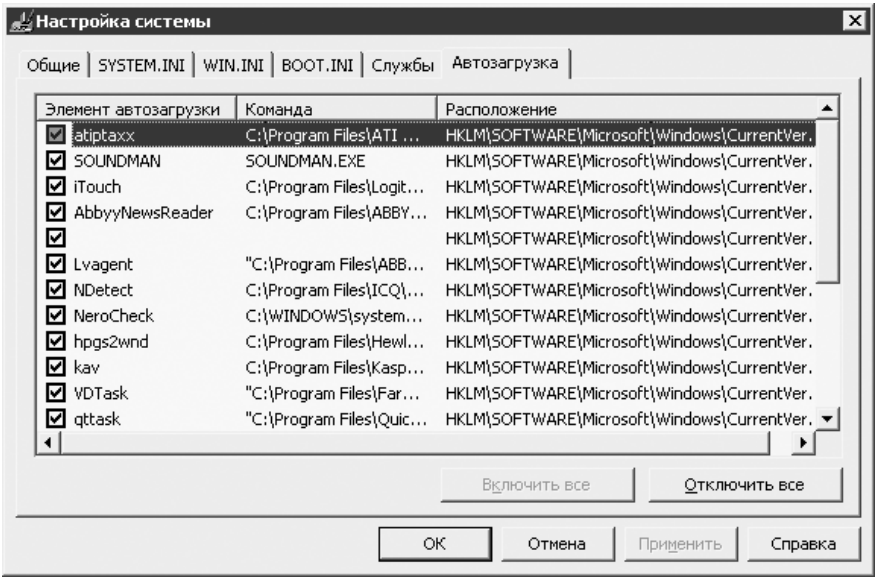


Рис. 7.49. Эта вкладка весьма удобна для отслеживания разного рода «нелегальных» программ, которые загружаются в автоматическом режиме при запуске системы

Команда nbtstat

Эта команда обеспечивает отображение статистики протокола NetBIOS over TCP/IP (NetBT), таблиц имен NetBIOS для локального и удаленного компьютеров, а также кэша имен NetBIOS. Команда Nbtstat, параметры которой приведены в табл. 7.4, позволяет обновить кэш имен NetBIOS и имена, зарегистрированные в службе имен Интернета Windows (WINS). Если эту команду запустить на выполнение без указания параметров, будет отображена справка.

Синтаксис

nbtstat [-a *имя_удаленного_компьютера*] [-A *IP-адрес*] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [*интервал*]

Таблица 7.4. Параметры команды nbtstat

Параметр	Описание
-a имя_удаленного_компьютера	Отображение таблицы имен NetBIOS удаленного компьютера, где параметр имя_удаленного_компьютера определяет имя NetBIOS удаленного компьютера. Таблица имен NetBIOS является списком имен NetBIOS, соответствующих приложениям NetBIOS, выполняющимся на данном компьютере
-A IP-адрес	Отображение таблицы имен NetBIOS удаленного компьютера, заданного IP-адресом
-c	Отображение содержимого кэша имен NetBIOS, таблицы имен NetBIOS и их разрешенных IP-адресов
-n	Отображение таблицы имен NetBIOS локального компьютера. Состояние Зарегистрирован означает, что это имя зарегистрировано на сервере WINS или в качестве широковещательного адреса
-r	Отображение статистики процесса разрешения имен NetBIOS. На компьютере Windows XP, настроенном для использования WINS, этот параметр возвращает количество имен, разрешенных и зарегистрированных для широковещательной рассылки или WINS
-R	Очистка содержимого кэша имен NetBIOS и перезагрузка записей #PRE из файла Lmhosts
-RR	Освобождение и обновление имен NetBIOS для локального компьютера, зарегистрированного на серверах WINS
-s	Отображение сеансов клиента и сервера NetBIOS с попыткой преобразования конечного IP-адреса в имя
-S	Вывод сведений о работе сервера и клиента NetBIOS; удаленные компьютеры выводятся только по IP-адресам
интервал	Обновление выбранной статистики на экране через промежутки времени, заданные значением интервал. Нажатие клавиш Ctrl+C останавливает обновление статистики. Если этот параметр не задан, команда nbtstat выводит сведения о текущей конфигурации один раз
/?	Отображение справки в командной строке

При определении параметров команды nbtstat учитывается регистр символов. В табл. 7.5. приведены заголовки столбцов, отображаемые программой nbtstat.

Таблица 7.5. Заголовки столбцов, отображаемые командой nbstat

Заголовок столбца	Описание
Ввод	Количество полученных байтов
Вывод	Количество отправленных байтов
Вид	Направление передачи от локального компьютера (Исх) или от удаленного компьютера (Вхд)
Время жизни	Время, оставшееся до сброса элемента кэша таблицы имен
Локальное имя	Локальное имя NetBIOS, соответствующее данному подключению
Удаленный узел	Имя или IP-адрес удаленного компьютера
<03>	Последний байт имени NetBIOS, преобразованный в шестнадцатеричную форму. Каждое имя NetBIOS может иметь длину 16 знаков. Последний байт часто имеет специальное значение, так как одно имя может встречаться несколько раз на одном компьютере, различаясь только последним байтом. Например, код <20> представляет собой пробел
Тип	Тип имени. Имя может быть уникальным именем или именем группы
Состояние	Значение Зарегистрирован (служба NetBIOS работает на удаленном компьютере) или Конфликт (в службе уже зарегистрировано такое же имя компьютера)
Состояние	Состояние подключений NetBIOS

В табл. 7.6 приведены возможные состояния подключения NetBIOS.

Таблица 7.6. Состояния подключения NetBIOS

Название состояния	Описание
Подключен	Сеансовое подключение установлено
Назначен	Конечная точка подключения создана и связана с IP-адресом
Ожидание	Конечная точка доступна для входящих подключений
Простаивает	Конечная точка создана, но подключение не получено
Подключается	Сеанс в состоянии подключения, установлено сопоставление имени и IP адреса для точки назначения
Прием	Запрос на входящее подключение принят, подключение будет установлено
Повторное подключение	Повторная попытка установки подключения после первой неудачной попытки
Исходящий	Сеанс находится в процессе подключения, создается подключение TCP
Входящий	Сеанс находится в процессе подключения
Отключение	Сеанс находится в процессе отключения
Отключен	Локальный компьютер отправил запрос на отключение и ожидает подтверждения от удаленной системы

Эта команда доступна, только если в свойствах сетевого адаптера в объекте Сетевые подключения в качестве компонента установлен протокол Интернета (TCP/IP).

Примеры применения

Чтобы отобразить таблицу имен удаленного компьютера, имеющего имя NetBIOS Ligthning, нужно использовать следующую команду:

```
nbtstat -a Lightning
```

Чтобы вывести таблицу имен NetBIOS удаленного компьютера, имеющего IP-адрес 10.1.24.9, достаточно ввести следующую команду:

```
nbtstat -A 10.1.24.9
```

Чтобы вывести таблицу имен локального компьютера, используется следующая команда:

```
nbtstat -n
```

Чтобы вывести содержимое кэша имен NetBIOS локального компьютера, достаточно ввести следующую команду:

```
nbtstat -c
```

Чтобы очистить кэш имен NetBIOS и перезагрузить записи #PRE из локального файла Lmhosts, нужно воспользоваться следующей командой:

```
nbtstat -R
```

Чтобы освободить имена NetBIOS, зарегистрированные на сервере WINS, и снова зарегистрировать их, следует ввести следующую команду:

```
nbtstat -RR
```

Чтобы просмотреть статистику сеанса NetBIOS по IP-адресу с обновлением каждые десять секунд, достаточно воспользоваться следующей командой:

```
nbtstat -S 5
```

Команда ping

Эта команда является любимым средством диагностики для многих сетевых администраторов. Она отправляет сообщения с эхо-запросом по протоколу ICMP, проверяя соединение на уровне протокола IP с другим компьютером, поддерживающим TCP/IP. После каждой передачи выводится соответствующее сообщение с полученным эхо-ответом. Команда ping — это основная команда TCP/IP, используемая для устранения неполадок в соединении, проверки возможности доступа и разрешения имен. Если ее запустить без параметров, будет отображена инструкция по использованию этой команды.

Синтаксис

ping [-t] [-a] [-n *счетчик*] [-l *размер*] [-f] [-i *TTL*] [-v *тип*] [-r *счетчик*] [-s *счетчик*] [{-j *список_узлов* | -k *список_узлов*}] [-w *интервал*] [*имя_целевого_компьютера*]

Команда ping позволяет проверить имя и IP-адрес компьютера. Если проверка IP-адреса прошла успешно, а проверка имени — нет, то можно считать, что имеет место проблема разрешения имен. В этом случае при помощи запросов DNS

(Domain Name System) или методов разрешения имен NetBIOS нужно удостовериться, что имя задаваемого компьютера было записано в локальном файле Hosts.

Команда ping, параметры которой приведены в табл. 7.7, может использоваться только в том случае, если в свойствах сетевого адаптера в объекте Сетевые подключения в качестве компонента установлен протокол Интернета (TCP/IP).

Таблица 7.7. Параметры команды ping

Параметр	Описание
-t	Параметр инициирует отправку сообщений с эхо-запросом к точке назначения до тех пор, пока команда не будет прервана. Для прерывания команды и вывода статистики необходимо нажать комбинацию клавиш CTRL+BREAK. Для прерывания команды ping и выхода из нее достаточно нажать клавиши CTRL+C
-a	Параметр задает разрешение обратного имени по IP-адресу назначения. В случае успешного выполнения выводится имя соответствующего узла
-n счетчик	Параметр задает количество отправляемых сообщений с эхо-запросом. По умолчанию это число равно четырем
-l размер	Параметр определяет в байтах длину поля данных в отправленных сообщениях с эхо-запросом. По умолчанию задается длина в 32 байта. Максимальное значение этой величины составляет 65 527 байтов
-f	Параметр задает отправку сообщений с эхо-запросом с флагом Don't Fragment в IP-заголовке с единичным значением. Сообщения с эхо-запросом не фрагментируются маршрутизаторами на пути к месту назначения. Этот параметр полезен для устранения проблем, возникающих с максимальным размером модуля данных для канала (Maximum Transmission Unit)
-i TTL	Параметр задает значение поля TTL в IP-заголовке для отправляемых сообщений с эхо-запросом. Для узлов Windows XP значение по умолчанию обычно равно 128. Максимальное значение TTL — 255
-v тип	Параметр задает значение поля типа службы (TOS) в IP-заголовке для отправляемых сообщений с эхо-запросом. По умолчанию это значение равно нулю. Параметр тип определяется как десятичное число в промежутке от 0 до 255
-r счетчик	Параметр задает способ записи маршрута (Record Route) в IP-заголовке для записи пути, по которому проходит сообщение с эхо-запросом и соответствующее ему сообщение с эхо-ответом. Каждый переход в пути использует указанный способ записи маршрута. По возможности значение счетчика задается равным или большим, чем количество переходов между источником и местом назначения. Значение параметра счетчика изменяется от 1 до 9
-s счетчик	Параметр определяет способ отображения штампа времени Интернета (Internet Timestamp) в заголовке IP для записи времени прибытия сообщения с эхо-запросом и соответствующего ему сообщения с эхо-ответом для каждого перехода. Значение параметра счетчик изменяется от 1 до 4

Продолжение ⇨

Таблица 7.7 (*продолжение*)

Параметр	Описание
-j список_ узлов	Для сообщений с эхо-запросом этот параметр гарантирует использование свободной маршрутизации в IP-заголовке с набором промежуточных точек назначения, указанным при помощи параметра список_узлов. При свободной маршрутизации последовательные промежуточные точки назначения могут быть разделены одним или несколькими маршрутизаторами. Максимальное число адресов или имен в списке узлов равно деавяти. Список узлов оформлен как набор IP-адресов в точечно-десятичной нотации, разделенных пробелами
-k список_узлов	Указывает для сообщений с эхо-запросом использование параметра строгой маршрутизации в IP-заголовке с набором промежуточных точек назначения, указанным в списке_узлов. При строгой маршрутизации следующая промежуточная точка назначения должна быть доступной напрямую (она должна быть соседней в интерфейсе маршрутизатора). Максимальное число адресов или имен в списке узлов равно 9. Список узлов — это набор IP-адресов (в точечно-десятичной нотации), разделенных пробелами
-w интервал	Параметр определяет в миллисекундах время ожидания получения сообщения с эхо-ответом, которое соответствует сообщению с эхо-запросом. Если сообщение с эхо-ответом не получено в пределах заданного интервала, то выдается сообщение об ошибке Request timed out. Интервал, заданный по умолчанию, равен 4000 (4 секунды)
имя_целевого_компьютера	Параметр задает точку назначения, идентифицированную IP-адресом или именем узла
/?	Параметр инициирует отображение справки в командной строке

Примеры применения

Приведенный ниже пример содержит результаты выполнения команды ping:

```
C:\>ping www.mail.ru
Обмен пакетами с www.mail.ru [194.67.57.26] по 32 байт:
Ответ от 194.67.57.26: число байт=32 время=101 мс TTL=114
Ответ от 194.67.57.26: число байт=32 время=96 мс TTL=114
Ответ от 194.67.57.26: число байт=32 время=100 мс TTL=114
Ответ от 194.67.57.26: число байт=32 время=102 мс TTL=114
```

Для отправки сообщения точке назначения 10.1.92.121 и сопоставления с ее узловым именем нужно ввести следующую команду:

```
ping -a 10.1.92.121
```

Для отправки по адресу 10.1.92.121 десяти собщений с эхо-запросом, каждое из которых имеет поле данных из 1000 байт, нужно воспользоваться следующей командой:

```
ping -n 10 -l 1000 10.1.92.121
```

Для отправки сообщения по адресу 10.1.92.121 и записи маршрута для пятипереходов используется следующая команда:

```
ping -r 5 10.1.92.121
```

Для отправки сообщения по адресу 10.1.92.121 и задания свободной маршрутизации для точек назначения в регионе 10.13.1.2-10.34.5.4-10.2.67.3 нужно ввести следующую команду:

```
ping -j 10.13.1.2 10.34.5.3 10.2.67.3 10.1.92.121
```

Для тестирования сетевого адаптера можно воспользоваться командой `ping`, указав так называемый адрес закольцовки — 127.0.0.1. В случае успешного выполнения будет выведен следующий результат:

```
C:\>ping 127.0.0.1
Обмен пакетами с 127.0.0.1 по 32 байт:
Ответ от 127.0.0.1: число байт=32 время<1 мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1 мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1 мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1 мс TTL=128
```

Как видите, в данном случае проблем с сетевым адаптером не возникло.

На этом можно завершить рассмотрение установки и настройки локальных сетей в среде Windows 2000/XP. Конечно, эта тема фактически неисчерпаема. Но основные стадии этого процесса были рассмотрены достаточно подробно. Осталось рассмотреть некоторые особенности установки и настройки беспроводных сетей, чья очередь придет в следующей главе.

8 ГЛАВА Особенности установки и настройки беспроводных сетей

В этой небольшой главе рассматриваются основные процессы настройки беспроводных сетей в среде Windows 2000 Server (Windows XP).

ПРИМЕЧАНИЕ В третьей главе уже рассматривались теоретические положения, относящиеся к беспроводным сетям.

В дальнейшем будут рассматриватьс преимущественноя установка и настройка радиосетей, поскольку этот тип беспроводных сетей наиболее распространен в настоящее время.

На практике чаще всего используются два типа беспроводных сетей.

- Сети, работающие в режиме «ad-hoc» («равноправные» сети). Сети этого типа характеризуются тем, что сетевые компьютеры обмениваются между собой данными в непосредственном режиме, не обращаясь к услугам всякого рода «посредников». Здесь невольно напрашивается аналогия с одноранговыми локальными сетями Ethernet, реализованными на коаксиальном кабеле без применения концентраторов и других промежуточных сетевых устройств.
- Сети, использующие точки доступа (access point). Здесь обмен данными в радиоэфире осуществляется при помощи специальных устройств, называемых точками доступа. В этом случае уместна аналогия с кабельными сетями Ethernet, реализованными на витой паре, когда обмен данными осуществляется с помощью центрального концентратора или коммутатора.

ВНИМАНИЕ В версии Windows XP появились средства автоматической настройки беспроводных сетей в режиме «ad hoc». Но для этого потребуется установить пакет обновлений Service Pack 2, в состав которого входит мастер настройки беспроводной сети. На самом деле в состав инсталляционного пакета Windows 2000 XP Professional (версия 2002 года) Service Pack 2 включен по умолчанию, поэтому необходимость в его отдельной установке отсутствует. В среде Windows 2000 Server все необходимые настройки придется выполнять вручную.

Сети, не использующие точки доступа, удобны в том случае, когда организуется временная сеть без связи с обычной кабельной сетью либо когда требуется организовать соединение между двумя компьютерами («точка-точка»). Во всех остальных случаях целесообразнее воспользоваться беспроводной сетью на основе точки доступа.

Точка доступа является центральным элементом беспроводной сети. Это компактное устройство объединяет беспроводных пользователей друг с другом и с внешним миром. Она получает, буферизует и передает данные, поддерживая группу беспроводных пользователей. Как правило, точка доступа располагается в отдельном хорошо защищенном месте. От выбора места расположения зависит излучаемая мощность радиосигнала, поэтому при подборе этого места необходимо воспользоваться соответствующей диагностической программой.

Точки доступа позволяют получить сразу несколько преимуществ.

- С их использованием устраняется потенциальная опасность конфликтов, неизбежно возникающих в том случае, когда два компьютера пытаются получить доступ к одному и тому же беспроводному каналу связи.
- Пользователи могут подключаться к локальной сети или непосредственно к Интернету.
- Как минимум, в два раза увеличивается дальность действия радиоканала.
- С использованием этих устройств увеличивается безопасность беспроводных сетей, поскольку точка доступа выполняет фильтрацию на основе аппаратных и сетевых адресов, а также указанных портов и протоколов.
- При помощи точек доступа можно распространить беспроводную сеть на большую область, устанавливая дополнительные точки доступа.

А теперь рассмотрим особенности подключения к беспроводным сетям различных устройств.

Подключение к беспроводной сети различных устройств

Спектр оборудования, подключаемого к беспроводным сетям, весьма широк. В этот список входят карманные компьютеры, ноутбуки, персональные компьютеры и даже цифровые фотоаппараты и принтеры. И во всех этих устройствах для подключения к беспроводной сети применяются *адаптеры* самых различных модификаций. Так, например, для подключения карманных компьютеров

к беспроводным сетям используются миниатюрные беспроводные адаптеры, вставляемые в разъем для подключения карт памяти CompactFlash. Подобный адаптер показан на рис. 8.1.

Рис. 8.1. Беспроводной адаптер Linksys Wireless-B CompactFlash Card WCF11

Для подключения к беспроводной сети ноутбуков применяются беспроводные адаптеры стандарта PCMCIA. Обычно эти устройства поставляются в комплекте с клиентским программным обеспечением, при помощи которого отслеживаются такие характеристики беспроводного соединения, как мощность сигнала и скорости передачи данных. Поскольку в портативных компьютерах используется система управления электропитанием, то при отсутствии приема или передачи данных применяется режим снижения потребляемой мощности. На рис. 8.2 показан беспроводной адаптер для ноутбука.

Рис. 8.2. Беспроводной адаптер Linksys Wireless Dual Band A+B PC Card WPC51AB

Рис. 8.3. Беспроводной USB-адаптер Linksys Wireless-B USB Adapter WUSB11

Если идет речь о подключении к беспроводной сети персонального компьютера, спектр возможных решений существенно расширяется. В частности, можно ис-

пользовать не только внутренние адаптеры с шиной PCI, но и внешние USB-адаптеры, не требующие отдельного источника электропитания. На рис. 8.3 показан один из таких адаптеров.

Беспроводной Ethernet-мост обеспечивает подключение к беспроводным сетям любого устройства, снабженного адаптером обычной кабельной сети, а также целых сегментов кабельных локальных сетей. Образец подобного устройства показан на рис. 8.4.

Рис. 8.4. Так выглядит беспроводной Ethernet-мост, существенно расширяющий возможности беспроводных сетей

Практически все современные ноутбуки оборудованы интегрированными адаптерами Wi-Fi. Это сильно облегчает дело, поскольку для подключения этого устройства к беспроводной сети потребуется лишь точка доступа. Интегрированные беспроводные адаптеры также являются неотъемлемой частью сетевых принтеров, цифровых фотокамер, а также многих других многофункциональных цифровых устройств.

При выборе точки доступа следует обратить внимание на ее надежность, простоту в обслуживании и защищенность от хакерских атак. Если точка доступа используется в локальной сети масштаба предприятия, в качестве промежуточного звена следует использовать коммутатор, а не концентратор, поскольку объем собственной памяти у точки доступа обычно невелик, из-за чего существует ограничение на максимальный размер внутренней таблицы физических адресов.

ВНИМАНИЕ Если в беспроводной сети предполагается использовать устройства, порождающие большой трафик (например, мультимедийные приложения), рекомендуется остановиться на выборе сетевого оборудования, совместимого со стандартами IEEE 802.11a и IEEE 802.11g. При этом скорость передачи данных в беспроводных сетях будет достигать 54 Мбит/с.

Существует ряд специализированных устройств, поддерживающих беспроводные подключения, причем их ассортимент постоянно растет. Так, например, в настоящее время появились *серверы печати*, с возможностью беспроводного подключения. Эти серверы очень удобно применять, если парк компьютерной техники состоит преимущественно из портативных ноутбуков, снабженных беспроводными адаптерами. Существуют также *видеопроекторы* с возможностями беспроводного доступа. Благодаря этим устройствам можно легко и быстро организовать дистанционное управление презентациями. Если требуется организовать

совершенную систему видеонаблюдения, можно воспользоваться видеокамерой с беспроводным подключением.

А теперь нужно рассмотреть ключевые моменты настройки беспроводных сетей.

Настройка беспроводных сетей: общие положения

В процессе настройки беспроводных сетей следует учитывать несколько важных аспектов.

- Профиль. Для обеспечения работы в разнородных беспроводных средах формируются *профили*, в которых содержится самая разнообразная информация, как, например, сведения о режиме работы, имя сети, занимаемый диапазон частот, а также параметры шифрования.
- Имя беспроводной сети (SSID, Servise Set ID). В нем указывается общий идентификатор для конкретной беспроводной сети, который не стоит путать с названием рабочей группы Microsoft.
- Шифрование данных.

В процессе определения используемого шифрования данных выбирается режим шифрования с применением 64- или 128-разрядного ключа. Можно также вообще отказаться от шифрования, хотя этого делать не рекомендуется, поскольку в беспроводных сетях велика вероятность перехвата трафика. При выборе между 64- и 128-разрядным ключами шифрования рекомендуется обратить внимание именно на 128-разрядную версию, хотя, в конечном счете, все определяется возможностями используемого оборудования.

Ключ шифрования задается непосредственно или генерируется при помощи кодового слова.

Параметр, определяющий используемый диапазон частот (частотный канал), обычно задается самой точкой доступа. Чаще всего настройка на используемый диапазон частот производится автоматически. Если же точка доступа не используется, то номер частотного канала выбирается на каждом компьютере отдельно.

Следует обратить внимание на то, что сети, работающие в диапазоне частот 2,4 ГГц (стандарт IEEE 802.11b), подвержены влиянию помех, излучаемых бытовыми приборами. Если подобные помехи имеют место, следует изменить применяемый диапазон частот, выбрав другой номер частотного канала.

Поскольку безопасность в беспроводных сетях находится под постоянной угрозой, этому вопросу следует уделять повышенное внимание. В частности, следует выполнить следующие процедуры:

- изменить имя сети, заданное по умолчанию;
- запретить для точки доступа трансляцию имени сети, если необходимость в этом отсутствует;
- изменить имя и пароль администратора точки доступа, заданные по умолчанию;

- установить максимально возможный уровень шифрования, даже если это негативно скажется на производительности беспроводной сети;
- сгенерировать уникальный ключ шифрования;
- доверить работу с ключами шифрования одному человеку, исполняющему роль системного администратора;
- ограничить доступ к беспроводной сети компьютерами с заранее определенными физическими (MAC) адресами;
- ограничить время действия ключей, особенно в случае гостевого доступа.

Если нужно поддерживать безопасность беспроводной сети на достойном уровне, то следует регулярно изменять значения следующих параметров:

- ключи шифрования;
- имя сети;
- имя и пароль администратора.

Обеспечивая безопасность беспроводной сети, не следует забывать об остальных аспектах информационной безопасности. Нужно использовать комплексный подход, охватывающий все стороны проблемы.

ПРИМЕЧАНИЕ Проблемы обеспечения безопасности в локальных сетях подробно рассматриваются в десятой главе.

Обеспечение безопасности в беспроводных сетях

Функции защиты протокола 802.11 реализованы на базе службы аутентификации и шифрования. Функция шифрования основана на технологии Wired Equivalent Privacy (WEP). Эта технология реализована в службах безопасности, используемых для защиты беспроводных сетей стандарта 802.11 от несанкционированного доступа, как это часто бывает, например, в случае несанкционированного перехвата сетевого трафика. В процессе автоматической настройки беспроводной сети можно определить использование сетевого ключа для шифрования данных, передаваемых по сети. Если активизирована процедура шифрования данных, то будут созданы общие секретные ключи шифрования, используемые передающей и получающей станциями для изменения сетевых фреймов, благодаря чему исключается перехват данных.

В протоколе 802.11 поддерживаются две категории сетевых служб проверки подлинности: *открытая система* и *общий ключ*. Если выбран тип проверки подлинности *открытая система*, то процедуру аутентификации может инициировать любая беспроводная станция. В процессе проверки станция-субъект отсылает особый фрейм, содержащий идентификатор отправляющей станции. Получающая станция возвращает фрейм, в котором определяется, была ли выполнена ли идентификация отправляющей станции.

Если же осуществляется проверка подлинности типа *общий ключ*, то каждая беспроводная станция должна получить общий секретный ключ по защищенному каналу, независимому от канала беспроводной сети 802.11. Если применяется проверка подлинности типа *Общий ключ*, требуется использовать именно сетевой ключ.

Применение сетевого ключа в целях шифрования возможно только в том случае, когда активизирован и выполняется протокол WEP. Этот ключ может предоставляться пользователю автоматически, в противном случае его следует ввести вручную. При ручном вводе ключа можно определить его длину (40 бит или 104 бит), формат ключа (символы ASCII или шестнадцатеричные цифры), а также индекс ключа, то есть место, где хранится указанный ключ. С ростом длины ключа повышается надежность шифрования.

В соответствии с протоколом IEEE 802.11 в беспроводной станции может быть задано до четырех ключей со значениями индекса 0, 1, 2 и 3. При этом в сообщении указывается индекс ключа, использованного для шифрования тела сообщения. Принимающая точка доступа или беспроводная станция имеет возможность извлечь ключ, хранящийся в индексе ключа, и использовать его для расшифровки зашифрованного сообщения.

Проверка подлинности 802.1x

Если требуется повышенная степень безопасности, можно воспользоваться проверкой подлинности IEEE 802.1x. Протокол проверки подлинности IEEE 802.1x позволяет осуществлять доступ с проверкой подлинности к беспроводным сетям 802.11 и кабельным сетям Ethernet. При этом осуществляется идентификация пользователя и компьютера, а также централизованная проверка подлинности и динамическое управление ключами. Благодаря протоколу IEEE 802.1x минимизируется ряд угроз безопасности беспроводных сетей, таких как, например, несанкционированный доступ и перехват данных. В протоколе IEEE 802.1x поддерживается служба Internet Authentication Service (IAS, служба удаленной идентификации в Интернете), реализующая протокол Remote Authentication Dial-In User Service (RADIUS, служба удаленной идентификации подключающегося пользователя).

При использовании данного протокола точка беспроводного доступа, использующая RADIUS, отправляет запрос на подключение и сообщения с учетными данными центральному серверу RADIUS. Центральный сервер RADIUS после обработки позволяет принять или отклонить запрос на подключение. Если запрос разрешен, то подлинность клиента считается установленной, и для данного сеанса могут быть созданы уникальные ключи в зависимости от выбранного метода проверки подлинности. Поддержка протоколом IEEE 802.1x защиты, реализованной с помощью протокола Extensible Authentication Protocol (EAP), позволяет использовать такие методы установления подлинности, как смарт-карты, сертификаты и алгоритм выборки сообщения Message Digest 5 (MD5).

При проверке подлинности в протоколе IEEE 802.1x имеется возможность указать, выполняется ли проверка подлинности при доступе к сетевым ресурсам в зависимости от того, зарегистрировался ли пользователь в системе или нет.

Например, операторы центра данных, управляющие удаленными серверами, могут указать, что серверы должны выполнять проверку подлинности при доступе к сетевым ресурсам. Кроме того, можно указать, следует ли выполнять попытки подключения к сети, если сведения о пользователе или компьютере недоступны. Например, провайдеры (ISP) могут использовать данный способ проверки подлинности для доступа пользователей к тем или иным сервисам. Компания может предоставлять посетителям ограниченный гостевой доступ, дающий возможность доступа к Интернету, но не к конфиденциальным сетевым ресурсам.

В процессе проверки доступа к сети порт может работать как *идентификатор* или *соискатель*. Роль идентификатора предусматривает проверку подлинности перед предоставлением пользователю доступа к службам через данный порт. Если же порт работает как соискатель, он запрашивает доступ к службам через порт-идентификатор. *Сервер проверки подлинности*, расположенный на отдельном компьютере или на одном компьютере с идентификатором, проверяет учетные данные соискателя от имени идентификатора. Затем сервер отвечает идентификатору, указывая, прошел ли соискатель проверку подлинности, требуемую для доступа к службам идентификатора.

Механизм контроля сетевого доступа на основании порта определяет две *логические точки доступа* к сети, используя единственный физический сетевой порт. Первая логическая точка доступа, которую называют неконтролируемым портом, допускает обмен данными между идентификатором и другими компьютерами или сетью вне зависимости от того, была ли проведена авторизация. Вторая логическая точка доступа, называемая контролируемым портом, допускает обмен данными между авторизованным пользователем сети и идентификатором.

ПРИМЕЧАНИЕ Подробнее протокол RADIUS рассматривается в главе 10.

Для установки протокола проверки подлинности 802.1x нужно выполнить несложную последовательность действий.

1. Открыть папку Сетевые подключения.
2. Правой кнопкой щелкнуть мыши на том соединении, для которого требуется включить или отключить протокол проверки подлинности 802.1x, после чего в контекстном меню выбрать пункт Свойства (рис. 8.5).
3. Перейти на вкладку Проверка подлинности.
4. Если требуется задействовать проверку подлинности IEEE 802.1x для данного соединения, то нужно взвести флажок Разрешить проверку подлинности IEEE 802.1x. По умолчанию этот флажок не установлен.
5. В поле Тип EAP следует выбрать тип протокола расширенной проверки подлинности (EAP), который будет использоваться для данного соединения.
6. Если в поле Тип EAP выбрано значение Смарт-карта или иной сертификат, можно настроить дополнительные параметры, нажав кнопку Свойства и перейдя на вкладку Свойства смарт-карты или другого сертификата.
7. Если при проверке подлинности будет использоваться сертификат, расположенный на смарт-карте, нужно взвести флажок Использовать мою смарт-карту.

8. Если при проверке подлинности будет использоваться сертификат, расположенный в хранилище сертификатов на компьютере, требуется взвести флажок Использовать сертификат на этом компьютере.
9. Для проверки действительности сертификата, находящегося на данном компьютере, нужно взвести флажок Проверять сертификат сервера. Требуется указать, следует ли устанавливать соединение только при условии, что сервер принадлежит к определенному домену, а затем определить доверенный корневой центр сертификации.
10. Чтобы использовать для подключения другое имя пользователя в случае, если имя пользователя в смарт-карте или сертификате отличается от имени пользователя домена, в который выполняется вход, нужно взвести флажок Использовать для подключения другое имя пользователя.

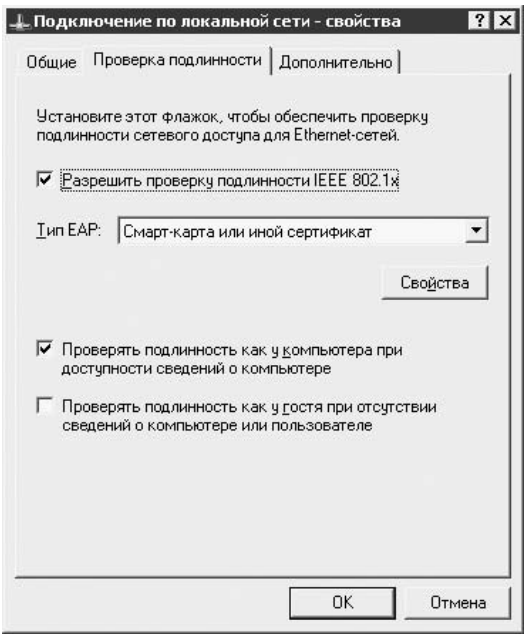


Рис. 8.5. Активизация процедуры проверки подлинности IEEE 802.1x

Для определения процедуры проверки подлинности в сети, если пользователь не зарегистрировался в системе и сведения о компьютере пользователя недоступны, нужно выполнить еще одну последовательность действий.

1. Если пользователь не зарегистрировался в системе, то для выполнения проверки подлинности в сети нужно взвести флажок Проверять подлинность как у компьютера при доступности сведений о компьютере.
2. Если сведения о пользователе и компьютере недоступны, то для выполнения проверки подлинности нужно взвести флажок Проверять подлинность как у гостя при недоступности сведений о компьютере.

Установка и настройка беспроводных сетей в Windows XP

В Windows XP по сравнению с предыдущими версиями Windows значительно улучшилась поддержка беспроводных сетей. В следующем списке указаны дополнительные возможности, предоставляемые этой системой.

- Имеется встроенная поддержка WPA. Все требуемые параметры настройки определяются на вкладке свойств соединения.
- Появился мастер настройки беспроводной сети, позволяющий до предела упростить необходимую настройку, которая выполняется в автоматическом режиме. И что самое приятное, параметры настройки могут сохраняться на чипе Flash-памяти, что упрощает настройку нескольких рабочих станций.
- Появилась служба Wireless Zero Configuration, которая обеспечивает обнаружение и подключение к беспроводным сетям, заранее указанным в списке предпочтительных сетей. Весь процесс установки соединения протоколируется, благодаря чему упрощается устранение проблем и их последствий.

Для установки беспроводной сети достаточно запустить на выполнение мастер установки беспроводной сети, доступ к которому обеспечивается из папки Сетевые подключения.

Установка и настройка программных мостов

Вообще говоря, беспроводной или обычный *сетевой мост* определяет способ, использующийся для объединения отдельных сегментов локальной сети. Как правило, для объединения нескольких сетевых сегментов используется маршрутизация или соединение при помощи мостов. Метод IP-маршрутизации уже рассматривался ранее, и в современных сетях он применяется чаще всего. Однако его практическая реализация сопряжена с дополнительными материальными затратами, поскольку требует установки аппаратных или программных маршрутизаторов и настройки IP-адресов для каждого отдельного компьютера или сегмента локальной сети. Этот метод идеально подходит в случае больших корпоративных сетей, поскольку именно в подобных случаях требуется масштабируемость, а также присутствует квалифицированный персонал, который в состоянии выполнить все необходимые работы, связанные с настройкой процедуры маршрутизации. Если же воспользоваться таким устройством, как мост, то IP-маршрутизация будет не нужна. Но потребуется приобрести дополнительное устройство, то есть сам аппаратный мост.

ПРИМЕЧАНИЕ Подробное описание физических сетевых компонентов, в том числе и мостов, можно найти в пятой главе.

Вполне естественно, что в небольших сетях в силу ряда причин использование аппаратных мостов либо IP-маршрутизации нецелесообразно.

Каков же выход из сложившейся ситуации? Если вы работаете в среде Windows XP, то можно воспользоваться *программным сетевым мостом*. Для установки этого программного компонента, объединяющего сегменты локальных сетей, следует выделить значки соответствующих сетевых подключений, а затем выполнить команду Подключения типа мост. Созданный ранее мост можно активизировать повторно, а также добавлять к нему иные сетевые подключения.

Благодаря программному сетевому мосту легко реализуется управление отдельными сетевыми сегментами, а также формируется единая подсеть для всей сети. Причем все это происходит в автоматическом режиме, не требующем дополнительной настройки. Также следует учитывать экономию средств, поскольку отсутствует необходимость в установке дополнительных сетевых модулей. К тому же, если установлена единственная подсеть, радикально упрощается IP-адресация и разрешение имен.

Функции сетевого моста заключаются в том, чтобы создавать подключения между сетевыми средами разных типов. Так, например, если требуется, чтобы в обычной локальной сети мирно сосуществовали различные сетевые среды, то для каждой такой среды формируется своя собственная подсеть, а затем с помощью сетевого моста реализуется пересылка сетевых пакетов между отдельными подсетями. Необходимость обмена пакетами связана с тем, что в различных сетевых средах выполняются совершенно разные сетевые протоколы. Благодаря сетевому мосту автоматизируется процесс настройки конфигурации, необходимой для передачи данных из среды одного типа в среду другого типа.

В среде операционной системы Windows XP поддерживается единственный сетевой мост, но в его состав может входить любое количество сетевых подключений.

ПРИМЕЧАНИЕ В процессе пересылки сетевых пакетов сетевой мост использует алгоритм связующего дерева (STA, spanning tree algorithm). Благодаря этому алгоритму можно избежать «зацикливания» передаваемых данных, поскольку возможно автоматическое отключение передачи данных через мост для отдельных портов.

Для объединения подключений с формированием моста нужно выполнить простую последовательность операций.

1. Открыть окно Сетевые подключения.
2. Перейти к списку ЛВС или высокоскоростной Интернет, в котором нужно выбрать все частные сетевые подключения, которые будут включены в состав данного моста.
3. Щелкнуть правой кнопкой мыши на одном из выделенных сетевых подключений и выполнить команду Подключения типа мост. Для создания сетевого моста следует предварительно выделить как минимум два сетевых подключения (рис. 8.6).

ПРИМЕЧАНИЕ Для получения доступа к папке Сетевые подключения следует зарегистрироваться в системе с учетной записью администратора, затем нажать кнопку Пуск, после чего выбрать в меню пункт Панель управления, а затем дважды щелкнуть на значке Сетевые подключения.

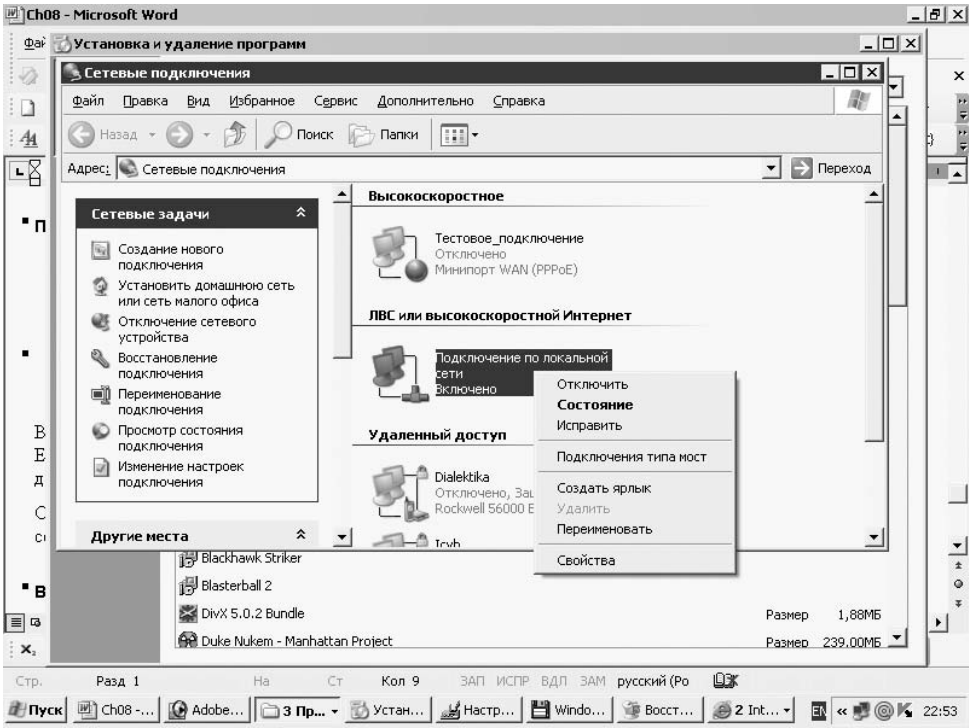


Рис. 8.6. Создание сетевого моста на основе нескольких подключений

В состав сетевого моста можно включать адаптеры Ethernet, IEEE 1394, а также иные совместимые с Ethernet адаптеры, такие как беспроводные адаптеры или адаптеры, предназначенные для домашних сетей на основе обычной телефонной линии.

ВНИМАНИЕ Если на компьютере установлена операционная система Windows 2000 или более ранняя версия, то установка и настройка моста невозможна.

Если из сетевого моста удалить все сетевые адаптеры, то мост не сможет функционировать в обычном режиме, хотя по-прежнему будет использовать системные ресурсы компьютера. Также следует учитывать, что сетевые мосты, содержащие лишь беспроводные подключения или подключения IEEE-1394, поддерживают передачу трафика исключительно через Internet Protocol версии 4 (IPv4).

Для добавления сетевого подключения к уже существующему мосту нужно выполнить простую последовательность действий.

1. Открыть папку Сетевые подключения.
2. Активировать список Сетевой мост, щелкнуть правой кнопкой мыши на пункте Сетевой мост и выбрать пункт Свойства.
3. В группе Адаптеры перейти на вкладку Общие, выделить добавляемые адаптеры и нажать кнопку OK.

Настройка клиентов беспроводных сетей

Благодаря механизмам автоматической настройки беспроводных сетей, имеющихся в Windows XP, обеспечивается простая настройка беспроводных сетей стандарта IEEE 802.11, а также сводятся к минимуму усилия, необходимые для настройки доступа к беспроводной сети. Благодаря режиму автоматической настройки беспроводной сети можно легко перемещаться между различными беспроводными сетями. При этом не требуется изменять параметры сетевого подключения для каждой сети. При перемещении в зону действия другой сети служба автоматической настройки проводит поиск доступных беспроводных сетей и извещает пользователя о появлении новой сети, доступной для подключения. После выбора беспроводной сети, подключение к которой следует установить, служба автоматической настройки изменяет параметры настройки адаптера беспроводной сети, а также пытается выполнить подключение.

На этом рассмотрение настройки беспроводных сетей завершается. Следующие две главы посвящены важной и интересной теме — интеграции локальных вычислительных сетей и Интернета.

Локальные сети и Интернет

В двух главах, входящих в эту часть книги, рассматриваются локальные сети и Интернет. В девятой главе можно узнать о том, как следует настраивать подключение удаленного доступа в среде Windows 2000 Server (Windows XP). Материал десятой главы посвящен важнейшим вопросам обеспечения безопасности в локальных сетях, подключенных к Интернету.

9 ГЛАВА Настройка удаленного доступа в Windows 2000/XP

Стоит начать с рассмотрения настройки удаленного доступа в Windows 2000 Server, а затем перейти к рассмотрению некоторых особенностей настройки и использования систем удаленного доступа в Windows XP.

ПРИМЕЧАНИЕ Поскольку операционные системы Windows 2000 Server и Windows XP являются «ближайшими родственниками», принципы удаленного доступа, применяемые для этих операционных систем, весьма схожи. Конечно, Windows XP обладает расширенным набором возможностей удаленного доступа, включая управление удаленными рабочими столами, о чем будет рассказано немного позже. Ну а пока нужно рассмотреть основные службы и протоколы удаленного доступа, применяемые в среде Windows 2000 Server.

Удаленный доступ в Windows 2000 Server

В среде Windows 2000 Server автоматическая установка связи клиентских компьютеров с сервером Windows 2000 Server обеспечивается при помощи *службы RAS* (Remote Access Service, Служба удаленного доступа). Эта служба позволяет устанавливать связь с удаленными сетями, включая Интернет. При этом компьютеры, работающие под управлением Windows 2000, могут исполнять роль сервера удаленного доступа для удаленных клиентов. *Служба маршрутизации и удаленного доступа* (RRAS, Routing and Remote Service) позволяет Windows 2000 Server исполнять роль маршрутизатора. Службы RAS и RRAS в Windows 2000 Server объединены в один сервис.

Благодаря *удаленному доступу* компьютер-клиент может подключаться к дистанционному компьютеру или к сети для получения доступа к вычислительным ресурсам так, как будто эти компоненты являются локальными. Например, пользователи, которые часто находятся в разъездах, могут легко получить удаленный

доступ к файлам, расположенным на корпоративном сервере, и к другим ресурсам корпоративной сети. Клиенты могут также использовать службы удаленного доступа для подключения к общедоступной сети, например к Интернет.у На рис. 9.1 показан принцип организации удаленного доступа.

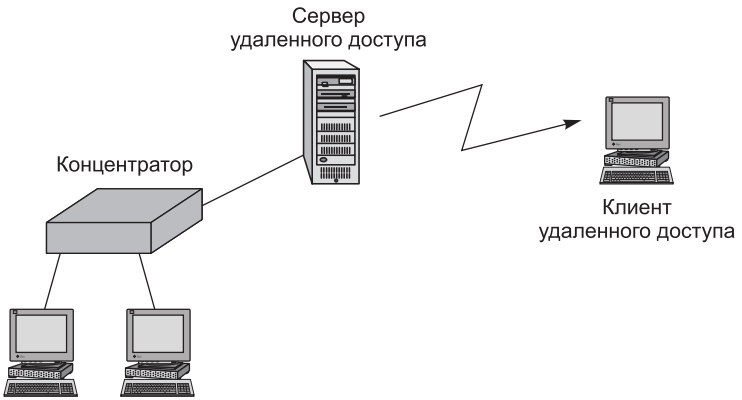


Рис. 9.1. Принцип функционирования удаленного доступа

ВНИМАНИЕ Если на компьютере Windows XP выполняется служба RRAS, он также будет исполнять роль сервера удаленного доступа.

В следующем списке перечислены три основных функции, выполняемые службой RRAS в среде Windows 2000 (Windows XP).

- Дистанционный клиент. Служба RRAS может применяться для создания и поддержки подключения к удаленным сетям при помощи различных средств (модем, ISDN- и DSL-линии, выделенная линия, инфракрасный и параллельный порты, протокол X.25, а также асинхронный режим передачи ATM). Клиенты Windows 2000 поддерживают достаточно большой перечень протоколов аутентификации и другие параметры подключения, которые будут рассмотрены в следующих разделах главы. Благодаря наличию протоколов *туннельного подключения* для клиентов можно настраивать безопасные подключения к удаленным сетям.
- Сервер удаленного доступа. Компьютер, на котором выполняется ОС Windows 2000, может выступать в качестве *сервера удаленного доступа*. В этом случае дистанционные клиенты могут подключаться к локальному серверу или к локальной сети, используя компоненты, применяемые для поддержки коммутируемых подключений. Для поддержки клиентской службы терминалов можно использовать службы удаленного доступа, поскольку они генерируют IP-адрес для клиентского подключения и задают необходимые протоколы. Операционная система Windows 2000 поддерживает несколько протоколов аутентификации, в результате чего становится возможной аутентификация пользователей, основанная на учетных записях локального пользователя или пользователя домена. В качестве механизма аутентификации может также применяться протокол RADIUS (Remote Authentication Dial In User Service, служба удаленной аутентификации пользователей коммутируемого подключения).

- Службы маршрутизации. Компоненты маршрутизации позволяют серверу Windows 2000 выступать в качестве однонаправленного или многоадресного маршрутизатора. Сервер Windows 2000 обеспечивает выполнение маршрутизации, фильтрование пакетов, подключение к ресурсам общего доступа, коммутируемую маршрутизацию, а также некоторые другие возможности.

Служба RRAS Windows 2000 предоставляет пользователю удаленный доступ, а также поддерживает службу маршрутизации. В более ранних версиях Windows NT Server эти возможности реализовывались при помощи отдельных служб. Служба RRAS в Windows 2000 претерпела значительные усовершенствования и дополнения по сравнению с аналогичной службой в Windows NT.

Одним из основных положительных качеств службы RRAS Windows 2000 является ее интегрированность в состав операционной системы Windows 2000. Для клиента это означает, что ему достаточно один раз создать подключение, после чего доступ к ресурсам сервера обеспечивается в точно таком же режиме, как если бы они находились на локальном компьютере. Клиент может составить схему удаленных ресурсов общего доступа на локальном диске, схему удаленных принтеров, а также выполнять многие другие действия. Иногда приложения могут непосредственно использовать удаленные ресурсы.

Применительно к серверу, интеграция означает, что Windows 2000 может применять единый метод идентификации для локальных и удаленных пользователей. Служба Windows 2000 выполняет аутентификацию, основываясь на учетных записях пользователей на локальном компьютере или учетных записях в домене. В этих целях также может применяться служба RADIUS. При поддержке RADIUS служба RRAS обеспечивает возможность использования сервера Windows 2000 в качестве шлюза для различных сетей, причем процедура аутентификации будет выполняться другим сервером. В качестве сервера аутентификации может применяться даже сервер UNIX.

Служба RRAS Windows 2000 полностью интегрирована со службой каталогов Active Directory. Тем самым обеспечивается выполнение репликации настроек параметров удаленного доступа пользователя, включая разрешения на доступ, параметры обратного вызова, политики безопасности и некоторые другие параметры. х администрирования при использовании других служб и свойств, которые связаны со службой каталогов Active Directory.

Следует отметить, что служба RRAS Windows 2000 поддерживает большое количество протоколов удаленного доступа, в том числе наиболее популярные в настоящее время протоколы SLIP и PPP. Эта служба поддерживает такие методы аутентификации, как MS-CHAP, протокол CHAP (Challenge Handshake Authentication Protocol, протокол проверки подлинности с предварительным согласованием вызова), протокол SPAP (Shiva Password Authentication Protocol, протокол проверки подлинности пароля Shiva) и протокол PAP (Password Authentication Protocol, протокол проверки подлинности пароля).

Как отмечалось выше, служба RRAS Windows 2000 связана со службой каталогов Active Directory. Благодаря этому клиенты могут настраивать репликации с помощью расширенного доступа для клиентов и упрощенных методов админи-

стрирования. Интеграция со службой каталогов Active Directory позволяет управлять сложными серверами RRAS с помощью консоли управления RRAS.

Используя *протоколы BAP* (Bandwidth Allocation Protocol, протокол выделения полосы пропускания) и *BACP* (Bandwidth Allocation Control Protocol, протокол управления выделением полосы пропускания), служба Windows 2000 RAS может в динамическом режиме регулировать полосу пропускания. Если полоса пропускания становится недостаточной, служба RAS добавляет дополнительные каналы связи, в результате чего увеличивается скорость загрузки данных, а также растет производительность. Протокол BAP можно настраивать с помощью политики удаленного доступа, которую следует применять к отдельным пользователям, группам или ко всей организации в целом.

Ранние версии службы удаленного доступа (в Windows NT) поддерживали *протокол MS-CHAP* (Microsoft Challenge Handshake Authentication, протокол для проверки подлинности удаленного клиента). *Протокол MS-CHAP версии 2* обеспечивает высокий уровень безопасности и предназначается для поддержки подключения к *виртуальной частной сети* (VPN, Virtual Private Network). Таким образом, удаленный клиент может устанавливать безопасное подключение к частной сети через Интернет. Протокол CHAP версии 2 поддерживает несколько способов повышения безопасности.

Шифрование ответа LAN Manager, используемое для обеспечения обратной совместимости с устаревшими клиентами удаленного доступа, теперь не поддерживается. Благодаря этому совершенствуется система обеспечения безопасности. Исходя из этих же соображений, протокол MS-CHAP версии 2 не поддерживает шифрование изменения пароля LAN Manager.

Протокол MS-CHAP версии 2 поддерживает двустороннюю аутентификацию, что позволяет обеспечивать двунаправленную проверку подлинности между клиентом и сервером удаленного доступа. Ранее протокол MS-CHAP поддерживал только однонаправленную аутентификацию, а также не предоставлял удаленному клиенту механизм, позволяющий определить, действительно ли удаленный сервер обладает доступом к паролю для выполнения аутентификации.

Протокол MS-CHAP версии 2 также позволяет шифровать данные. Алгоритм 40-разрядного шифрованиия в предыдущих версиях содержал пользовательские пароли, а результат использования одного и того же ключа шифрования был общим для каждого сеанса. В версии 2 этого протокола для создания уникального ключа кодирования каждого сеанса используется пароль удаленного клиента наравне с произвольно выбранной строкой.

Во второй версии протокола обеспечивается большая степень безопасности в процессе передачи данных благодаря использованию отдельных ключей шифрования для пересылаемых данных каждого каталога.

ПРИМЕЧАНИЕ Подробнее методы шифрования рассматриваются в десятой главе.

Протокол EAP (Extensible Authentication Protocol, расширенный протокол аутентификации) обеспечивает выполнение аутентификации. Протокол EAP позволяет клиенту и серверу согласовывать механизм, применяемый в целях

проверки подлинности клиента. В настоящее время протокол EAP в Windows 2000 поддерживает протоколы EAP-MD5 CHAP (Challenge Handshake Authentication Protocol), EAP-TLS (Transport Level Security, безопасность на уровне передачи), а также переадресацию сервера RADIUS. Каждый из перечисленных протоколов будет более подробно рассмотрен в следующих разделах главы.

Служба RRAS Windows 2000 может работать как клиент RADIUS, отсылать запросы на регистрацию в системе серверу RADIUS, который поддерживает службу IAS (Internet Authentication Service, служба аутентификации в Интернете), входящую в состав Windows 2000. Сервер RADIUS может выполняться не только на платформе Windows 2000, что позволяет службе RRAS использовать серверы RADIUS UNIX или службы RADIUS от других поставщиков. Одним из преимуществ применения службы RADIUS является поддержка аудита. Появились также дополнительные утилиты, которые обеспечивают интеграцию с базами данных, например для контроля доступа клиентов.

В Windows 2000 значительно улучшены административные возможности контроля учетных записей удаленных пользователей и параметров коммутируемого подключения. Служба RAS позволяет контролировать только параметры обратного вызова и параметры канала связи между клиентами. Хотя Windows 2000 позволяет устанавливать разрешения удаленного доступа при помощи учетных записей пользователя, эту политику можно также использовать для определения параметров удаленной учетной записи для одного или нескольких пользователей. Политики удаленного доступа обеспечивают великолепные возможности контроля параметров пользователей и таких характеристик, как разрешенное время доступа, максимальная продолжительность сеанса, аутентификация, безопасность, политики BAP и многое другое.

В Windows 2000 появилась поддержка удаленных учетных записей для клиентов Macintosh, реализованная при помощи поддержки сети AppleTalk для протокола PPP. Это позволяет клиентским системам Macintosh подключаться к серверу RAS Windows 2000 при помощи стандартного протокола подключения «точка-точка» в сети AppleTalk.

В службе RAS Windows 2000 за счет блокировки учетной записи была улучшена степень безопасности. В результате после определенного количества неудачных попыток регистрации в системе обеспечивается блокирование учетной записи службы удаленного доступа. Данный параметр позволяет защититься от атак хакеров, которые пытаются получить доступ к удаленной учетной записи, многократно регистрируясь в системе (метод атаки со словарем). Можно настроить два параметра для контроля блокировки — количество неудачных попыток, приводящих к блокированию учетной записи, и период, когда учетная запись будет оставаться заблокированной до обнуления счетчика блокировки.

Маршрутизация и удаленный доступ

Большинство административных и управляющих функций интегрированы Microsoft в оснастку консоли управления MMC. Это касается и службы RRAS. Благодаря оснастке Маршрутизация и удаленный доступ (рис. 9.2) можно выполнять первичную настройку сервера RRAS и изменять параметры его работы.

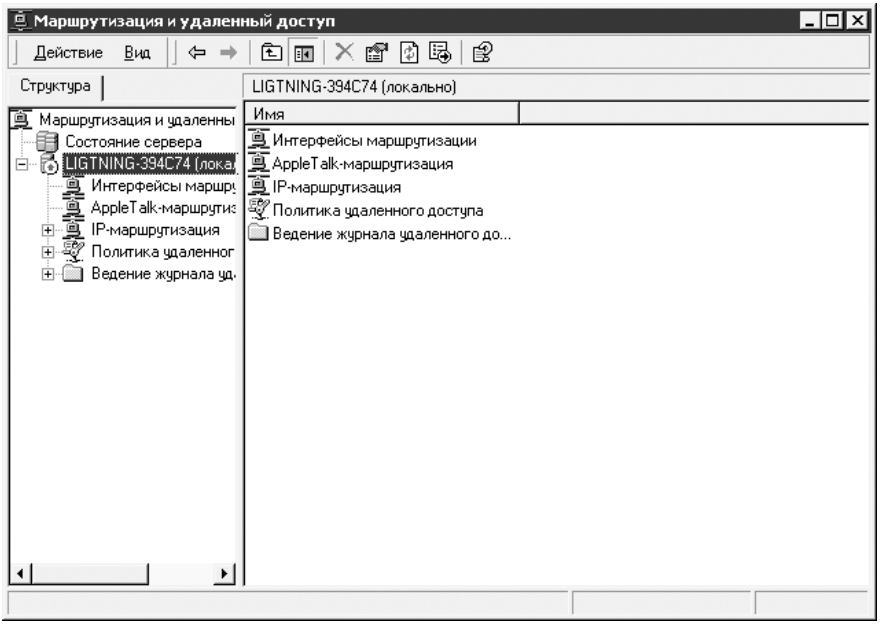


Рис. 9.2. Оснастка консоли MMC, выполняющая функции маршрутизации и удаленного доступа

Протоколы удаленного доступа

В Windows 2000 поддерживается несколько протоколов подключений и служб удаленного доступа, которые следует рассмотреть достаточно подробно.

ВНИМАНИЕ Эти же протоколы были унаследованы системой Windows XP.

Протокол SLIP (Serial Line Internet Protocol, межсетевой протокол для последовательного канала) широко применялся еще в первых версиях UNIX. Набор присущих ему функций весьма невелик, и отсутствует коррекция ошибок. Клиенты Windows 2000 могут применять протокол SLIP для подключения к серверам, работающим под управлением UNIX, но Windows 2000 Server не поддерживает SLIP для коммутируемых подключений.

Протокол PPP (Point-to-Point Protocol, протокол подключения «точка-точка») изначально предназначался для использования в качестве унифицированного протокола, обеспечивающего высокую производительность и надежность. В отличие от SLIP, протокол PPP создавался на основе промышленных стандартов, поэтому любой хороший клиент может подключаться к PPP-серверу. В Windows 2000 поддерживается использование протокола PPP для входящих и исходящих подключений. В службе удаленного доступа Windows 2000 удаленные клиенты могут использовать протоколы IPX, TCP/IP, NetBEUI, AplleTalk и их комбинации. Клиенты, работающие под управлением Windows (Windows 2000, Windows NT, Windows 9x и Windows 3.x), могут использовать любую комбинацию из протоколов IPX, TCP/IP, NetBEUI, однако не могут применять протокол AppleTalk.

Клиенты Macintosh могут использовать либо протокол TCP/IP, либо протокол AppleTalk. Протокол PPP поддерживает несколько методов аутентификации, включая MS-CHAP, EAP, CHAP (Challenge Handshake Authentication Protocol, протокол аутентификации с предварительным согласованием вызова), SPAP и PAP.

Протоколы PPMP (PPP Multilink, многоканальный протокол подключения «точка-точка») и *BAP* позволяют использовать несколько линий PPP в целях расширения полосы пропускания. Например, можно воспользоваться протоколом Multilink в целях объединения двух аналоговых модемов со скоростью передачи данных 33,6 Кбит/с, что обеспечит суммарную скорость передачи данных в 67,2 Кбит/с.

Протокол BAP функционирует совместно с Multilink, формируя суммарную полосу пропускания. Как только полоса пропускания увеличивается, протокол BAP позволяет клиенту группировать дополнительные подключения для повышения общей производительности. Как только полоса пропускания уменьшается, протокол BAP позволяет клиенту удалять подключения, чтобы сгруппировать связи для уменьшения общей стоимости подключения.

Набор протоколов TCP/IP не может самостоятельно шифровать передаваемые данные, хотя при работе в такой незащищенной среде, как Интернет, необходимость в этом возникает крайне часто. В подобных случаях можно воспользоваться *протоколом PPTP* (Point-to-Point Tunneling Protocol, протокол туннелирования «точка-точка»), который обеспечивает создание безопасного «туннеля» в Интернете с последующей передачей по нему зашифрованных IP-пакетов. Протокол PPTP появился в результате эволюции протокола PPP и предназначается для создания виртуальных частных сетей (VPN, Virtual Private Network), объединяющих в единое целое серверы и клиентские компьютеры.

ПРИМЕЧАНИЕ Подробнее виртуальные частные сети рассматриваются в конце этой главы. Там же описывается пример создания частной виртуальной сети на платформе Windows XP.

Протокол PPTP может применяться для создания безопасного подключения частных сетей в том случае, когда в качестве среды передачи данных используется Интернет, а удаленная сеть не поддерживает протокол IPSec.

Протокол L2TP (Layer Two Tunneling Protocol, двухуровневый протокол туннелирования) обладает свойствами протокола PPTP, а также поддерживает протокол IPSec, благодаря чему обеспечивается повышенный уровень безопасности. В отличие от протокола PPTP, который в процессе шифрования использует стандарт MPPE, протокол L2TP полагается на стандарт IPSec. Поэтому при установке подключений исходный и целевой маршрутизаторы должны поддерживать протоколы как L2TP, так и IPSec.

Протокол L2TP, поддерживающий IPSec, обеспечивает повышенный уровень безопасности по сравнению с протоколом PPTP, поэтому при подключении к виртуальной частной сети этот протокол является наилучшим выбором.

Организация удаленного доступа для всех пользователей

Во многих небольших организациях или отделах крупных организаций пользователям требуется доступ к Интернету для работы с электронной почтой и просмотра некоторых сайтов. В этом случае предоставление каждому пользователю отдельного подключения вряд ли оправдано, поскольку повлечет за собой дополнительные затраты, связанные с организацией дополнительных учетных записей, а также с наличием издержек на администрирование. Поэтому, если используется система Windows 2000 Server, рекомендуется воспользоваться программой Internet Connection Sharing (ICS, общий доступ к подключению Интернета).

Компьютер с операционной системой Windows 2000, на котором установлен общий доступ к подключению Интернета, превращается в прокси-сервер, сервер имен и маршрутизатор для подключенных клиентов. Чаще всего он становится DHCP-сервером, выполняя функции назначения адресов компьютеров в сети. При организации общего доступа для назначения адресов используется пространство адресов класса C, 192.168.0.0 (маска подсети 255.255.255.0). Если разрешается общий доступ к подключению Интернета, Windows 2000 автоматически назначает адрес 192.168.0.0 сетевому интерфейсу, при помощи которого пользователи будут получать доступ к подключению.

Например, если на сервере установлен один сетевой адаптер и модем, то при использовании общего доступа IP-адрес сетевого адаптера изменится и получит значение 192.168.0.1. При включении других компьютеров им назначаются адреса из того же диапазона, причем адрес 192.168.0.1 будет выступать в качестве шлюза. Общий доступ к подключению Интернета предназначается для небольших офисных и домашних сетей, поэтому в нем отсутствуют расширенные возможности по настройке. Например, невозможно изменить диапазон адресов, выделяемый клиентам локальных сетей, отключить назначение адресов службой DHCP, отключить прокси-DNS и т. д. Однако для небольших сетей выбор ICS оказывается достаточно неплохим вариантом общего доступа к Интернету. Если требуется контроль на более высоком уровне или если в состав сети входят контроллеры доменов Windows 2000, DHCP-серверы или RAS-серверы, придется использовать преобразование сетевых адресов (NAT).

Настройка общего доступа к подключению Интернета в Windows 2000 Server

Активизация общего доступа к Интернету осуществляется при помощи диалогового окна свойств подключения в папке Сеть и удаленный доступ к сети. Как только будут настроены параметры подключения, а пользователь убедится в его работоспособности, нужно перейти в папку Сеть и удаленный доступ к сети. Правой кнопкой мыши нужно щелкнуть на значке подключения, а в отобразившемся контекстном меню выбрать пункт Свойства. В диалоговом окне свойств подключения следует активировать вкладку Общий доступ (рис. 9.3).

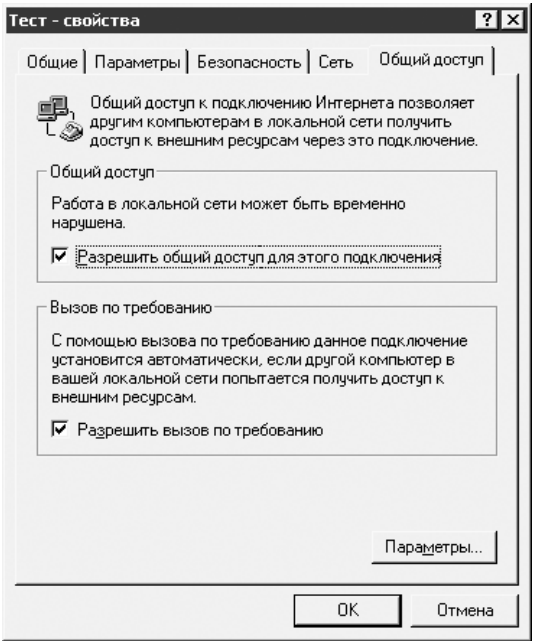


Рис. 9.3. В этом диалоговом окне настраивается общий доступ к подключению Интернета

Для организации общего доступа сначала создается подключение и производится его проверка. Как только подключение будет успешно протестировано, его можно настроить для совместного доступа пользователей локальной сети. Для настройки общего доступа к подключению Интернета нужно выполнить простую последовательность операций.

1. Открыть папку Сеть и удаленный доступ к сети, после чего активировать диалоговое окно свойств подключения. В данном случае речь идет о подключении к Интернету, а не к локальной сети.
2. Перейти на вкладку Общий доступ.
3. Установить флажок Разрешить общий доступ для этого подключения.
4. Установить флажок Разрешить вызов по требованию, если нужно, чтобы компьютер-посредник автоматически устанавливал подключение к Интернету при поступлении запроса от клиента.
5. Щелкнуть на кнопке Параметры, чтобы настроить все необходимые сетевые приложения и службы, или на кнопке OK, что приведет к разрешению передачи трафика без изменения.

Можно оптимизировать использование созданного подключения. Для этого нужно перейти на вкладку Параметры диалогового окна свойств подключения и указать значение параметра Время простоя до разъединения. Здесь можно, например, указать интервал времени, равный тридцати минутам. Многие провайдеры услуг Интернета разрывают подключение после простоя в течение 15–20 минут.

При подключении клиентов к ICS-серверу не требуется какое-либо специальное программное обеспечение. Достаточно лишь убедиться в том, что клиенты находятся в той же подсети, что и ICS-сервер, и что они обращаются к нему как к стандартному шлюзу. Для этого достаточно настроить клиенты на автоматическое получение настроек набора протоколов TCP/IP от DHCP-сервера.

Если требуется, можно настроить параметры компьютера-клиента вручную, назначив ему статический IP-адрес из диапазона адресов класса C (192.168.0.2–192.168.0.254) с маской подсети 255.255.255.0. В качестве стандартного шлюза следует использовать адрес 192.168.0.1.

Операционная система Windows 2000 Server позволяет настроить удаленные приложения для локальных клиентов и локальные службы для удаленных пользователей. Например, если в сети располагается веб-сайт, следует настроить параметры ICS таким образом, чтобы удаленные клиенты могли обращаться к соответствующей службе. Процесс настройки удаленных приложений и локальных служб достаточно прост. Для этого нужно лишь нажать кнопку Настройка на вкладке Общий доступ в окне свойств подключения.

Для настройки клиентов, получающих доступ из локальной сети к удаленным приложениям, нужно перейти на вкладку Приложения. Там следует нажать кнопку Установить для выбора соответствующего приложения. Все доступные в этом случае параметры перечислены в следующем списке.

- Имя приложения. В поле указывается имя приложения, которое будет отображаться на вкладке Приложения.
- Порты удаленного сервера. Требуется указать номер порта на удаленном сервере, который будет использоваться приложением.
- TCP. Этот флажок нужно взвести, если удаленный порт будет использовать протокол TCP.
- UDP. Этот флажок нужно взвести, если удаленный порт будет использовать протокол UDP.
- Порты входящих вызовов. В поле необходимо указать порты входящих вызовов для протокола TCP или UDP — для удаленного приложения.

Чтобы настроить доступ удаленных клиентов к локальным службам, например к веб-сайту, установленному в локальной сети, следует выбрать вкладку Службы и настроить необходимые параметры. Они перечислены в следующем списке.

- Имя службы. В поле указывается название службы, отображаемое на вкладке Службы.
- Номер порта службы. В поле задается номер порта, используемого службой.
- TCP. Этот флажок нужно взвести, если удаленный порт применяет протокол TCP.
- UDP. Этот флажок определяет использование протокола UDP.
- Имя или адрес сервера в частной сети. В поле указывается имя или IP-адрес локального компьютера, на котором выполняется служба.

Безопасность удаленного доступа

Обширная тема безопасности в локальных сетях в целом и безопасности удаленного доступа в частности рассматривается в следующей главе. Сейчас же нужно рассмотреть настройку удаленного доступа в среде Windows 2000 Server, позволяющую добиться максимального уровня безопасности.

Безопасность сервера RRAS обеспечивается при помощи настройки определенной политики. Управление политиками осуществляется через консоль RRAS. Для этого нужно выбрать настраиваемый сервер и открыть ветвь Политика удаленного доступа. При этом в правой части консоли отображаются установленные политики. По умолчанию используется политика Разрешить доступ, если разрешены входящие подключения. Нужно дважды щелкнуть на названии политики. Следует обратить внимание на то, что выбран переключатель Отказать в праве удаленного доступа.

Можно воспользоваться стандартной политикой удаленного доступа, просто добавляя к ней дополнительные компоненты, или создать новую политику.

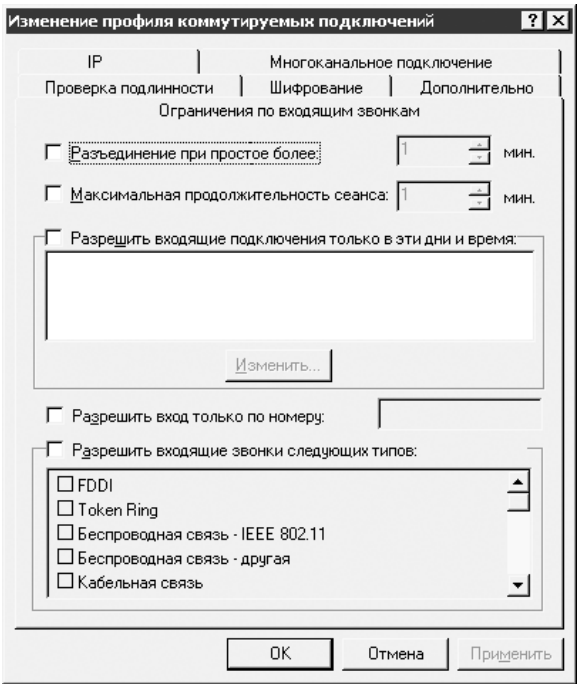


Рис. 9.4. Здесь можно изменять настройки коммутируемых подключений

Для создания новой политики в консоли RRAS нужно выбрать настраиваемый сервер и перейти к ветви Политика удаленного доступа. В контекстном меню правой панели нужно выполнить команду Создать политику удаленного доступа. После этого мастер предложит указать параметры настройки.

- Имя политики. В этом поле указывается имя политики, отображаемое в окне консоли RRAS. Можно ввести, например, название «Engineering».
- Условия. В этом окне определяются критерии, используемые для разрешения или запрета доступа. В рассматриваемом примере нужно нажать кнопку Добавить, выбрать команду Windows-Groups, а затем снова нажать кнопку Добавить. Останется лишь выбрать требуемую группу, дважды нажать кнопку OK, а затем нажать кнопку Далее.
- Предоставить/отказать в праве удаленного доступа. Если требуется отказать в праве удаленного доступа выбранной группе, следует взвести флажок Отказать в праве удаленного доступа, а затем нажать кнопку Далее.
- Изменить профиль. Эта кнопка позволяет изменять другие свойства политики удаленного доступа. Если ничего изменять не требуется, остается нажать кнопку Готово.

После щелчка на кнопке Изменить профиль будет отображено диалоговое окно Изменение профиля коммутируемых подключений (рис. 9.4). Расширенный набор параметров позволяет в широких пределах изменять свойства коммутируемых подключений.

Настройка удаленного доступа в среде Windows XP

Удаленный доступ в системе Windows XP настраивается почти так же, как и в системе Windows 2000 Server, за исключением некоторых особенностей, речь о которых пойдет в данном разделе.

Мастер создания подключения удаленного доступа позволяет не только создать новое подключение, но и установить домашнюю сеть, все компьютеры которой получают возможность общего доступа к Интернету. Также следует отметить, что любое создаваемое подключение удаленного доступа может быть защищено брандмауэром.

ВНИМАНИЕ Возможность подключения удаленного доступа имеется только в версии Windows XP Professional. Если же вы являетесь обладателем версии Windows XP Home Edition, забудьте о возможности удаленного подключения.

Установка нового подключения

Для установки нового подключения нужно нажать кнопку Пуск и выполнить команду Подключение ▸ Отобразить все подключения. В левой части отобразившегося окна нужно выбрать сетевую задачу Создание нового подключения. После этого появится диалоговое окно мастера создания новых подключений (рис. 9.5), которое позволяет подключить компьютер или частную сеть к Интернету или установить домашнюю сеть.

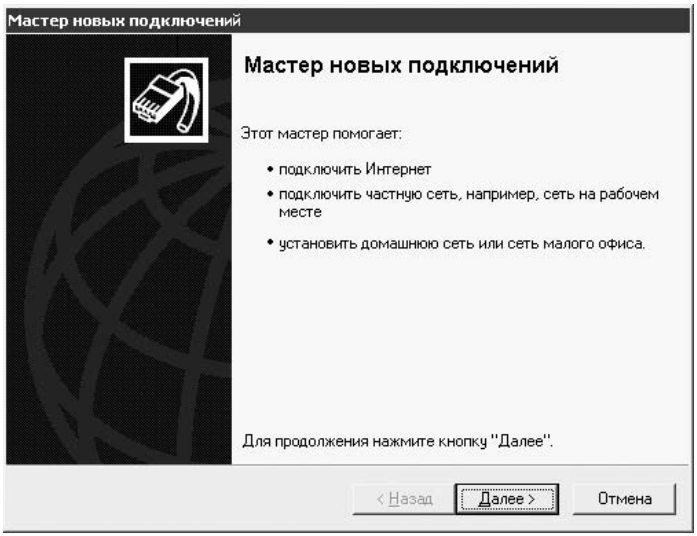


Рис. 9.5. Начальное окно мастера установки новых подключений

Подключение компьютера Windows XP к Интернету

Для подключения компьютера к Интернету в диалоговом окне типа сетевого подключения (рис. 9.6) следует взвести флажок Подключить к Интернету.

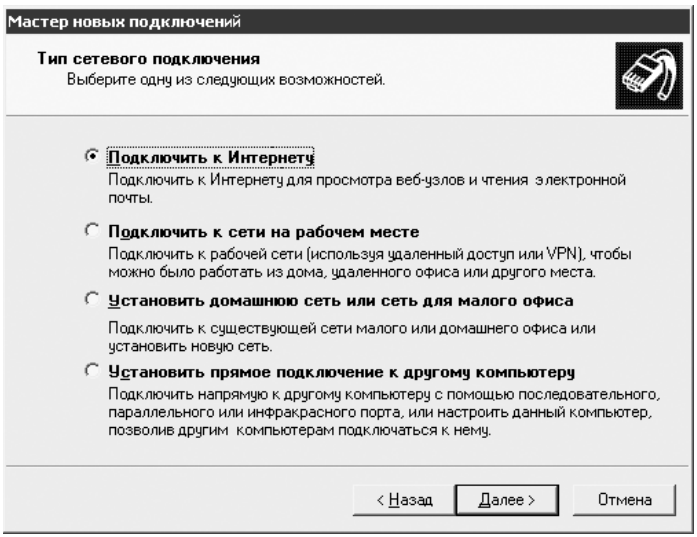


Рис. 9.6. Окно выбора типа подключения к Интернету

После этого будет активировано диалоговое окно (рис. 9.7), в котором можно выбрать тип настройки подключения к Интернету:

- выбрать из списка поставщиков услуг Интернета;

- установить подключение вручную;
- использовать компакт-диск поставщика услуг Интернета.

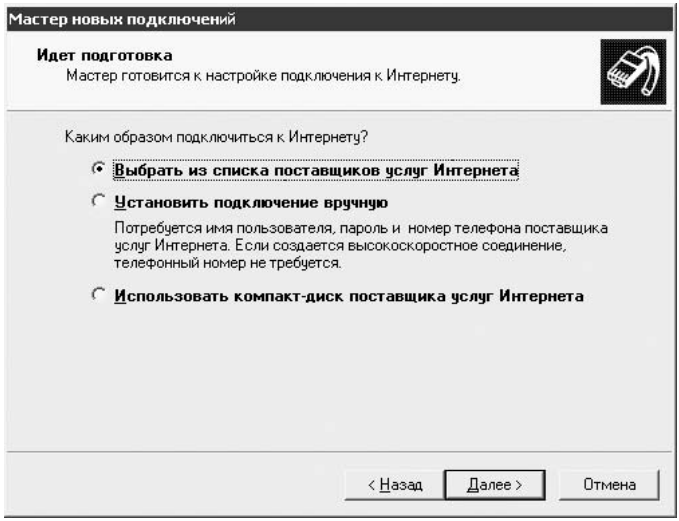


Рис. 9.7. Укажите тип настройки подключения к Интернету

ПРИМЕЧАНИЕ Как правило, выбирается второй вариант настройки подключения к Интернету.

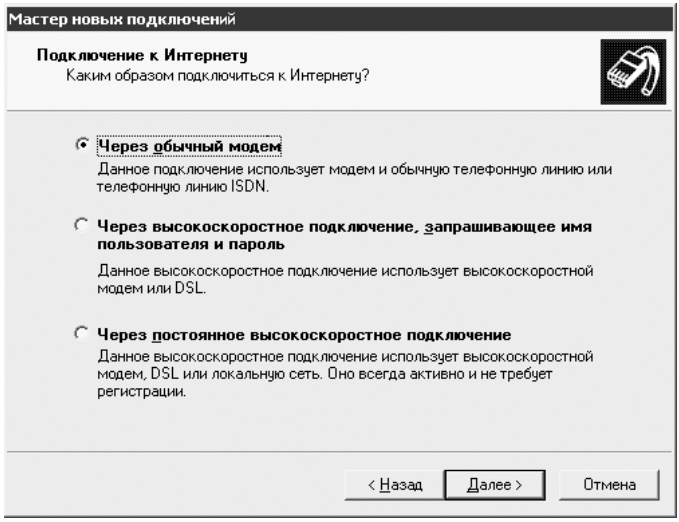


Рис. 9.8. Выбор типа подключения удаленного доступа

После выбора требуемого варианта настройки (в рассматриваемом случае используется второй пункт) и нажатия кнопки Далее будет отображено следующее

диалоговое окно, в котором нужно указать тип подключения к Интернету (рис. 9.8):

- через обычный модем (модем, подключенный к обычной телефонной линии или линии ISDN);
- через высокоскоростное подключение, запрашивающее имя пользователя или пароль (используется высокоскоростной кабельный модем или линия DSL);
- через постоянное высокоскоростное подключение (кабельный модем, линия DSL или локальная сеть — подключение всегда активно и требует регистрации пользователя).

При выборе первых двух пунктов отображается диалоговое окно, в котором требуется ввести имя подключения удаленного доступа, а при выборе третьего пункта мастер завершает свою работу, после чего пользователь может непосредственно подключаться к локальной сети, имеющей общий доступ к Интернету.

Как правило, все настройки удаленного доступа определяются автоматически, но при необходимости их можно задать вручную.

Так, например, если выбрано постоянное высокоскоростное подключение, то нужно задать IP-адрес, DNS-адрес, основной шлюз, порядок использования таблицы LMHOSTS, а также активизировать поддержку протокола NetBIOS поверх TCP/IP.

Заданные ранее настройки можно изменить. Для этого достаточно щелкнуть правой кнопкой мыши на значке сетевого подключения, затем выбрать пункт Состояние, после чего перейти на вкладку Свойства (рис. 9.9).

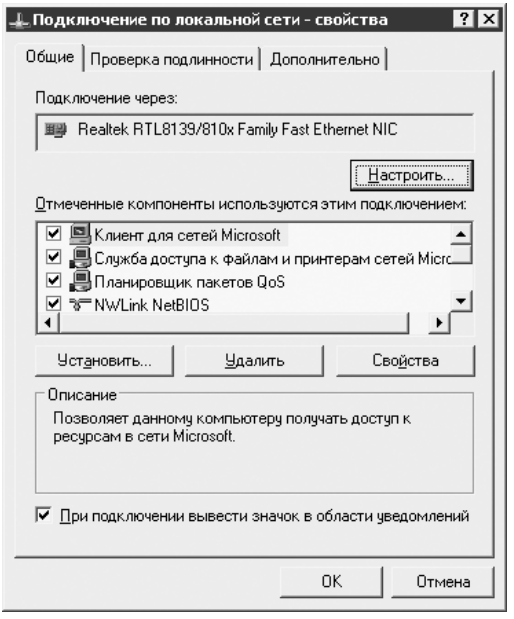


Рис. 9.9. Изменение ранее заданных настроек подключения удаленного доступа

Мастер новых подключений позволяет подключаться к сети, установленной ранее в офисе, напрямую подключаться к другому компьютеру при помощи параллельного или последовательного порта, что весьма полезно в случае прокладки «временной сети» между двумя компьютерами, а также установить домашнюю сеть. Последний пункт предусматривает выполнение некоторых подготовительных работ.

Нужно составить предварительный план сети. Нарисовать схему своего дома или офиса, отметив расположение каждого компьютера и принтера. Также можно создать таблицу с указанием аппаратной конфигурации каждого компьютера.

1. Рядом со значком каждого компьютера нужно описать установленное на нем оборудование, такое как модемы и сетевые адаптеры.
2. Выбрать компьютер, используемый в качестве узла общего доступа к подключению Интернета (ICS, Internet Connection Sharing). Для этого рекомендуется использовать компьютер с операционной системой Windows XP Professional и настроенным подключением к Интернету.
3. Определить типы сетевых адаптеров, используемых в сети (Ethernet, HPNA, беспроводные адаптеры или IEEE 1394).
4. Составить список оборудования, которое нужно купить. В этот перечень нужно включить модемы, сетевые адаптеры, концентраторы (коммутаторы) и сетевые кабели.
5. Приобрести необходимое оборудование.
6. Установить сетевые адаптеры и модемы для создания сетевых подключений на всех компьютерах.
7. Физически соединить компьютеры друг с другом. Подключить кабели к концентраторам (коммутаторам), телефонным розеткам и компьютерам.
8. Включить все компьютеры и принтеры, подключенные к сети.
9. Убедиться, что на узловом компьютере ICS имеется активное подключение к Интернету. Чтобы получить доступ к Интернету, достаточно просто запустить мастер создания подключения.
10. Запустить мастер настройки сети Windows XP Professional на узловом компьютере ICS.
11. Запустить мастер настройки сети на остальных компьютерах.
12. После этого просто останется лишь запустить мастер настройки домашней сети, который настроит все необходимые параметры сети.

Безопасность удаленного доступа в среде Windows XP

Вообще говоря, тема безопасности будет всесторонне рассматриваться в следующей главе, но поскольку сейчас обсуждаются удаленные подключения, уместно обговорить проблемы их безопасности именно в этой главе.

Подключение к Интернету в среде Windows XP может быть защищено программным брандмауэром. Благодаря этому компоненту обеспечивается фильтрация входящих сетевых пакетов, поступающих на тот или иной входящий порт.

ПРИМЕЧАНИЕ Брандмауэры в версиях Windows XP с Service Pack 1 и Service Pack 2 несколько отличаются друг от друга. Хотя принцип действия брандмауэров разных версий остается тем же.

Брандмауэр ICF

Сначала будет рассмотрен брандмауэр подключения к Интернету, который был реализован в Windows XP Service Pack 1.

Брандмауэром (противопожарной стеной) называется «заградительный барьер», устанавливаемый между локальной сетью и окружающей ее внешней средой, под которой в данном случае понимается Интернет. Создатели операционной системы Windows XP реализовали программный брандмауэр. (ICF, Internet Connection Firewall). Этот программный компонент устанавливается при настройке подключения удаленного доступа и позволяет фильтровать трафик между Интернетом и домашней или небольшой офисной сетью.

Если в локальной сети активизирована служба общего доступа к подключению Интернета (ICS, Internet Connection Sharing), посредством которой сразу несколько компьютеров могут получать доступ к Интернету, именно для этого подключения следует активизировать программный брандмауэр ICF. Хотя на самом деле компоненты ICS и ICF могут функционировать независимо друг от друга.

ВНИМАНИЕ Рекомендуется использовать брандмауэр для любого компьютера, имеющего непосредственное подключение к Интернету. Не рекомендуется использовать брандмауэр ICF для подключения ICF, поскольку это может привести к проблемам при осуществлении общего доступа к файлам и принтерам.

Брандмауэр ICF является представителем обширной категории *брандмауэров, регистрирующих состояние канала связи*. Подобные брандмауэры отслеживают все характеристики передаваемого через них трафика, а также проверяют IP-адреса компьютера-отправителя и компьютера-получателя в каждом пересылаемом сообщении. Для того чтобы предотвратить «проникновение» в частную зону сети данных, поступающих с общедоступной стороны подключения без запроса, брандмауэр подключения к Интернету поддерживает таблицу всех исходящих сеансов связи, инициированных с компьютера, на котором выполняется брандмауэр ICF.

При работе на одиночном компьютере ICF контролирует его исходящий трафик. Если брандмауэр ICF используется в сочетании со службой ICS, то он отслеживает весь трафик, отправляемый с компьютера ICF/ICS, а также весь трафик, исходящий из компьютеров частной сети. Весь входящий трафик из Интернета проверяется по записям таблицы брандмауэра. Этот трафик пропускается на компьютеры сети только в том случае, если в таблице имеется соответствующая запись, показывающая, что обмен данными был начат с данного компьютера или из частной сети.

Сеансы связи, которые инициируются извне, например из Интернета, блокируются брандмауэром всегда, кроме тех случаев, когда на вкладке Службы определе-

но соответствующее разрешение. При этом брандмауэр ICF не отсылает соответствующих уведомлений, а просто прерывает передачу данных, которые он не запрашивал. Это помогает остановить многие распространенные виды атак, например сканирование портов. Если бы каждый раз генерировалось соответствующее сообщение, это бы слишком сильно загружало брандмауэр. Поэтому просто ведется журнал безопасности, в котором фиксируются все попытки незаконного доступа к компьютеру, защищенному брандмауэром.

Службы можно настроить таким образом, чтобы разрешить ICF пересылать в частную сеть данные, поступающие из Интернета без предварительного запроса. Например, если на компьютере ICF функционирует веб-сервер, то все данные HTTP, которые не были предварительно запрошены, будут направляться компьютером ICF веб-серверу. Чтобы пропускать входящий трафик на веб-сервер частной сети, брандмауэру подключения к Интернету требуется указать набор рабочих параметров, называемый *определением службы*.

Если в сети имеется подключение, которое не связано непосредственно с Интернетом, не стоит активизировать брандмауэр ICF. Так, например, если брандмауэр ICF установлен для сетевого адаптера клиентского компьютера ICS, он будет мешать обмену данными между этим компьютером и остальными компьютерами сети. По этой же причине мастер настройки сети не позволяет устанавливать ICF для частного подключения главного компьютера ICS, которое связывает его с компьютерами клиентов ICS, так как в этом случае брандмауэр полностью блокирует сетевой трафик.

Вряд ли стоит устанавливать брандмауэр подключения к Интернету, если в сети ранее был установлен другой аппаратный или программный брандмауэр или прокси-сервер.

Если в сети имеется только одно общее подключение к Интернету, оно должно быть защищено при помощи брандмауэра ICF. При этом следует иметь в виду, что брандмауэр ICF может проверять только трафик, проходящий через то подключение к Интернету, на котором он активизирован. Поэтому для обеспечения защиты сети в целом его необходимо включить на всех компьютерах, подключенных к Интернету, либо использовать одно общее подключение к Интернету, защищенное брандмауэром.

Параметры служб, позволяющие службам работать под защитой брандмауэра подключения к Интернету, задаются для каждого подключения отдельно. Если в сети брандмауэр использует несколько подключений, то необходимо составить определение службы для каждого подключения, на котором должна действовать эта служба.

Однако стоит обратить внимание и на отрицательные стороны брандмауэра ICF.

Поскольку брандмауэр подключения к Интернету проверяет все входящие соединения, его включение может влиять на режим работы некоторых программ, особенно клиентов электронной почты. Некоторые программы для получения новых сообщений периодически опрашивают свой сервер электронной почты, а другие программы могут быть настроены на ожидание уведомления от сервера.

Например, почтовая программа Outlook Express автоматически проверяет наличие новых сообщений по команде таймера. При наличии новой почты Outlook

Express отправляет пользователю соответствующее уведомление. Брандмауэр подключения к Интернету не влияет на работу данной программы, поскольку запрос на уведомление о наличии новой почты не проходит через брандмауэр. Брандмауэр создает в таблице запись об исходящем соединении. Когда почтовый сервер подтвердит получение ответа о наличии новой почты, брандмауэр найдет соответствующую запись в таблице и разрешит прохождение данного соединения, после чего пользователь получит уведомление о поступлении новой почты.

Подобная проблема отсутствует в почтовой программе Outlook 2000, которая подключена к серверу Microsoft Exchange, рассылающему клиентам уведомления о новой почте с помощью *удаленных вызовов процедур* (RPC). Outlook 2000 не выполняет поиск новой почты при подключении к серверу Exchange. Сервер извещает приложение Outlook 2000 о поступлении новой почты. Поскольку уведомление RPC инициируется сервером Exchange, находящимся вне зоны действия брандмауэра, ICF не может найти соответствующую запись в таблице и блокирует прохождение сообщений RPC из Интернета в домашнюю сеть. Пользователи могут отправлять и получать электронную почту, но вынуждены вручную проверять поступление новой почты.

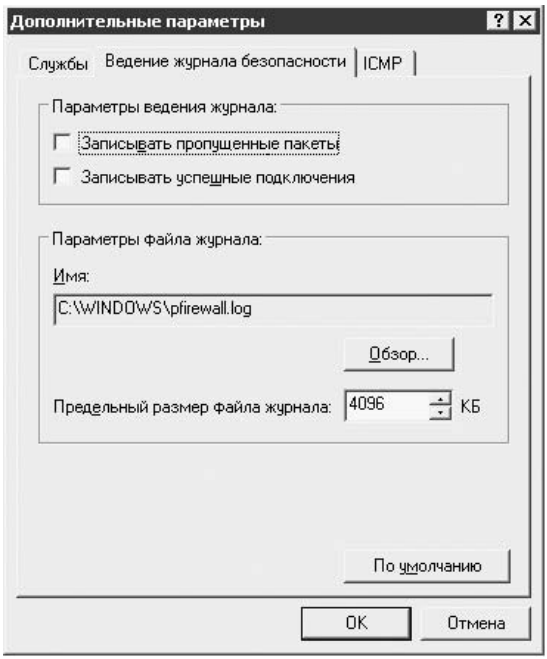


Рис. 9.10. Настройка параметров журнала безопасности ICF

В журнале безопасности ICF (рис. 9.10) регистрируются сведения обо всех событиях, связанных с работой брандмауэра. Брандмауэр подключения к Интернету может регистрировать как пропускаемый трафик, так и отклоняемый. По умолчанию брандмауэр не пропускает входящие эхо-запросы из Интернета. На-

пример, если параметр Разрешить входящий запрос эха не активизирован для протокола ICMP (Internet Control Message Protocol), входящий запрос отвергается, а в журнал заносится запись о неудачной попытке доступа. Для получения доступа к журналу безопасности следует выбрать соответствующее подключение удаленного доступа, в контекстном меню выбрать пункт Свойства, а затем перейти на вкладку Дополнительно. В открывшемся диалоговом окне нужно нажать кнопку Параметры, после чего перейти на вкладку Ведение журнала безопасности. Здесь можно задать параметры ведения журнала.

Благодаря указанию максимального размера журнала безопасности можно избежать ситуации «переполнения», которое может быть вызвано атаками типа «отказ в обслуживании». При создании журнала используется формат Extended Log File Format (расширенный формат файла журнала), стандартизированный организацией W3C.

В диалоговом окне Дополнительные параметры также имеется вкладка ICMP (рис. 9.11), позволяющая задавать правила обработки сообщений, попадающих на данный компьютер.

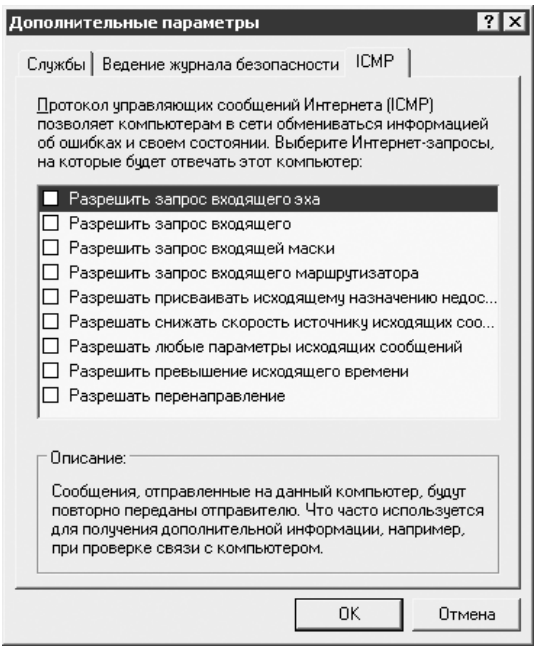


Рис. 9.11. С помощью параметров этой вкладки можно изменять способ обработки оповещений

Благодаря *протоколу ICMP* можно изменять режим работы брандмауэра, используя различные параметры настройки ICMP, такие как Разрешить входящий запрос эха, Разрешить входящий запрос отметки времени, Разрешить входящий запрос маршрутизатора и Разрешать перенаправление. На вкладке ICMP можно найти краткое описание этих параметров.

Брандмауэр для Windows XP SP2

С появлением версии Windows XP, включающей пакет обновлений Service Pack 2, встроенный брандмауэр приобрел новые качества.

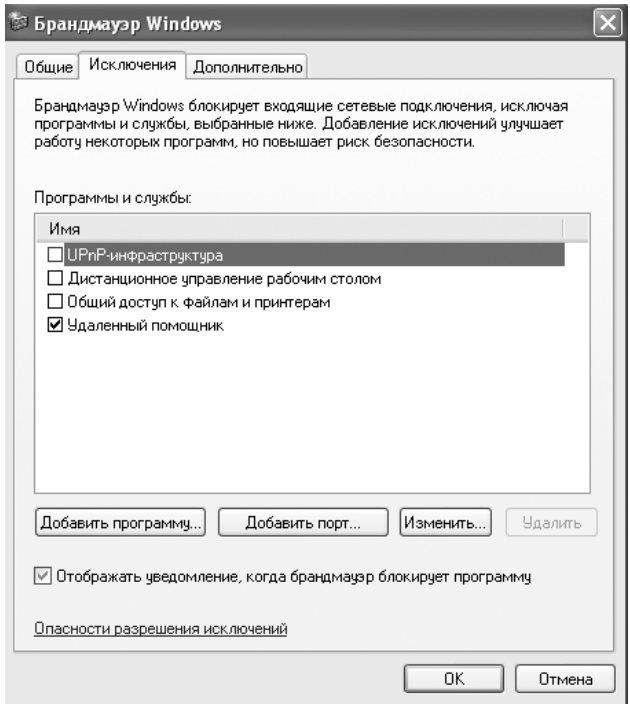


Рис. 9.12. Диалоговое окно брандмауэра Windows XP SP2

В процессе установки подключения удаленного доступа пользователю предлагается защитить систему брандмауэром (в версии Windows XP SP1 брандмауэр предлагался в качестве дополнительной опции).

- Предполагается защита всех соединений при помощи брандмауэра.
- Заданные настройки по умолчанию распространяются на все соединения. При этом пользователь может задавать особые правила для некоторых соединений.
- Осуществляется фильтрация трафика по отдельным портам и приложениям.
- Обеспечивается фильтрация трафика в соответствии с заданным диапазоном IP-адресов.
- Встроена поддержка протокола IPv6.
- Пользователь может конфигурировать брандмауэр, используя утилиту netsh или групповую политику.

Если требуется настроить брандмауэр Windows XP SP2, достаточно щелкнуть на значке панели управления Центр обеспечения безопасности, после чего будет предоставлен доступ к интерфейсу управления. В нижней части раздела Настрой-

ки параметров безопасности нужно выбрать пункт Брандмауэр Windows. После этого будет открыто соответствующее диалоговое окно (рис. 9.12), в котором можно выполнять все необходимые настройки.

Дистанционное управление рабочим столом

С приходом эры Windows XP появилась приятная возможность управления рабочим столом. На самом деле эта возможность возникла в процессе эволюции сервера RAS, который использовался в Windows 2000 Server. Доступ к этому компоненту обеспечивается при помощи команды Пуск ▸ Все программы ▸ Стандартные ▸ Связь ▸ Подключение к удаленному рабочему столу. После этого на экране будет отображено диалоговое окно настройки свойств подключения (рис. 9.13). Все приведенные параметры очевидны и не требуют какого-либо дополнительного объяснения.

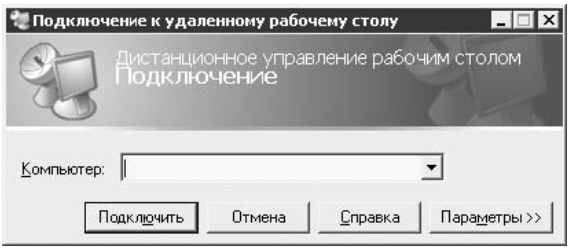


Рис. 9.13. В этом диалоговом окне можно настроить свойства удаленного доступа

Но для чего нужно удаленное управление рабочим столом? На самом деле этот компонент весьма полезен, поскольку с его помощью пользователь может получить доступ к сеансу Windows на своем компьютере, находясь при этом за другим компьютером. Например, можно подключиться к рабочему компьютеру из дома и получить доступ ко всем файлам, приложениям и сетевым ресурсам точно так же, как и при работе на рабочем компьютере. Можно оставить программы работать на рабочем компьютере и дома продолжить работу с теми же программами, окна которых будут отображаться на экране домашнего компьютера.

В процессе подключения к рабочему компьютеру при помощи компонента Дистанционное управление рабочим столом выполняется его блокировка, в результате чего другие пользователи не могут получить доступ к приложениям и файлам. Отменить режим блокировки можно в том случае, если воспользоваться сочетанием клавиш Ctrl+Alt+Del>.

Этот компонент может использоваться несколькими пользователями одновременно. При этом они подключаются к одному и тому же компьютеру, на котором запущено несколько рабочих сеансов.

При работе с этим компонентом можно реализовать быстрое переключение между задачами, выполняемыми различными пользователями. Предположим, что один из пользователей работает с электронной таблицей, а другому в это время нужно проверить электронную почту. Нет ничего проще! Первый пользователь просто разрывает соединение дистанционного управления рабочим столом,

второй пользователь устанавливает его, проверяет свою электронную почту, затем первый пользователь восстанавливает свое подключение, причем все данные электронной таблицы отображаются на экране в неизменном виде. Возможность быстрого переключения пользователей доступна как на отдельных компьютерах, так и на компьютерах, входящих в рабочую группу.

Используя компонент Дистанционное управление рабочим столом, можно реализовать на практике несколько сценариев.

- Работа из дома — доступ к рабочему компьютеру с домашнего компьютера, включая полный доступ к локальным и удаленным устройствам.
- Совместная работа — отображение рабочего стола своего компьютера на экране компьютера сотрудника, например для отладки программы, обновления презентации слайдов в программе Microsoft PowerPoint или для корректуры документа.
- Общий доступ к консоли — поддержка на одном компьютере сеансов нескольких пользователей с разными приложениями и параметрами (например, для бухгалтеров или работников склада).

Для дистанционного управления рабочим столом требуются, как минимум, два компьютера, на каждом из которых выполняется операционная система Windows XP Professional. Первый компьютер выполняет роль сервера, а второй — роль клиента. Компонент Дистанционное управление рабочим столом может быть установлен только на втором компьютере.

На этом можно завершить рассмотрение большой и интересной темы установки и настройки удаленного доступа в Windows 2000 Server (Windows XP) и перейти к рассмотрению захватывающих вопросов безопасности в локальных сетях.

10 ГЛАВА Безопасность в локальных сетях

В этой главе рассматриваются вопросы обеспечения безопасности локальных сетей. Также большое внимание будет уделено выбору средств обеспечения компьютерной безопасности и проблемам защиты сети от частичного или полного разрушения.

Что может угрожать вашей сети?

Каждый сетевой администратор неоднократно сталкивался с различными вторжениями при работе в локальных сетях, особенно, когда они подключены к Интернету. Степень опасности переоценивать не следует, но также не стоит сильно расслабляться, поскольку после нервничать после удачной атаки будет уже поздно. Нанесенный ущерб может варьироваться от минимального (например, поврежденные или похищенные графические и текстовые файлы) до катастрофического. В случае выхода из строя центрального корпоративного сервера наступит паралич всей системы. Также вероятна утрата данных, накопленных за долгие годы работы. Конечно, последняя ситуация маловероятна, поскольку, в каждой сети должно регулярно выполняться резервное копирование информации. В любом случае, прежде чем перейти к осуществлению мер по защите информации, следует оценить важность защищаемой информации, а такжеь стоимость реализации защитных мер. Это нужно сделать для того, чтобы стоимость мероприятий по обеспечению безопасности не превысила ценность сохраняемых данных.

А начать изложение материала следует с рассмотрения категорий рисков, связанных с эксплуатацией локальных сетей.

Внешние угрозы

В настоящее время ситуация с безопасностью локальных сетей крайне обострилась. Простота доступа к Интернету позволяет хакерам использовать эту среду для организации различного рода атак. В сеть, подключенную к Интернету, может проникнуть извне любой достаточно опытный пользователь, владеющий соответствующим инструментарием. Разумеется, это может произойти только тогда, когда не разработана четкая иерархия мер соблюдения безопасности, которая планомерно внедряется на всех уровнях сети — от отдельной рабочей станции до выделенного сервера.

Причины внешнего вторжения могут быть самыми различными, но независимо от причин следует уделять самое пристальное внимание вопросам обеспечения безопасности. В следующем перечне приводится классификация внешних опасностей.

- Доступ посторонних лиц к ключам и паролям сети, что чаще всего вызвано беспечностью самих пользователей.
- Атаки типа DoS (Denial of Service, отказ в обслуживании) и DDoS (Distributed Denial of Service, распределенная атака на отказ в обслуживании).
- Имитация IP-адреса.
- Разрушительные действия компьютерных вирусов, троянских коней и червей.
- Активные действия хакеров, направленные на взлом веб-сайтов и целых локальных сетей.
- Продвинутые пользователи, вооруженные инструментарием для перехвата трафика кабельных и беспроводных сетей.

В дальнейшем все эти угрозы будут рассмотрены подробнее.

Несанкционированный доступ к ключам и паролям

Согласно определению, *паролем* называется последовательность символов, которую обязан ввести пользователь, пытающийся зарегистрироваться в сети. При помощи *ключа* гарантируется целостность коммуникационного канала в локальной сети, соединяющего сеть с Интернетом, а также канала, реализующего подключение VPN.

Благодаря этим простейшим методам защиты информации эффективно предотвращается несанкционированный доступ посторонних лиц к сетевым ресурсам. Конечно, «суперсекретный» пароль возможен только в фантастических романах, и даже самый замысловатый пароль может стать достоянием гласности в результате проведения процедуры *взлома*. Причем для незаконного получения пароля не требуется обладать мастерством высококлассного программиста или специальными знаниями, приобретаемыми за долгие годы обучения в университете. Часто достаточно быть просто хорошим психологом.

Многие пользователи пренебрежительно относятся к возможным опасностям, связанным с несанкционированным доступом к сети и похищением ценных данных. Человеку свойственна беспечность и наивное представление о том, что беда может случиться с кем угодно, но только не с ним самим. Но, к сожалению, на практике часто бывает иначе. Именно поэтому многие пользователи в качестве пароля указывают собственное имя, фамилию или вообще ограничиваются пробелом. Поэтому подбор пароля в данном случае представляет довольно простую задачу. Некоторые легкомысленные сотрудники записывают секретные пароли на листках бумаги, которые затем приклеиваются на лицевых панелях мониторов. Чтобы получить доступ к подобной сети, не требуется быть крутым хакером. Достаточно зайти в офис, представившись сотрудником компании, и внимательно осмотреться вокруг. А еще лучше иметь при себе мобильный телефон со встроенной цифровой фотокамерой. Подобные средства значительно облегчают задачу по фиксации регистрационных имен и паролей.

В предыдущем абзаце был вкратце описан типичный прием, относящийся к арсеналу технических средств *социотехники*. Все эти приемы разрабатывались с учетом особенностей человеческой психики, поэтому очень часто приводят к успеху. Например, хакер может просто позвонить вам лично и, представившись представителем технической поддержки провайдера, попросит назвать имя вашей учетной записи и пароль. При этом он совершенно правильно назовет ваши имя и фамилию и сошлется на аварию, якобы имевшую место на сервере, в результате чего необходимо восстановить данные. Именно для этого ему может потребоваться ваш пароль. Вы можете получить также электронное письмо с обратным адресом типа support@mail.ru, содержащее просьбу выслать ваше имя и пароль. И многие поддаются на подобные уловки, хотя нет недостатка в соответствующих предупреждениях со стороны провайдеров и сетевых администраторов.

Конечно, бывает и такое, что пользователи интересующей потенциального взломщика сети обладают иммунитетом по отношению к методам социотехники. В этом случае остается попробовать подобрать пароль. Конечно, подбор осуществляется не вручную, так как это потребовало бы колоссальных затрат времени. С возникновением компьютерной техники подбор пароля производится намного проще. Существует целый ряд специальных программ, которые используются для подбора паролей в автоматическом режиме. Альтернативное название подобных программ, довольно точно отражающее суть дела, — взломщики паролей. Подобная программа перебирает все возможные комбинации букв, цифр и других символов со скоростью несколько десятков тысяч комбинаций в секунду. При этом используется либо метод «грубого взлома», при котором просто перебираются все возможные сочетания символов, либо метод подбора пароля со словарем. Существуют версии подобных программ, предназначенные для взлома файловых архивов, защищенных паролями. На рис. 10.1 показано диалоговое окно программы, предназначенной для «взлома» RAR-архивов — Advanced RAR Password Recovery.

Рис. 10.1. Забыли пароль от архива — не беда, воспользуйтесь специальной программой

Конечно, бывают такие ситуации, когда перечисленные средства недостаточны для получения вожделенного пароля. Как всегда, в этом случае доступны некие альтернативные способы.

Например, хакер вполне может воспользоваться программой сетевого анализатора пакетов для того, чтобы перехватить пакет данных, который включает пароль. Подобных программ существует достаточно много. К их числу относятся EtherPeek, LANWatch32, NetBoy, Observer, Sniffer Basic и т. д.

ПРИМЕЧАНИЕ Более подробно анализаторы пакетов будут рассмотрены в следующей главе.

Атаки DoS

Предмет рассмотрения данного раздела — активные действия хакеров, направленные на разрушение сети. Одним из наиболее распространенных типов подобных действий является *атака типа DoS* (Denial of Service, отказ в обслуживании). Довольно часто эти виды атак применяются организованными группами хакеров, которые стремятся вывести из строя корпоративные веб-сайты или даже целые сети.

Если целью атаки DoS является отдельный компьютер, то в процессе ее организации используются различного рода слабые места в системном и прикладном

программном обеспечении, установленном на этом компьютере. Если же атака направлена на сеть, то будут использованы недостатки в системе сетевой защиты. Устранение слабых мест в программах реализуется с помощью так называемых «заплат» (код, используемый для устранения недоработок в программе). В результате применения подобного кода закрываются лазейки для предпринимаемых атак типа DoS.

Выполнение атак этого типа не влияет на работоспособность компьютера, их цель — повредить сеть. Эта цель достигается при помощи массированной отсылки в сеть бесполезных пакетов, а также при помощи имитации различных сетевых неисправностей.

Атаки DoS делятся на несколько категорий:

- атаки, использующие сообщения протокола ICMP;
- атаки «пингом смерти»;
- атаки типа Smurf;
- атаки типа SYN;
- распределенные атаки DoS.

А теперь вкратце остановимся на описании каждой из упомянутых выше категорий.

Атаки, использующие сообщения протокола ICMP, насыщают систему пакетами ICMP, которые изначально предназначаются для проверки корректности информации, а также обнаружения ошибок в передаваемых в Интернет пакетов данных. Пакеты ICMP обычно передаются с помощью команды `ping`, главное назначение которой заключается в определении факта подключения компьютера к сети. В процессе выполнения команды `ping` отсылается ICMP-сообщение Echo Request (эхо-запрос), а затем ожидается ответное ICMP-сообщение — Echo Replay (эхо-ответ). В процессе осуществления подобных атак реализуется отсылка непрерывного потока данных по IP-адресу целевого компьютера. В результате производительность сервера резко уменьшается, а затем он отключается вовсе из-за превышения значения параметра времени ожидания ответа.

При *атаке «пингом смерти»* используется ограничение на длину передаваемого пакета (MTU, Maximum Transmission Unit). Фактическая величина этого ограничения зависит от типа сетевой среды, а также от вида применяемой сетевой архитектуры. Если длина передаваемого пакета превышает величину, определенную значением MTU, производится его разбиение на несколько меньших пакетов, которые затем собираются на компьютере-получателе. Длина IP-пакета, в которую включено ответное сообщение ICMP, ограничена значением 65 535 октетов. Организатор атаки прекрасно осведомлен об этом, поэтому отсылает пакеты, в которых длина поля данных ответного сообщения ICMP превышает предельное количество октетов. Процесс сборки подобных пакетов заведомо обречен на неудачу, поэтому сеть полностью парализуется.

При организации *атаки Smurf* формируется поток пакетов ICMP, который затрагивает все службы провайдера или даже весь сетевой сегмент. Сообщения

ICMP, отсылаемые по широковещательному адресу, приводят к генерированию ответов всех компьютеров подсети. Поэтому производительность всех сетевых компонентов падает, в результате чего происходит отключение всех пользователей. Следует обратить внимание на то, что как только хакер получает доступ к сети, он отсылает широковещательное сообщение, в котором указывается один из адресов атакуемой сети. В результате все сетевые устройства, входящие в состав данной сети, посылают ICMP-сообщения по указанному адресу. Таким образом, сеть «переполняется» десятками тысяч битов ответных сообщений, отправляемых сотнями узлов атакованной сети. Особенно быстро исчерпываются ресурсы низкоскоростных глобальных каналов связи между провайдером и сетью. При этом блокируется не только сеть, на которую направлена атака, но и все промежуточные сети, пропускающие поток сгенерированных в этом случае сообщений.

В процессе *атаки SYN* в попытке нарушить «естественный ход событий» хакер может вмешаться в последовательность согласования, выполняемого в процессе установки сеанса связи TCP.

Процесс установки сеанса связи TCP можно условно разделить на три этапа:

- клиентский компьютер передает запрос согласования SYN, представляющий собой сгенерированную последовательность цифр;
- сервер передает подтверждение ACK, которое сформировано в виде полученного сервером числа, сгенерированного клиентом, плюс единица;
- клиентский компьютер добавляет единицу к биту SYN, сформированному сервером, затем передает его серверу в качестве ACK-подтверждения. После того как сервер и клиент получат подтверждения, устанавливается соединение.

В процессе проведения атак подобного рода хакер выполняет ряд запросов на установление сеанса, как правило, используя ложный IP-адрес. На основе этих запросов формируется очередь сообщений компьютером-получателем. Таким образом, хакер может легко добиться состояния переполнения очереди, в результате чего практически полностью блокируется обработка запросов и установка сеансов. В итоге легальные сетевые пользователи не могут установить соединение.

Распределенная атака DoS (DDoS) является опаснейшим оружием в руках злоумышленника. В своей время ее жертвами стали такие компании, как Yahoo!, eBay, Buy.com, Amazon.com, CNN.com и многие другие. В результате осуществления этой атаки становится невозможным подключиться к серверу, на котором функционирует целевой веб-сайт. Особенностью этой атаки является то, что атакуются, как правило, мощные серверы, подключенные к широкополосному каналу связи.

ПРИМЕЧАНИЕ

10 октября 2003 года один из крупнейших хост-серверов Рунета подвергся распределенной атаке. В результате проблем у «Зенона» в течение некоторого времени был затруднен доступ к целому ряду сайтов, в числе которых Газета.Ру.

В последнее время атаки типа DDoS являются одним из наиболее распространенных киберпреступлений. Бывает и так, когда хакеры просто шантажируют свои жертвы угрозой проведения подобного рода атаки. Жертвами такого шантажа становятся компании, бизнес которых непосредственно связан со стабильным функционированием веб-серверов, например Интернет-магазины.

Существует два основных типа атак DDoS. Первый тип приводит к нарушению работы всей системы или сети. Если хакер посылает жертве данные или пакеты, которые она не ожидает, это приводит либо к остановке системы, либо к ее перезагрузке. Эти атаки примечательны тем, что при помощи всего нескольких пакетов можно сделать систему неработоспособной. В большинстве случаев для того, чтобы вернуть систему в нормальный режим работы, необходима перезагрузка системы администратором. Таким образом, первый тип атак является наиболее разрушительным, поскольку осуществить атаку легко, а для устранения ее последствий требуется вмешательство оператора.

Второй, и более распространенный тип атак DDoS приводит к переполнению системы или локальной сети при помощи такого большого количества информации, которое невозможно обработать. Например, если система может обрабатывать только 100 пакетов в секунду, а взломщик отправляет 400 пакетов в секунду, законные пользователи, пытаясь подключиться к системе, получают отказ в обслуживании, поскольку все ресурсы заняты. При такой атаке злоумышленник должен постоянно переполнять систему пакетами. После того как он перестает это делать, проведение атаки прекращается и система возобновляет нормальную работу.

Этот тип атаки требует больше усилий со стороны хакера, поскольку ему необходимо постоянно активно воздействовать на систему. Иногда этот тип атаки приводит к остановке системы, однако в большинстве случаев восстановление после ее проведения требует минимального вмешательства человека. При проведении DDoS-атаки второго типа подвергшийся нападению компьютер получает пакеты одновременно от большого количества компьютеров, хозяева которых сами могут и не подозревать о происходящем. Кроме того, поскольку эти атаки проводятся с множества компьютеров, снабженных большим диапазоном IP-адресов, становится гораздо сложнее блокировать и обнаруживать нападение по той причине, что небольшое количество пакетов с каждой машины может не вызвать реакции со стороны систем обнаружения вторжений.

Если атака проводится с одного IP-адреса, его можно блокировать с помощью аппаратного или программного брандмауэра. Если же атака реализована при помощи большого количества компьютеров, то воспрепятствовать ей будет очень трудно. Причем, как правило, атака против единственного компьютера-жертвы проводится с множества компьютеров, разбросанных по всему миру. Если учитывать, что даже проводимые с одного источника атаки DDoS бывает сложно предотвращать, то можно себе представить, насколько сложнее защищаться от таких атак, которые проводятся с множества машин, расположенных в разных местах.

От атак DDoS защититься довольно сложно еще и потому, что жертва никогда не может полностью исключить возможность ее проведения. Если компьютерная система подключается к Интернету, то всегда есть вероятность того, что хакер может отправить ей такое количество данных, которое она будет не в состоянии обрабатывать.

ПРИМЕЧАНИЕ Обычно участниками атак типа DDoS становятся компьютеры пользователей Интернета, причем последние даже не подозревают об этом. Для этого компьютеры-исполнители атаки, обычно называемые зомби, заражаются троянскими программами. После заражения достаточного количества компьютеров-зомби по сигналу хакера происходит одновременная активизация троянских программ и осуществление самой атаки.

Естественно, способы защиты от DDoS-атак являются принципиально важным вопросом для специалистов в области компьютерной безопасности. Универсального рецепта нет до сих пор. Пока основной упор делается на быстрое обнаружение и способность скоординировать действия технического персонала провайдера. Персонал должен моментально задействовать фильтры входящего трафика, чтобы блокировать «мусорный» трафик в тех точках, где он входит в сеть провайдера. Пока это лучший способ подготовиться к массированной DDoS-атаке и при необходимости быстро ее остановить.

Следует помнить, что большинство операционных систем, маршрутизаторов и сетевых компонентов, которые должны обрабатывать пакеты на каком-либо уровне, являются уязвимыми для атак DDoS. Хотя атаки DDoS предотвратить довольно сложно, ограничение доступа к важным учетным записям, ресурсам и файлам, а также защита их от неправомочных пользователей может существенно затруднить проведение многих атак DDoS.

Согласно предсказаниям специалистов, в будущем атаки типа DDoS будут одним из основных видов оружия в киберпространстве. В Интернете уже давно идет война, причем масштабы конфликтов варьируются от взломов веб-сайтов небольших фирм и агентств новостей до нарушения работы сетей транснациональных корпораций и крупных государственных структур. Хотя, как правило, атаки типа DDoS чаще всего используются организованными киберпреступниками в своих целях. Например, для шантажа компаний, бизнес которых осуществляется в Интернете.

Имитация IP-адреса

Процесс *имитации IP-адреса* осуществляется при помощи изменения заголовка передаваемого пакета. В результате создается впечатление, что этот пакет передается компьютером, которому принадлежит имитируемый адрес. Этот метод даже не заслуживает звания «атаки», а скорее используется для получения доступа к сетевым компьютерам, чтобы похитить или повредить их данные. Изменение заголовков адресов может осуществляться динамическим образом, и только в течение небольшого промежутка времени, поэтому обнаружить подобный вид вторжения не так уж и просто.

ПРИМЕЧАНИЕ

А вот еще один пример действий вредных хакеров. Здесь идет речь скорее не об имитации IP-адреса, а о своего рода мимикрии. Пользователи Интернета, небрежно или в спешке набирающие веб-адреса, рискуют стать жертвами мошенников. К такому выводу пришли специалисты компании F-Secure. Они обнаружили, что всего один неверно набранный символ в URL-ссылке Google.com приводит к загрузке вредоносной программы. Ничего не подозревающие пользователи могут подвергнуться атаке различных видов троянских коней и шпионских программ, попав на сайт Googkle.com. Идея этого вида атаки относится к арсеналу средств социотехники. Суть ее заключается в том, что литера «k» расположена рядом с литерой «l», поэтому ее можно нажать совершенно случайно. Специалисты из фирмы F-Secure настоятельно рекомендуют пользователям Интернета быть более внимательными при наборе электронного адреса и не посещать страницу Googkle.com. Тот, кто все-таки по оплошности попадет на этот ресурс, увидит два всплывающих рекламных объявления со ссылками на зараженные вирусами веб-сайты. При посещении одного сайта на компьютер устанавливается троянская программа, которая записывает и отсылает мошенникам персональную информацию, связанную с данным пользователем. На втором веб-сайте пользователя Интернета ожидает другая вредоносная программа. Инфицировав компьютер жертвы, она время от времени подает ложные предупреждения об обнаружении вирусов и пытается заманить пользователя на другие зараженные страницы. Представители Google ситуацию комментировать отказались, хотя в прошлом компания пыталась принимать меры для защиты пользователей, допустивших опечатку при наборе адреса. Так, например, если пользователь Интернета вводил третью, лишнюю букву «o» в URL Google, он автоматически перенаправлялся на домашнюю страницу компании. Однако тем, кто вместо двух набирал четыре литеры «o» в слове Google, везло меньше — они попадали на портал USseek.com, на котором размещалась всплывающая реклама интерактивного казино. Схема мошенничества, основанная на ошибках пользователей при наборе веб-адреса, довольно широко распространена. Она используется как некоторыми фирмами, пытающимися похитить таким образом трафик у конкурентов или попаразитировать на успехе крупных компаний, так и киберпреступниками, которые промышляют фишингом. Наиболее известным примером URL-мошенничества, является сайт Whitehouse.com. Пользователи, желавшие посетить веб-страницу администрации президента США, были немало удивлены, так как несколько лет на этом ресурсе размещались рекламные объявления порнографического содержания. Естественно, страница Whitehouse.com не имела никакого отношения к Белому дому, чей официальный сайт располагается по адресу Whitehouse.gov.

Компьютерные вирусы и черви

Довольно часто в средствах массовой информации поднимается нездоровый шум из-за появления новых опасных вирусов и червей. Чаще всего подобного рода сведения можно найти в пресс-релизах фирм-разработчиков антивирусных программ. За последние годы сонм новых вирусов и червей нанесли огромный и во многих случаях непоправимый ущерб компьютерам и сетям, а также неоднократно блокировали передачу данных по глобальным каналам Интернета. С глубоким прискорбием приходится констатировать факт, что жертвами очередных

атак зловредных вирусов и червей чаще всего оказываются пользователи Windows, которые не обращают внимания на подобные угрозы до тех пор, пока однажды их любимый компьютер просто перестанет загружаться.

Чтобы избежать опасностей подобного рода, следует четко представлять характер и последствия, связанные с инфицированием вашего компьютера. Приведем несколько основных определений вредоносных программ, которые будут применяться в дальнейшем.

- *Вирус*. Фрагмент программного кода, который может дублироваться при помощи присоединения к другому объекту. Достаточно часто появление нового вируса вовсе не связано с написанием новой и оригинальной программы. На самом деле многие вирусные атаки, которые изначально воспринимались как результат появления новых образований, возникали из-за применения переписанных, а также повторно упакованных версий старых вирусных кодов. Когда компьютер, работающий под управлением операционных систем из семейства Windows, поражается вирусом, то изменяется содержимое системного реестра, а затем переписывается код системных файлов. Также очень часто вирус пытается использовать почтовые программы для своего дальнейшего распространения. Вирусная программа может производить самые различные действия. В частности, могут повреждаться или уничтожаться файлы данных, удаляться ранее установленные прикладные программы, нарушается работа операционных систем либо даже повреждаются некоторые аппаратные компоненты ПК, как это бывает при уничтожении информации, которая хранится в микросхеме BIOS.
- *Черви*. Компьютерные черви — это независимые программы, главное свойство которых заключается в том, что они могут воспроизводить самих себя, распространяясь между компьютерами. Обычно процесс распространения происходит при помощи сети или через электронную почту. Многие черви также содержат в себе вирусный код, повреждающий данные или запрашивающий столь большой объем системных ресурсов, что система выходит из строя.

Появление компьютерных вирусов датируется уже далеким 1980 годом, когда возникла первая вирусная пандемия. В качестве среды распространения тогда выступали обыкновенные дискеты, содержащие файлы с инфицированным кодом. Конечно, скорость распространения вирусов в те годы была незначительной и ограничивалась одним географическим районом, а чаще всего офисом, в котором работали обладатели дискет с вирусным кодом. Однако технический прогресс и глобализация привели к тому, что ситуация с распространением вирусов все чаще и чаще выходит из-под контроля.

У этого явления достаточно много причин. Так, например, платформа Windows получила очень широкое распространение, а популярные почтовые программы, такие как Microsoft Outlook и Outlook Express, установлены практически на каждом ПК, подключенном к Интернету, что облегчает распространение червей. Авторы вирусов постоянно усложняют свои вредоносные программы, снабжая их интеллектуальными процедурами инфицирования, применяя замысловатые приемы шифрования, загружая подключаемые блоки кода и даже модули, реализующие автоматическое обновление вирусов через Интернет. Код полиморфных вирусов может изменяться в процессе инфицирования новых файлов, что приводит к существенному затруднению их обнаружения и удаления. Поэтому вирусный сканер может воспринять две копии одного и того же вируса в качестве двух совершенно различных вирусов.

Следует также упомянуть о целом классе вредоносных программ, называемых *стелс-вирусами*. Этим кодам присущи столь изощренные приемы маскировки, что антивирусные программы просто бессильны в борьбе с ними. К сожалению, в наше время появились редакторы вирусных кодов, поставляемые вместе с образцами вполне работоспособных вирусов. Используя подобный инструментарий, любой студент может создать вполне функциональный вирус. Что ж, далеко не всегда плоды прогресса сладкие, чаще всего им присуща горечь.

Обратите внимание на то, что многие вирусы и черви могут распространяться путем присоединения к электронным сообщениям, после чего вирусы рассылают собственные копии по адресам, обнаруженным на инфицированном компьютере. Некоторые же, подобно вирусу CIH (Chernobyl), могут скрывать собственный вирусный код в системном файле, причем запуск кода на выполнение производится в заданное автором вируса время. Часто бывает так, что в момент открытия пользователем зараженного почтового файла, содержащего вложения, в отдельном окне начинает воспроизводиться Flash-ролик, который способен отвлечь внимание пользователей от внешних признаков, характеризующих разрушительную деятельность вируса. Другие вирусы, находящиеся в почтовых вложениях, маскируются путем добавления дополнительного расширения имени к инфицированному файлу. Эта стратегия основана на предположении о том, что потенциальная цель вируса использует заданные по умолчанию настройки Windows Explorer, позволяющие не отображать расширения известных типов файлов. Например, вирус SirCam может инфицировать случайным образом выбранный файл, добавляя к нему свое расширение, а также преобразуя его в исполняемый файл. Если отключено свойство по отображению расширений имен файлов, присоединенный файл имеет вид стандартного документа Microsoft Word, поэтому появляется соблазн посмотреть его содержимое в окне текстового редактора. Хотя большинство вирусов и червей распространяются в виде файлов, присоединенных к электронным сообщениям, этот метод передачи не является единственным. Вирусный код может попадать на незащищенные компьютеры через общедоступные сетевые ресурсы, сценарии, а также элементы управления ActiveX.

ВНИМАНИЕ Следует помнить, что очень часто веб-сайты с «веселыми» картинками в качестве бесплатных бонусов распространяют вирусы и троянские программы. Наиболее безобидная из подобных программ может любезно подключить ваш компьютер к службе удаленного доступа, находящейся в далекой Австралии. Вы можете наслаждаться просмотром эротического шоу, а в конце месяца получите счет на астрономическую сумму в несколько тысяч долларов. Поэтому будьте осторожнее и не подключайтесь к «сомнительным» веб-сайтам, особенно, если работаете на компьютере, содержащем очень важные данные.

Каким же образом можно остановить вирусы и черви на начальном этапе, не допустив фатального повреждения данных и программ, установленных на компьютере или в сети? Для этого следует выполнять следующие рекомендации.

- Обращайте внимание на признаки, свидетельствующие о появлении новых вирусов. Придерживаться подобной тактики особенно важно на протяжении первых нескольких часов или дней после того, как поступила информация о появлении нового вируса или червя, так как в это время еще отсутствуют

обновления антивирусных программ, направленные на выявление и ликвидацию новой вредоносной программы. Файлы, присоединенные к электронным сообщениям, которые присылаются даже вашими хорошими знакомыми, должны восприниматься весьма критично.

- Установите антивирусные программы, которые нужно своевременно обновлять. Желательно выполнять обновления еженедельно, поскольку в противном случае пользы от подобных программ будет немного. Идентификация инфицированных файлов грамотно спроектированной антивирусной программой осуществляется при помощи отслеживания загружаемых файлов, а также файлов почтовых вложений в режиме реального времени.
- Обучайте других сетевых пользователей методикам, позволяющим предотвратить инфицирование вирусными программами. Удостоверьтесь в том, что пользователи, работающие совместно с вами в сети, не склонны посещать подозрительные веб-сайты, а также открывать файлы, вложенные в почтовые сообщения. Рассказывайте им о важности своевременного обновления антивирусных программ.
- Возводите дополнительные преграды, препятствующие проникновению вирусов на компьютеры. Наилучшая защита от вирусов и червей заключается в их изоляции от пользователя. Некоторые программные брандмауэры, разработанные независимыми фирмами-производителями, поддерживают дополнительные уровни защиты, позволяющие блокировать зловредный код. Более подробно программные и аппаратные брандмауэры будут рассмотрены несколько позже. Последние версии Outlook и Outlook Express позволяют отключать потенциально опасные присоединенные файлы. В корпоративной сети, включающей сервер и шлюзы электронной почты, может устанавливаться карантин для подозрительных сообщений и файлов, загружаемых из Интернета.

Троянские кони

Троянские кони также известны под названием программ «черного хода». Этот код может функционировать в качестве скрытого сервера, позволяя получать контроль над удаленным компьютером, причем владелец компьютера может и не знать об этом. Троянские кони выдают себя за обычные программы, и доверчивые пользователи устанавливают их на своих компьютерах. Компьютеры, на которых установлены троянские кони, иногда называются *зомби*. Целые армии подобных зомби могут применяться для проведения массированных атак, в результате осуществления которых наносится вред функционирующим веб-сайтам.

ПРИМЕЧАНИЕ Ранее в данной главе уже описывались атаки типа DDoS, в которых принимают участие компьютеры-зомби.

Чтобы предупредить возможные атаки со стороны авторов троянских коней, нужно воспользоваться следующими советами.

- Отключайте службы, которыми не пользуетесь в данный момент. Если вы ранее установили персональный веб-сервер для экспериментирования в сфере

разработок веб-страниц, но уже не пользуетесь им, удостоверьтесь в том, что он не запущен. Подобный сервер представляет для злоумышленника легкую добычу.

- Используйте брандмауэры для блокировки доступа к компьютеру и отслеживания попыток несанкционированного вмешательства. Программы брандмауэров, созданные сторонними производителями, предлагают целый ряд возможностей, среди которых блокировка нежелательных подключений и ограничение доступа к Интернету определенными приложениями.
- Применяйте аппаратные барьеры для создания дополнительного уровня защиты. Простой маршрутизатор или шлюз поддерживает трансляцию сетевых адресов, в результате чего маскируются IP-адреса сетевых компьютеров, и таким образом предотвращает попытки вмешательства в работу сети. Более сложные и более дорогие брандмауэры имеют дополнительную возможность по блокировке определенных портов и протоколов, которые могли бы стать мишенью посягательства извне.

Кто же вы, мистер хакер?

Если вы периодически читаете газеты или смотрите голливудские фильмы, наверняка имеете представление о хакерах. Этакие небритые личности, которые проводят ночи напролет за клавиатурой компьютера и питаются гамбургерами, запивая их литрами растворимого кофе. Таланты хакера поистине не имеют границ. Он может легко взломать защиту любой банковской системы, корпоративной базы данных или даже проникнуть в военные сети.

Конечно, в реальном мире хакеры не столь могущественны, как их романтизированные образы. Хотя и не следует недооценивать возможной опасности, поскольку если компьютер, подключенный к Интернету, не защищен, хранящиеся на нем данные могут быть легко похищены или просто уничтожены.

Некоторые профессионалы в области компьютерной безопасности полагают, что средства массовой информации неверно толкуют и используют слово *хакер*. Вообще говоря, хакером считается любой специалист в области программирования, который занимается изучением компьютеров и операционных систем, а также осваивает их возможности, обнаруживая при этом различные уязвимости. Так называемые *белые хакеры* занимаются поиском и устранением слабых мест в операционных системах, приложениях и сетях. Именно эти специалисты пользуются заслуженным уважением в профессиональной среде. Однако есть еще и так называемые *черные хакеры*, которые могут анонимным образом проникать в другие компьютеры и сети, осуществляя несанкционированный доступ. Иногда подобные действия предпринимаются в целях самоутверждения, но чаще всего преследуется коммерческий интерес — например, при «взломе» банковской системы или воровстве номеров кредитных карточек.

В большинстве случаев злоумышленники, нарушающие работу компьютеров и вычислительных систем, не имеют какой-либо определенной цели. Они используют широко доступные утилиты, позволяющие автоматизировать процесс взлома и регистрации в системе. С помощью подобных инструментов можно сканировать сотни и даже тысячи IP-адресов в поисках определенных слабых

мест. Особенно эффективен этот метод при тестировании постоянных подключений к Интернету (кабельные модемы, DSL-линии и т. д.), когда соответствующие IP-адреса не изменяются. Примеры подобных уязвимостей описываются ниже.

- *Незащищенные совместно используемые ресурсы*. Как правило, ресурсы общего доступа должны быть открытыми только для пользователей сети. Практически же, если совместно используемые ресурсы защищены слабо, доступ к ним можно получить с других компьютеров из того же сегмента сети, а также, при определенных обстоятельствах, с любого компьютера, подсоединенного к Интернету. Злоумышленник, обнаруживший открытые ресурсы общего доступа, которые не защищены паролем, может по собственному усмотрению распоряжаться всеми файлами и папками этого компьютера. И что особенно важно, он сможет установить одну из нескольких программ удаленного доступа, при помощи которой получит полный контроль над данным компьютером.
- *Открытые служебные порты*. Если на компьютере выполняется некая серверная программа и злоумышленник обнаружит это, то он может прозондировать компьютер на предмет уязвимости парольной защиты или по ряду других параметров, которые получили репутацию «слабых» звеньев» системы безопасности. Если постоянно не работать над устранением подобных дыр в системе безопасности, хакер может воспользоваться ими и получить доступ к ресурсам компьютера. Объектами подобного рода атак часто являются веб-серверы, FTP-серверы, программы удаленного доступа типа pcAnywhere, а также программные пейджеры, как, например, ICQ.

Угрозы, связанные с беспроводными сетями

Несмотря на многие преимущества беспроводных локальных сетей, им присущ недостаточный уровень защиты. Причем опасность существует даже в том случае, если сетевые администраторы используют встроенный протокол обеспечения безопасности WEP (Wired Equivalent Privacy). Довольно распространена транзитная атака, когда хакеры разъезжают на машине по районам, где расположено множество бизнес-центров и офисов, и пытаются получить несанкционированный доступ к локальным корпоративным сетям прямо с улицы. Поиск локальных беспроводных сетей производится при помощи портативных сканеров, способных улавливать радиоизлучение в широком диапазоне частот.

Результаты исследований трех специалистов из Калифорнийского университета в Беркли (Berkeley) Никиты Борисова (Nikita Borisov), Яна Голдберга (Ian Goldberg) и Дэвида Вагнера (David Wagner) позволили обнаружить серьезное уязвимое место в системе шифрования протокола WEP. Более того, в августе 2001 года специалисты по криптографическим системам Скотт Флюрер (Scott Fluhrer), Ицик Мантин (Itsik Mantin) и Ади Шамир (Adi Shamir) опубликовали статью с описанием уязвимостей технологии шифрования RC4, на базе которой был разработан протокол WEP. В конце августа 2001 года студент университета Rice и два сотрудника лаборатории AT&T Research Адам Стаблфилд (Adam Stubblefield), Джон Иоаннидес (John Ioannidis) и Авель Д. Рубин (Aviel D. Rubin) применили на практике идеи, высказанные в двух упомянутых выше статьях. Наиболее прискорбным фактом было то, что обнаруженная дыра откры-

вала доступ к системе, причем для этого не требовалось какое-либо специальное оборудование. Все, что нужно злоумышленникам в этом случае, — компьютер со стандартным беспроводным адаптером, который работает с измененными драйверами, загруженными из Интернета. Подобная технология позволяет записывать и оценивать сотни тысяч пакетов данных, передаваемых по радиосетям.

На этом можно завершить краткое описание основных угроз, связанных с эксплуатацией локальных сетей. Это описание является далеко не полным, но дает общее представление о масштабах всей проблемы.

Внутренние угрозы

Часто встречается ситуация, когда сами работники той или иной компании воруют ценные сведения или даже присваивают деньги фирмы, воспользовавшись информацией, которая циркулирует во внутренних сетях компании. Поэтому вопросам, связанным с внутренними угрозами, следует уделить самое пристальное внимание.

В следующем перечне указаны некоторые источники внутренних угроз:

- внутренние противоречия в компании;
- недовольные работники;
- промышленный шпионаж;
- случайные сбои или нарушения.

А теперь подробнее рассмотрим эти вопросы.

Внутренние противоречия в компании

Весьма опасна ситуация, когда в компании работают не в меру амбициозные служащие, которые готовы пойти на все, чтобы добраться до сияющих вершин власти. Добравшись до вершины, эти люди обнаруживают, что положение начальника дает им власть над людьми, свободу унижать подчиненных, что еще больше возвышает их в собственных глазах. На пути к возвышению подобные типы используют любые методы. Так, например, они могут попытаться вывести из строя сеть, чтобы помешать работе более успешного коллеги. Либо попробуют собрать на него досье при помощи просмотра электронной корреспонденции или личной записной книжки. Вооружившись компроматом, подобные субъекты начинают подрывать репутацию жертвы. Некоторые могут даже отсылать от имени жертвы компрометирующие письма (например, от имени женщины-коллеги отправить письмо-анкету на специализированный веб-сайт по оказанию интимных услуг, в котором указать домашний телефон). Диапазон подобных средств достаточно велик, поэтому не хотелось бы, чтобы кто-то нажил себе врага в лице подобного товарища.

Конечно, наиболее простой способ избавиться от такого рода внутренней угрозы — уволить недоброжелателя. К сожалению, это не всегда возможно. В данном случае следует придерживаться заранее спланированной стратегии обеспечения сетевой безопасности. В частности, стоит задуматься над тем, чтобы использовать трудно подбираемые пароли, вести аудит сетевых событий, а также предпринять

некоторые другие меры, способные помочь в выявлении и пресечении подобного рода неприятностей. Не забывайте о том, что здоровый моральный климат в коллективе положительно сказывается на результатах производственной деятельности.

Недовольные работники

Наиболее опасными могут быть работники, в том числе и бывшие, которые в силу ряда причин затаили зло на компанию и стремятся отомстить любой ценой. В этом случае вполне реальна угроза потери ценных данных, а также блокирования работы сети.

Особенно велика угроза будет в том случае, если увольняется кто-либо из ведущих технических специалистов компании. Подобный бывший сотрудник может отформатировать несколько жестких дисков, содержащих особо ценные данные, испортить оборудование или оставить на память о себе парочку особенно злобных вирусов.

Поэтому следует немедленно удалить учетную запись уволенного сотрудника, а также ограничить его доступ к компьютерам фирмы во время сборов.

Промышленный шпионаж

Даже если ваша компания не занимается разработкой и внедрением новых технологий, не следует недооценивать угрозу промышленного шпионажа. Эта угроза наиболее серьезна, поскольку в результате ее осуществления компания может быть полностью разорена за весьма короткий промежуток времени.

Существует достаточно много методик промышленного шпионажа. Часто конкуренты привлекают сотрудников компании, о которой нужно собрать важные данные, посулами высокого гонорара в обмен на некоторые услуги. Может также разыгрываться вариант с «подсадной уткой», когда на работу в компанию устраивается новый сотрудник, обладающий знаниями и опытом работы, который достаточно быстро завоевывает доверие руководства компании со всеми вытекающими отсюда последствиями. В распоряжении промышленных шпионов также находится целый арсенал вспомогательных технических средств, позволяющих получать доступ к интересующей их информации.

Поэтому если ваша компания работает в отрасли промышленности, где промышленный шпионаж особо распространен, следует придерживаться повышенных мер безопасности. В частности, для проведения важных переговоров следует оборудовать специальную комнату, снабженную активными и пассивными экранами, которые могут нейтрализовать действие подслушивающих устройств. Не стоит вести важные служебные переговоры по телефону или доверять коммерческие секреты электронной почте. Лучше всего будет, если компьютер, на котором хранятся особо важные сведения, снабжен дублирующими системами и не подключен к сети. В этом случае риск вторжения хакеров, охотящихся за ценными коммерческими сведениями, будет минимальным. Не следует пренебрегать консультациями специалистов в области защиты данных, хотя это может быть очень недешевым удовольствием. Помните о том, что потеря важных данных обойдется гораздо дороже.

Случайные сбои или нарушения

Часто причиной появления внутренних угроз являются разрушительные действия пользователей, предпринятые по недомыслию или вследствие технической неграмотности. Многие сетевые администраторы могут припомнить случаи из своей практики, когда пользователи удаляли файлы операционной системы или приложений, пытаясь освободить место на диске. И хорошо, если объектом подобных экспериментов не становится выделенный файл-сервер! Некоторым становится скучно на работе, в результате чего пользователи устанавливают различные компьютерные игры, зачастую включающие в себя небезопасный код.

Удаление или перемещение жизненно важных системных файлов может быть предотвращено при помощи ограничения прав доступа к этим файлам. В этом случае используются системные или групповые политики Windows NT/2000.

Средства обеспечения безопасности

В предыдущих разделах главы были рассмотрены различные угрозы безопасности локальных сетей, а также проведена их классификация. В этом разделе описываются методы, обеспечивающие защиту циркулирующих в сетях данных.

Все меры, направленные на обеспечение защиты сетевых данных, делятся на организационные и технические. К организационным мерам относится назначение прав доступа различным пользователям и группам, разработка политики обеспечения безопасности и т. д. Технические меры подразумевают использование специальных аппаратных и программных средств, позволяющих обезопасить сети от внутренних и внешних угроз.

Безопасность на уровне операционных систем

Разным операционным системам присуща различная степень безопасности. Например, устаревшие операционные системы MS-DOS не поддерживают идентификацию пользовательских учетных записей. Хотя, в принципе, каждый пользователь может загрузить ОС MS-DOS и выполнять любые приглянувшиеся ему приложения либо получать доступ к файлам, которые хранятся на жестком диске.

Относительно современные ОС, например Windows 95, поддерживают механизм пользовательских учетных записей. Правда, соответствующие пароли хранятся в обычных текстовых файлах. И этот файл может быть легко прочтен, если, например, загрузиться в режиме MS-DOS с загрузочной дискеты.

При работе в операционных системах, которым присуща высокая степень безопасности (например, Windows NT/2000 или Linux), для нормальной загрузки системы и последующей работы с ней потребуется указать правильное имя пользователя и пароль. В данном случае пароли хранятся в зашифрованном виде, поэтому получить к ним доступ не столь уж и просто.

Группы, пользователи и права доступа

Современные операционные системы обеспечивают назначение отдельных учетных записей каждому пользователю. Причем каждой учетной записи присваива-

ется свой отдельный пароль. Если при загрузке ОС имя учетной записи и пароль были указаны верно, пользователь может выполнить следующие действия:

- получить доступ к сетям и операционным системам;
- считывать и изменять те общедоступные ресурсы, для которых текущая учетная запись обладает соответствующими правами доступа;
- выполнять любые действия, допускаемые текущей учетной записью;
- загружать элементы персональной конфигурации.

Бывает и так, что хранящиеся в компьютере данные не представляют особой ценности для хакера, а требования к безопасности данных не слишком строги. В этом случае можно не создавать отдельные пользовательские учетные записи. Тогда пользователи получают одинаковые права доступа к компьютерным ресурсам. При этом не только формируется полностью открытая и ненадежная среда, но и сами пользователи испытывают ряд определенных неудобств, прежде всего из-за того, что во время загрузки не происходит автоматическое конфигурирование системы в соответствии с предпочтениями каждого пользователя.

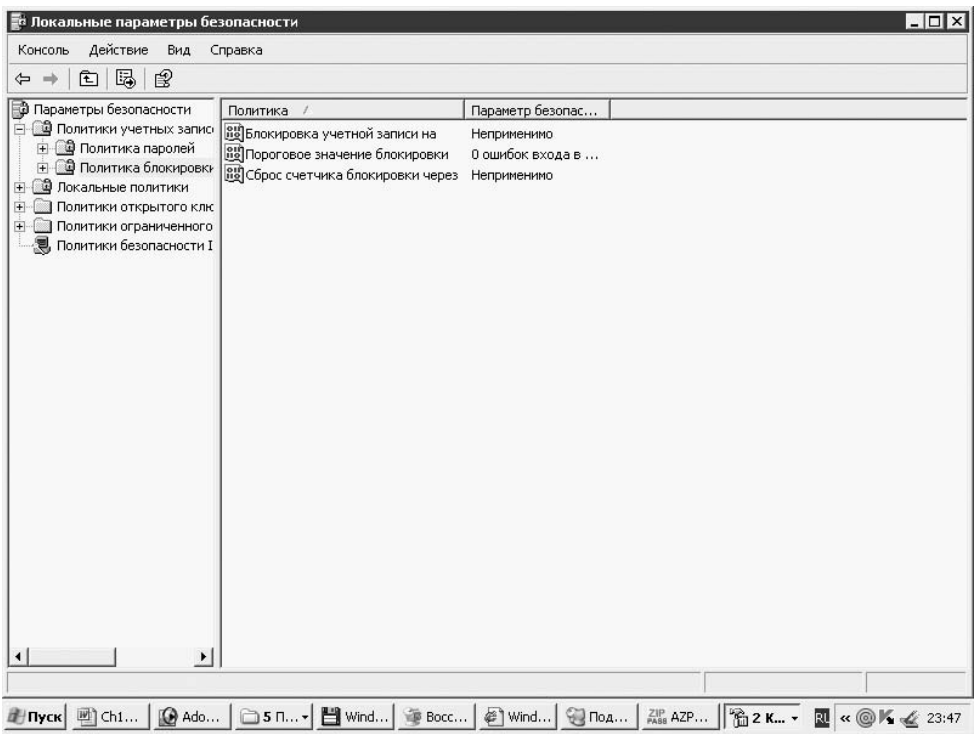


Рис. 10.2. Здесь настраиваются параметры блокирования учетной записи

Учитывая указанные выше причины, лучше для каждого пользователя создавать отдельную учетную запись. Если требования к обеспечению безопасности не столь высоки, можно указывать пустые пароли.

ПРИМЕЧАНИЕ

Весьма полезной в целях обеспечения безопасности системы является политика блокировки учетной записи. Для ее активизации в папке Администрирование панели управления Windows XP нужно активировать оснастку Локальная политика безопасности. Затем в группе Политики учетных записей нужно выбрать пункт Политика блокировки учетной записи и настроить соответствующие параметры (рис. 10.2).

Разблокировать учетную запись может только пользователь, обладающий правами администратора.

Назначение и применение паролей

В комплексе мер по обеспечению безопасности следует предотвратить вероятность использования плохо защищенного пароля. Если пользователи могут выбирать пароли самостоятельно, должны устанавливаться правила создания хорошего пароля.

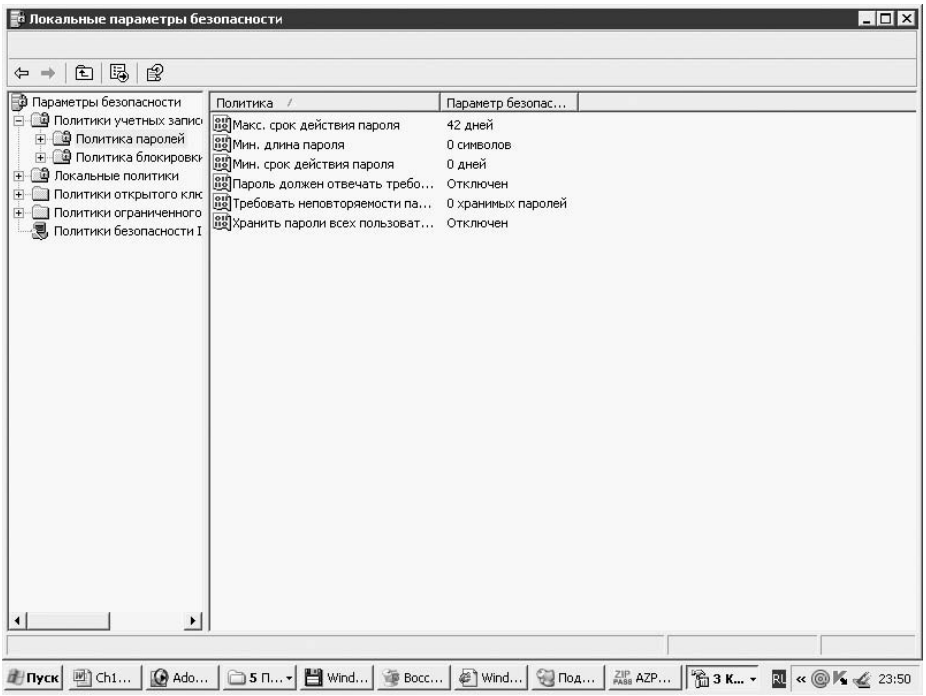
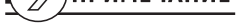


Рис. 10.3. Изменение параметров паролей

В следующем перечне приведены некоторые правила, используемые в процессе создания паролей.

- Ни в коем случае не следует использовать пароль, который представляет собой число или слово, имеющее прямое отношение к пользователю. Например, номер водительских прав или кличка домашнего кота.

- Не рекомендуется применять в качестве пароля обычные слова, поскольку многие программы взлома паролей используют атаку со словарем. Поэтому следует использовать комбинированные буквенно-цифровые пароли.
- Большинство операционных систем характеризуются чувствительностью паролей к изменению регистра символов, поэтому лучше использовать смесь символов верхнего и нижнего регистров.
- Следует подбирать пароль таким образом, чтобы он легко запоминался. К сожалению, это требование противоречит условиям секретности пароля, поэтому тут нужен разумный компромисс.
- Следует учитывать тот факт, что с увеличением длины пароля затрудняется процесс его взлома. Но здесь важно соблюдать чувство меры. Ведь с увеличением длины пароля его запоминание становится весьма проблематичным. К тому же, защищенность пароля растет в геометрической прогрессии, поэтому длина пароля, равная 7–8 символам, будет вполне достаточной.



ПРИМЕЧАНИЕ В среде Windows XP политика управления паролями настраивается при помощи оснастки Локальная политика безопасности, которая находится в папке Администрирование панели управления. Достаточно просто выбрать группу Политики учетных записей, перейти к пункту Политика паролей и в правой панели настроить все необходимые параметры (рис. 10.3).

Если к безопасности предъявляются очень высокие требования, следует внедрять политику периодического изменения паролей. Причем новый пароль не должен напоминать старый, что должно затруднять процесс возможного подбора. Пароли не следует менять слишком часто, иначе пользователям будет труднее их запоминать.

Во многих сетевых операционных системах администратор может определять собственные критерии выбора паролей. Можно даже задавать время существования пароля. Этот параметр определяет поведение системы таким образом, что по истечении заданного промежутка времени отображается системное сообщение о необходимости изменения пароля. Существуют также вспомогательные программы, помогающие выбрать правильный пароль. Например, подобная программа проверяет, имеется ли данное слово в словаре, и если обнаруживает совпадение, то предлагает пользователю изменить пароль.

Доступ к вычислительным ресурсам системы

Современные операционные системы обеспечивают улучшенный контроль за доступом к сетевым ресурсам. К примеру, пользователю с учетной записью Guest может разрешаться доступ исключительно к папке SharedDocs, где будут находиться относящиеся к нему документы, но при этом ему запрещается вносить изменения в эти документы. Одновременно с этим, пользователь данной учетной записи может изменять файлы в подпапке MyFiles.

При назначении прав доступа следует придерживаться принципа разумной достаточности. На практике это означает, что каждый пользователь получает только те права доступа, которые ему потребуются для выполнения своих обязанностей. Если файловая система обеспечивает высокий уровень безопасности (как это делает NTFS), следует создавать отдельные права доступа для использова-

ния ресурсов на одном и том же локальном компьютере. При этом локальные и сетевые права доступа далеко не всегда совпадают. Например, если пользователь Алекс регистрируется на локальном компьютере, он может получить права полного доступа по отношению к файлу alex.doc, но при регистрации в локальной сети ему запрещается модификация файла.

Администратору также следует принимать во внимание права доступа, предоставляемые в той или иной операционной системе по умолчанию. Например, серверы, реализованные на базе операционных систем из семейства Windows NT/2000, обеспечивают полный доступ к общим ресурсам для каждого пользователя сети. Поэтому права доступа следует указывать явно. Если же рассматривать вычислительную среду NetWare, то здесь по умолчанию общий сетевой ресурс никому не доступен до тех пор, пока в дело не вмешается сетевой администратор. Как видите, создатели операционной системы Windows NT/2000 излишне доверчивы, а разработчики NetWare никому не доверяют.

Как всегда, лучше отыскать золотую середину, которая достигается при помощи внедрения правил обеспечения сетевой безопасности. Следует тщательно продумать набор соответствующих правил, чтобы предоставлять права доступа тем, кто в них действительно нуждается, а также контролировать их использование с учетом возможных злоупотреблений.

Шифрование файлов

Одно из средств обеспечения безопасности заключается в шифровании данных таким образом, чтобы доступ к ним не смог получить никто, за исключением обладателя *ключа шифрования*. Некоторые операционные системы (к их числу относятся Windows 2000/XP) оборудованы встроенными средствами, позволяющими осуществлять шифрование данных. Другие операционные системы лишены подобной возможности, как, например, Windows 9x или Windows NT, поэтому в данном случае придется воспользоваться программами кодирования, разработанными независимыми производителями.

Шифрованная файловая система

Прежде всего следует отметить, что возможность шифрования файлов, обеспечиваемая *шифрованной файловой системой* (EFS, Encrypted File System), может использоваться только при работе с томами NTFS. Выбор формата тома осуществляется на этапе установки операционной системы. Преимущества, связанные с использованием файловой системы NTFS, подробнее рассматриваются в следующей главе. Здесь следует учесть, что перейти к использованию этой файловой системы можно и позднее, а вот вернуться к FAT16 или FAT32 будет уже сложнее. Это может понадобиться в том случае, если на вашем компьютере установлено несколько операционных систем.

Благодаря EPS файлы шифруются в момент их создания и изменения, в результате чего потенциальный злоумышленник, получивший доступ к важной информации на жестком диске, не сможет ею воспользоваться. Чтение подобных файлов возможно лишь в том случае, если пользователь вошел в систему с правами владельца этих данных. Пользователь, который подключился к компьютеру с зашифрованными данными, не сможет ими воспользоваться, поскольку он работает

под другой учетной записью. Поэтому EFS обеспечивает должный уровень защиты даже в сетях, в которых разрешен общий доступ.

Защита данных с помощью EFS

В случае правильной настройки системы EPS она работает в фоновом режиме, и при этом какого-либо вмешательства со стороны пользователей не требуется. Но если были допущены какие-либо ошибки на этапах установки или настройки EFS, безопасность всей системы может оказаться под угрозой. Например, распространенные текстовые редакторы сохраняют на системном диске временные файлы, которые не будут зашифрованными. Поэтому если требуется надежно защитить свои данные, следует обратить внимание на необходимость выполнения следующих действий.

- Если используется Windows 2000, нужно установить Service Pack 2 или службу High Encryption Pack, что позволит воспользоваться преимуществами 128-битового шифрования.
- После шифрования файла или папки необходимо создать персональный сертификат, о котором будет рассказано в одном из следующих разделов главы.
- Экспортировать сертификат нужно таким образом, чтобы он был доступен всем учетным записям.
- Экспортировать в безопасное место все закрытые ключи, применяемых в процессе восстановления данных, и организовать их надежную защиту, после чего нужно удалить их из локальной системы. Благодаря этому будет предотвращена возможность несанкционированного доступа к компьютеру со стороны хакера, который воспользуется агентом восстановления данных.

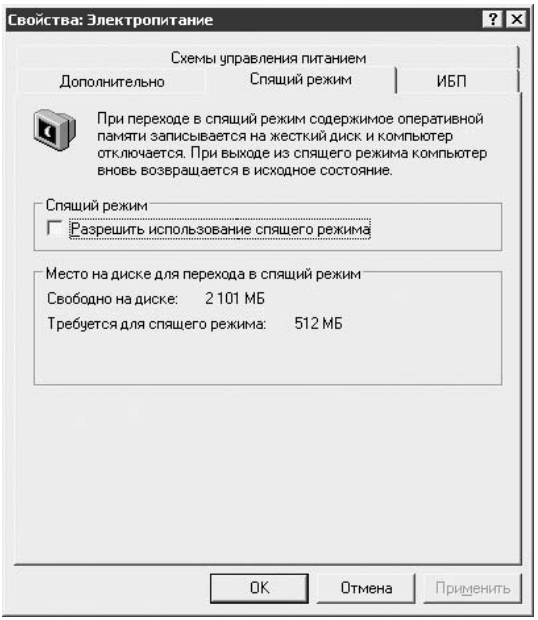


Рис. 10.4. Здесь можно выбрать спящий режим для данного компьютера

- В обязательном порядке следует шифровать папку Мои Документы, а также другие локальные папки, в которых организовано хранение документов.
- Нужно шифровать папки, а не файлы. Все файлы, создаваемые в подобной папке, всегда будут зашифрованы. Многие программы сохраняют копии документов в процессе редактирования. Эти копии также будут зашифрованы автоматически, если защищается вся папка, а не отдельный файл.
- Если настройки агента восстановления данных нужно изменить, не следует удалять сертификаты восстановления и закрытые ключи до тех пор, пока все защищенные файлы не будут модифицированы в соответствии с новыми условиями.
- Нужно настроить систему таким образом, чтобы файл pagefile.sys удалялся после отключения компьютера. Если этого не сделать, в файле могут оставаться фрагменты данных из обрабатываемых в процессе рабочего сеанса файлов.
- Отключить режим засыпания компьютера. Для этого в панели управления нужно запустить оснастку Электропитание и перейти на вкладку Спящий режим (рис. 10.4). Здесь необходимо отменить установку флажка После приостановки перейти в спящий режим.

Усиленное шифрование в Windows 2000

Прежде чем приступить к работе с файловой системой EFS, нужно убедиться в том, что в установленной версии Windows 2000 используется 128-битовый усиленный алгоритм шифрования.

В исходном комплекте поставки Windows 2000 Server используется 56-битовый алгоритм. Однако уже Service Pack 2 добавляет 128-битовый алгоритм кодирования, так что защита системы будет усилена.

Если на компьютере установлена устаревшая версия операционной системы Windows 2000, не поддерживающая 128-битовый алгоритм кодирования, потребуется обновить ее. Для проверки системы нужно перейти в папку \WINNT\SYTEM32 и попытаться найти файл Rsaenh.dll. Наличие подобного файла свидетельствует о том, что усиленный алгоритм кодирования установлен. Если же файла нет, то систему можно обновить с помощью одного из следующих трех способов.

- Установить пакет Service Pack 2 для Windows 2000. Данный метод является наиболее предпочтительным, поскольку это обновление содержит множество дополнительных исправлений и улучшений, касающихся системы безопасности, а также некоторых других служб.
- Запустить файл Encpack.exe, находящийся на дискете High Encryption Floppy Disk, входящей в комплект поставки Windows 2000 Professional.
- Загрузить и установить пакет High Encryption Pack с веб-сайта Microsoft по адресу http://www.microsoft.com/windows2000/downloads/recommended/encryption.

ПРИМЕЧАНИЕ Если вы работаете в среде Windows XP, необходимость в проверке отсутствует, поскольку возможности шифрования имеются в любых версиях этой операционной системы.

Работа с зашифрованной файловой системой

Благодаря подобной файловой системе обеспечивается шифрование файлов в томах NTFS, в результате чего исключается доступ к ним посторонних лиц. Таким образом добавляется еще один уровень безопасности в дополнение к правам доступа, присущим файловой системе NTFS. И этот уровень нельзя назвать лишним, поскольку права доступа NTFS не лишены уязвимости. Во-первых, все пользователи, имеющие права доступа администратора, могут получать доступ к самой секретной информации. Также любой пользователь, обладающий физическим доступом к вашему компьютеру, может загрузить операционную систему с дискеты, а затем использовать утилиту типа NTFSDOS.exe. Эта утилита обеспечивает доступ к любым файлам на жестком диске, причем для этого не требуется указывать имя пользователя и пароль.

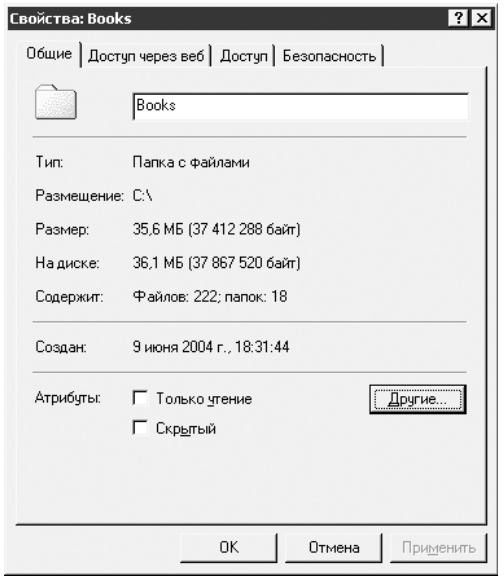


Рис. 10.5. В этом диалоговом окне устанавливаются свойства тома NTFS

Активизация шифрования файлов или папок производится следующим образом.

1. В окне Мой компьютер выбрать том NTFS, а затем папку, для которой требуется установить шифрование.
2. Щелкнуть на выбранной папке правой кнопкой мыши.
3. В контекстном меню выбрать пункт Свойства. В результате появится окно, изображенное на рис. 10.5.
4. В этом окне нажать кнопку Другие.... После этого отобразится диалоговое окно Дополнительные атрибуты, показанное на рис. 10.6.
5. В этом окне взвести флажок Шифровать содержимое для защиты данных.

Эта последовательность действий позволяет установить параметры шифрования для папки. Теперь все данные, сохраняемые в этой папке, будут шифроваться.

Если требуется установить шифрование для отдельного файла, рекомендуется проделать указанные действия, выбрав вместо папки отдельный файл.

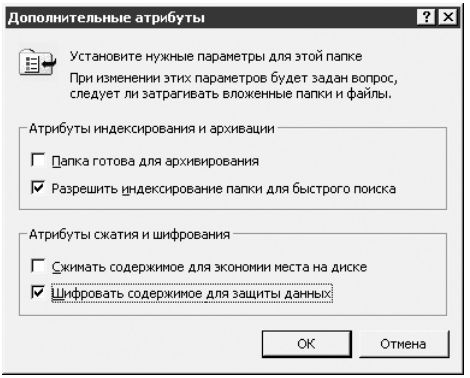


Рис. 10.6. Выбор шифрования для папки (файла)

Проблемы, связанные с использованием EFS

В процессе разработки файловой системы EFS был использован настолько сильный метод шифрования, что в случае утери ключа дешифрования информация будет полностью утрачена. Причем возможность восстановления данных, находящихся в зашифрованных файлах, сведена к нулю.

Вероятность случайной утери ключа весьма высока. Предположим, что зашифрованные данные хранятся на логическом диске `D`. Неизбежно наступает момент, когда жесткий диск компьютера переполняется ненужными файлами, в результате чего работа системы сильно замедляется. Что же делать в подобной ситуации? Существует стандартное решение, которое много раз проверено на практике — форматирование системного раздела жесткого диска с установкой копии ОС Windows 2000/XP. Недолго думая, пользователь берет системный компакт-диск и приступает к решительным действиям. Но надо учитывать, что в результате любой переустановки Windows создаются новые идентификаторы безопасности (SID, Security Identifier) для каждого пользователя, даже если точно повторялись все действия, производимые в процессе предыдущей установки. Поэтому будут изменены абсолютно все сертификаты шифрования, принадлежащие пользователям, вследствие чего никто из них не сможет получить доступ к собственным данным, хранящимся на диске `D`. Даже пользователь с правами доступа администратора, которому тоже присваивается новый идентификатор безопасности, ничего не сможет сделать в подобной ситуации.

К счастью, описанная выше ситуация не относится к категории безвыходных. Следующая последовательность действий поможет сохранить все необходимые данные.

1. Создать пустую папку и зашифровать ее.
2. В зашифрованной папке создать какой-либо файл и убедиться, что доступ к нему работает хорошо.
3. Если компьютер не включен в состав домена, необходимо создать агент восстановления данных (Data Recovery Agent). Под этим понятием подразумевается

учетная запись пользователя, при помощи которой можно восстановить файлы в случае утери персонального сертификата.

4. Выполнить резервное копирование сертификата восстановления, а также персонального сертификата вместе с принадлежащими им закрытыми ключами. Обратите внимание, что не требуется сохранять эти файлы до тех пор, пока не будет закодирован хотя бы один файл или папка. После установки Windows сертификаты не создаются. Они генерируются в процессе выполнения первой процедуры кодирования.
5. Теперь можно использовать файловую систему EPS для хранения важных данных.

Если файлы шифруются на компьютере, не входящем в состав домена, следует использовать агент восстановления данных. Персональный сертификат и сертификат агента восстановления данных следует хранить в надежном месте.

Отключение и включение кодированной файловой системы производится при помощи оснастки Локальная политика безопасности, входящей в группу администрирования панели управления.

Отключение и повторное включение EFS

На платформе Windows 2000 (Windows XP) отключение EFS производится следующим образом.

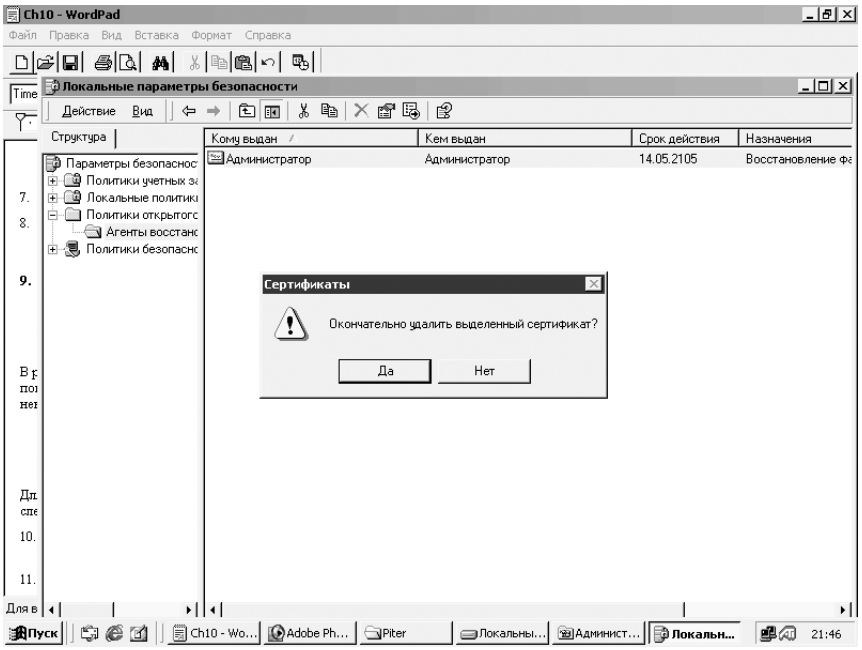


Рис. 10.7. Удаление агента восстановления данных

1. Запустить оснастку Локальная политика безопасности (рис. 10.7). Для этого нужно перейти в панель управления, затем открыть папку Администрирование

и дважды щелкнуть на пиктограмме Локальная политика безопасности. Можно также в командной строке ввести команду secpol.msc.

2. Перейти в раздел Политики открытого ключа\Агенты восстановления данных.
3. Правой кнопкой мыши щелкнуть на сертификате Administrators и в отобразившемся контекстном меню выбрать пункт Delete (Удалить). Перед удалением сертификата нужно убедиться в том, что сертификат восстановления файлов был экспортирован вместе с закрытым ключом. Если этого не сделать, произойдет повторный запуск системы EFS без полной переустановки Windows 2000.
4. В отобразившемся диалоговом окне нажать кнопку Yes (Да).

В результате применения описанной пошаговой процедуры создается пустая политика восстановления данных. Если пользователи попытаются зашифровать файлы и папки, появится соответствующее диалоговое окно, отображающее предупреждение о невозможности выполнения запрошенных действий.

Для перезапуска EFS потребуется переустановить сертификат агента восстановления данных. Для этого достаточно выполнить следующие действия.

1. Находясь в окне оснастки Локальная политика безопасности, нужно перейти в раздел Политики открытого ключа\Агенты восстановления данных.
2. Щелкнуть правой кнопкой мыши на пункте Агенты восстановления шифрованных данных, а в контекстном меню выбрать пункт Инициализация пустой политики. Если в контекстном меню упомянутый пункт отсутствует, значит, одна пустая политика уже была выбрана. Поэтому можно просто пропустить этот шаг.

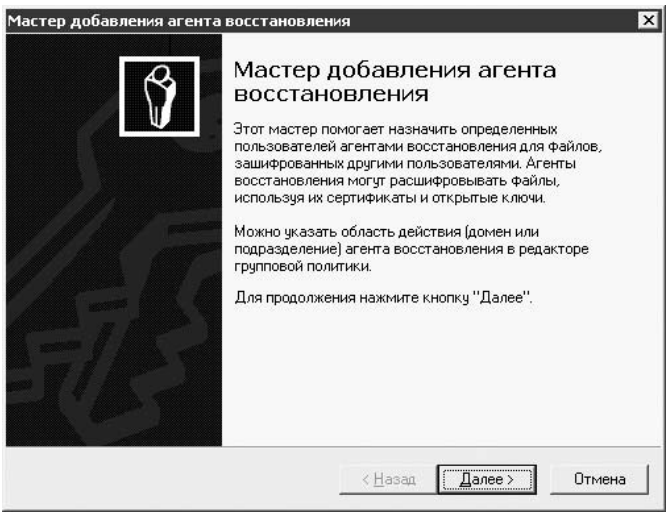


Рис. 10.8. Мастер установки агента восстановления данных

3. Правой кнопкой мыши щелкнуть на пункте Агенты восстановления шифрованных данных, а затем в контекстном меню выбрать пункт Добавить ▸ Агент шифрованных данных. После этого будет активировано окно мастера добавления агента восстановления (рис. 10.8). Затем нужно нажать кнопку Далее.

4. На странице Мастер добавления агента восстановления нужно нажать кнопку Обзор папок, после чего перейти в папку, содержащую файл сертификата с расширением .cer. Кнопка Просмотр каталога позволяет просматривать структуру Active Directory, если там опубликованы сертификаты пользователей. После завершения этой операции нужно нажать кнопку Открыть.
5. После этого на странице появится отображение нового агента USER_UNKNOWN. Затем нужно последовательно нажать кнопки Далее и Готово.
6. В результате этих действий будет отображено сообщение Сертификат не может быть удостоверен. На самом деле все в порядке и сертификат создан правильно. Осталось лишь нажать кнопку OK.

После завершения всех описанных шагов на панели отобразится сертификат агента восстановления данных, назначенный конкретному пользователю, и можно будет приступать к шифрованию файлов.

Ключи, шифры и цифровые сертификаты

Шифрование данных в компьютерных системах осуществляется при помощи *алгоритмов шифрования*. Алгоритмы шифрования/дешифрования, а также используемый при этом ключ называются *кодом* или шифром. Ключ представляет собой последовательность символов, соответствующую шифруемым данным. С ростом длины ключа шифра затрудняется взлом зашифрованного текста. В связи с этим ключи, длина которых равна 40 и 56 бит, называются *стандартными*, а ключи с длиной 128 бит — *сильными*.

Наиболее широко используются коды с секретными, а также открытыми/закрытыми ключами. Коды с *секретными ключами* иногда называют *симметричными кодами*, так как в этом случае применяется один и тот же ключ для шифрования и дешифрования данных.

Также широко применяются коды с секретными ключами DES (Data Encryption Standard, стандарт шифрования данных) и 3DES («тройной» DES), утвержденными Министерством обороны США. Однако применение секретного ключа может привести к определенным проблемам:

- на этапе генерирования секретных ключей;
- в процессе обмена ключами между уполномоченными пользователями, который должен организовываться таким образом, чтобы ключи не попали в руки посторонних лиц;
- при обеспечении безопасной коммуникации между большим количеством пользователей.

Часто используются коды с открытыми/закрытыми ключами, которые иногда называются *асимметричными*. *Открытый ключ* известен многим пользователям, а *закрытый* знает лишь один пользователь. В процессе шифрования сообщения применяется открытый ключ, а его дешифрование возможно только с помощью *закрытого ключа*, который должен храниться в тайне. Пример кода с открытым/закрытым ключом может представлять алгоритм RSA.

Цифровая подпись — это фрагмент данных, зашифрованных с помощью закрытого ключа компьютера-отправителя, которая добавлена в документ. Получатель дешифрует подпись с помощью открытого ключа отправителя, убеждаясь при

этом в ее подлинности. Цифровая подпись может применяться как для подтверждения подлинности личности отправителя, так и для проверки целостности отсылаемого документа.

Цифровые сертификаты содержат подпись третьего доверенного лица, именуемого *полномочным агентством сертификатов*. Сертификаты применяются для обеспечения подлинности сообщений, передаваемых по сетям с невысоким уровнем безопасности. При этом агентство гарантирует, что применяемый открытый ключ принадлежит данному пользователю.

Пользователь, чей закрытый ключ связан с рассматриваемым открытым ключом, запрашивает сертификат от полномочного агентства сертификатов. Полномочное агентство сертификатов проверяет, действительно ли этот открытый ключ принадлежит данному пользователю. Цифровые сертификаты распространяются следующими агентствами:

- GTE Cybertrust;
- Keywitness;
- TradeWave;
- Verisign.

Протоколы обеспечения безопасности

В этом разделе будет проведен обзор основных протоколов, обеспечивающих безопасность данных.

Протокол IP Security

Естественно, шифрование данных обеспечивает достаточно высокую степень безопасности, но оно хорошо работает только на локальном компьютере. Если же потребуется обеспечить защиту данных, передаваемых по сети, то нужны иные решения. И одно из таких решений предлагает *протокол IPSec* (IPSecurity, безопасность IP-пакетов). Этот протокол обеспечивает защиту передаваемых пакетов и выполняется на сетевом уровне модели OSI — именно поэтому он и невидим для выполняемых приложений.

На самом деле протокол IPSec состоит из двух протоколов: AH (Authentication Header, аутентификация заголовка) и ESP (Encapsulating Security Payloads, инкапсуляция данных о системе безопасности). Эти протоколы позволяют проверять подлинность личности отправителя, а также обеспечивают конфиденциальность при передаче данных.

Протокол IPSec может функционировать в транспортном режиме, а также в режиме туннелирования. При работе в транспортном режиме данные кодируются на пути от передающего до принимающего компьютера. Если же используется режим туннелирования, то данные кодируются на пути от точки выхода из одной сети до точки входа в другую сеть.

Процедуры защиты и шифрования при установке подключения между двумя компьютерами реализованы на уровне протокола IP. При этом зашифрованные пакеты не фильтруются брандмауэрами или маршрутизаторами, а просто передаются

в исходном виде. Этот процесс совершенно прозрачен для пользователей и приложений с каждой стороны установленного подключения.

Протокол IPSec функционирует на уровнях шифрования и инкапсуляции, аутентификации и устойчивости к повторениям, управления ключами, а также цифровых подписей и сертификатов.

Для шифрования IP-адреса отправителя используется 40/56- или 112/168-битовый стандарт шифрования DES. Это пресекает попытки перехватить передаваемые пакеты, не давая возможности хакеру определить адрес компьютера-отправителя или компьютера-получателя, без чего провести атаку просто невозможно. Исходный пакет также инкапсулируется в новый пакет, причем как его заголовок, так и содержание.

В целях обеспечения целостности данных используется алгоритм шифрования данных (SHA-1 или MD-5), который гарантирует, что данные не будут изменены во время передачи. Каждой дейтаграмме присваивается определенный номер последовательности. Когда дейтаграмма достигает точки назначения, проверяется ее номер последовательности, который должен лежать в определенном диапазоне значений. Если номер последовательности выходит за пределы диапазона, дейтаграмма удаляется.

Компонент управления ключами поддерживается восьмой версией протокола ISAKMP (Internet Security Association Key Management Protocol)/Oakley, который обеспечивает применение единой архитектуры для обеспечения безопасных транзакций при использовании программных продуктов, совместимых с протоколом IPSec, от различных поставщиков. За подтверждение действительности подписей на цифровых сертификатах отвечает стандарт DSS (Digital Signature Standard, стандарт цифровых подписей).

Протокол IPSec также поддерживает возможность импортирования уникального цифрового сертификата компании, соответствующего третьей версии спецификации X.509, в IPSec-совместимое ПО. Это означает, что IPSec можно легко интегрировать в инфраструктуру PKI, которая уже рассматривалась в этой главе. Интеграция протокола IPSec и инфраструктуры PKI обеспечивает еще больший уровень защищенности сети.

Теперь следует рассмотреть принципы работы протокола IPSec.

1. Сначала компьютер *А* отправляет данные компьютеру *Б* по незащищенной IP-сети. Прежде чем начнется передача данных, соответствующий алгоритм на компьютере *А* проверит, как должны быть закодированы данные в соответствии с определенной на этом компьютере политикой безопасности. Правила политики безопасности определяют, насколько безопасным является подключение.
2. После определения необходимых фильтров, компьютер *А* устанавливает соединение с компьютером *Б*, используя протокол IKE (Internet Key Exchange, протокол обмена ключами в Интернете). Затем компьютеры обмениваются необходимыми идентифицирующими их сведениями в соответствии с методом идентификации, определенным правилом безопасности. В качестве метода аутентификации могут использоваться протокол Kerberos, сертификаты открытого ключа и т. д.

3. Как только соединение между компьютерами будет установлено, определяется один из двух типов соглашений, называемых безопасными связями (SA, Security Association). Первый тип, Phase I IKE SA, определяет, на какой основе будут базироваться доверительные отношения между компьютерами. Второй тип соглашения определяет, каким образом компьютеры будут обеспечивать безопасность взаимодействующих приложений. Протокол IKE отвечает за автоматическое создание и обновление общего ключа для каждого соглашения SA. А закрытые ключи создаются на обоих концах соединения, что избавляет от необходимости передавать их по сети.
4. Компьютер *А* подписывает все исходящие пакеты, подтверждая их целостность, а также шифрует пакеты в соответствии с раньше определенными методами. После этого пакеты передаются компьютеру *Б*.
5. Компьютер *Б* проверяет целостность полученных данных и декодирует их. После этого данные передаются приложению.

Несмотря на то, что протокол IPSec изначально предназначался для обеспечения защиты данных в незащищенных сетях, он также может применяться и во внутренних сетях, особенно тех из них, которые созданы на основе Windows 2000 Server (Windows XP).

Протокол SSL

Повышение степени безопасности передаваемых по сети данных обеспечивается также с помощью *протокола SSL* (Secure Sockets Layer, уровень безопасности сокетов). Этот протокол реализует комбинацию криптографической системы с открытым ключом и блочное шифрование данных. Протокол SSL выполняется на прикладном уровне модели OSI, поэтому его поддержка должна включаться в состав приложений.

Изначально протокол SSL был разработан компанией Netscape и предназначался для защиты браузера Netscape. В настоящее время его поддержка внедрена в браузере Internet Explorer, а также в некоторых других менее распространенных браузерах. С помощью этого протокола реализуется защищенный канал связи между браузером и веб-сервером, используемый в процессе проведения банковских транзакций, а также при передаче других важных данных.

Протокол Kerberos

Работа *протокола Kerberos* основана на совокупности билетов, которые представляют собой пакеты кодированных данных, выдаваемые центром распространения ключей КОС (Key Distribution Center). Билет выступает в роли своего рода сертификата, хранящего различные секретные данные. Каждый центр распространения ключей КОС отвечает за определенную сферу. В среде Windows 2000 отдельной сферой является каждый домен. Кроме того, каждый контроллер домена Active Directory выступает в роли центра распространения ключей КОС.

Когда пользователь регистрируется в Windows 2000, локальные средства защиты LSA (Local Security Authority) выполняют авторизацию, предоставляя ему билет TGT (Ticket Granting Ticket, билет для получения билета), выступающий в качестве некоего пропуска. Затем, когда пользователю потребуется доступ к определенным ресурсам сети, он предъявит свой билет TGT контроллеру

домена и запросит билет для получения доступа к ресурсу. Билет на доступ к определенному ресурсу также известен как билет службы ST (Service Ticket). Если требуется получить доступ к ресурсу, то билет службы предоставляется ресурсу. После этого пользователь получает доступ к ресурсу, а его права в этом случае будут определяться списком контроля доступа ACL для этого ресурса.

Реализация протокола Kerberos в Windows 2000 полностью совместима с пятой версией этого протокола, разработанной проблемной группой проектирования Интернета (IETF), изначально созданного в Массачусетском технологическом институте. Эта спецификация поддерживается многими производителями ПО, поэтому билеты, выданные в домене Windows 2000 (сфере протокола Kerberos), принимают другие области, среди которых есть сети Mac OS, Novell NetWare, UNIX, AIX, IRIX.

Таким образом, между контроллерами доменов Kerberos (KDC, Kerberos Domain Controller) в соответствующих доменах можно устанавливать доверительные отношения. Эти отношения работают точно так же, как и доверительные отношения Windows NT, настраиваемые между главными контроллерами доменов POC. А поскольку Windows 2000 поддерживает NT LAN Manager (NTLM), то поддерживаются и доверительные отношения с наследуемыми доменами Windows.

Однако протокол Kerberos требует более тонкой настройки и администрирования, чем для доменов Windows NT при использовании NTLM. Это связано с тем, что пользователи должны проходить проверку со стороны контроллера домена Kerberos несколько раз в день. Например, если пользователь работает в сети 6 часов подряд, ему придется пройти проверку 6–8 раз. Если домен поддерживает 1000 пользователей, это приведет к восьми тысячам обращений к контроллеру домена Kerberos.

Кроме того, доверительные отношения между неоднородными сетями не настолько прозрачны, как между доменами Active Directory, когда контроллеры домена явным образом гарантируют лояльность всех своих пользователей. Доверительные отношения между лесами Windows 2000, Windows NT и другими областями должны быть настроены вручную администратором. Процесс настройки доверительных отношений в доменах UNIX или IRIX может значительно отличаться от настройки доверительных отношений между доменами Windows 2000.

В процессе планирования сети, в которой будут присутствовать несколько доменов, взаимодействующих через глобальную сеть, следует наилучшим образом настроить маршруты, которые бы использовались при передаче билета из одного домена в другой. Ярлыки понадобятся для того, чтобы снизить влияние процесса *аутентификации* на сетевой трафик.

В данном случае под аутентификацией понимается процесс регистрации пользователя в сети.

Электронная почта — источник повышенной опасности

Многие пользователи полагают, что безопасность электронной почты сродни безопасности при отсылке писем в обычных конвертах. И здесь они серьезно ошиба-

ются. Даже обычные письма могут просматриваться во время их долгого пути от отправителя до получателя корреспонденции (закон о перлюстрации почтовой корреспонденции еще никто не отменял), ну, а электронные письма представляют собой обыкновенные текстовые файлы, передаваемые в Интернете. И слишком много любопытных глаз могут ознакомиться с их содержимым — иногда просто из праздного любопытства, а порой в силу суровой служебной необходимости (рис. 10.9).

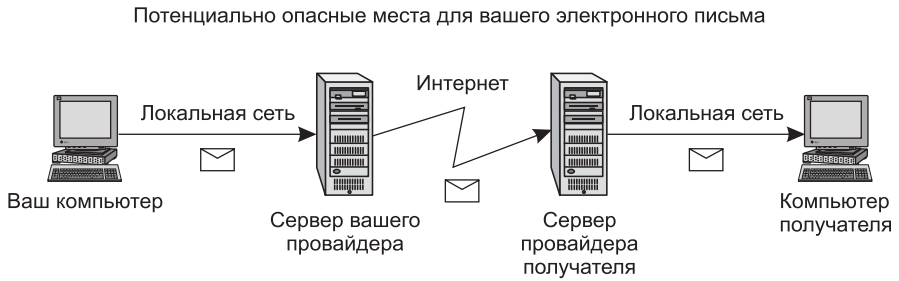


Рис. 10.9. Утверждение о защищенности электронной почты — всего лишь только миф

Конечно, перехват электронных сообщений — это очень печально, но гораздо хуже будет, если кто-либо перехватит ваше письмо, изменит его содержимое и отошлет дальше по первоначальному адресу. В этом случае вашей репутации может быть нанесен непоправимый урон, не говоря уже о том, что могут быть и прямые финансовые убытки.

Обратите внимание на потенциальную опасность почтовых вложений в получаемых вами письмах. Эти файлы являются удобнейшей средой распространения для вирусов, червей и троянских коней. Также может представлять опасность сценарий, написанный хакером, или даже непроверенный элемент управления ActiveX, включенный в HTML-сообщение.

К счастью, существуют относительно простые средства, при помощи которых можно нейтрализовать многочисленные угрозы. Например, потенциальную опасность почтовых вложений можно свести к минимуму, если перед открытием такого файла воспользоваться антивирусной программой. Защиту от подобных вложений также обеспечивает распространенный почтовый клиент Microsoft Outlook 2000. При работе с Internet Explorer можно воспользоваться зонами безопасности с целью защиты от вирусного кода, вмонтированного в электронные сообщения. Открытый ключ шифрования гарантирует тайну электронной переписки, а цифровая подпись подтверждает подлинность и целостность почтовых сообщений.

Защита от опасных почтовых вложений

Каждый вложенный файл электронной почты может служить потенциальной угрозой безопасности вашего компьютера. Поэтому следует относиться с подозрением ко всем входящим почтовым вложениям, поступившим из любого источника, даже если обратный адрес отправителя заслуживает доверия. Никогда не запускайте или не открывайте почтовые вложения независимо от их происхождения, пока не осуществите проверку с помощью новейшей версии антивирусной программы. Даже если ваша антивирусная программа не настроена на сканирование

входящих почтовых сообщений, она будет обезвреживать любое инфицированное почтовое вложение в случае попытки его запуска или сохранения. Если вы не уверены в том, что ваша антивирусная программа сможет обеспечить автоматическую защиту, сохраняйте все вложенные файлы на жестком диске, а затем проверяйте их вручную до открытия.

Этот совет относится как к файлам, содержащим документы, так и к исполняемым файлам. Макроязыки, встроенные в современные приложения (например, Microsoft Visual Basic for Applications, который поддерживается Microsoft Office и многими другими программами), позволяют встраивать в файлы документов вирусный код, обладающий разрушительными возможностями. Если запустить подобный макрос на выполнение без предварительной проверки, то могут пострадать важнейшие ресурсы системы. Даже рабочая книга Microsoft Excel (файл с расширением .xls) или документ Microsoft Word (файл с расширением .doc) могут обладать такими же разрушительными возможностями, как и исполняемая программа. Следует еще больше внимания уделять безопасности макросов в случае применения устаревших версий Microsoft Office, особенно Office 97. Версии Office XP и Office 2000 значительно безопаснее. Особенно если установлены соответствующие обновления. В этих программах по умолчанию выбирается высокий уровень защиты от макросов (High), что позволяет блокировать запуск неподписанных макросов, которые не вызывают доверия.

Существует достаточно много программ от независимых производителей, которые обеспечивают защиту электронных сообщений. Ниже указаны лишь некоторые из них:

- Micrisoft AntiSpyware;
- Kerberos;
- PSP (Pretty Good Privacy).

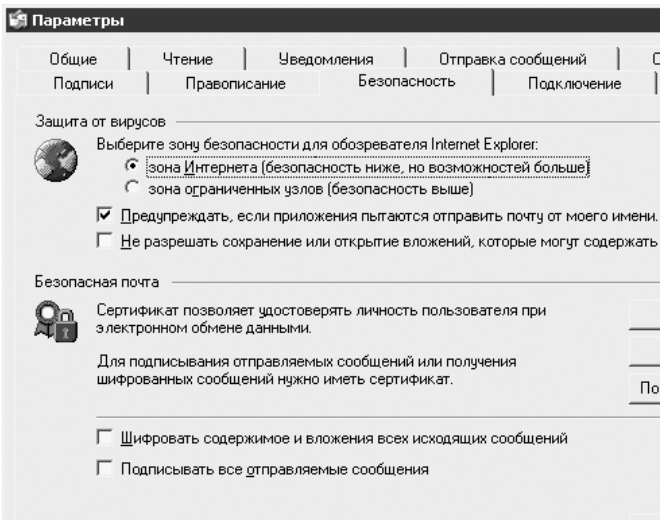


Рис. 10.10. Пользователи этой популярной почтовой программы достаточно неплохо защищены

Возможности по защите электронных сообщений предоставляет такая популярная программа, как Microsoft Outlook Express от шестой версии и выше. Эта программа, обеспечивающая возможность получения цифровых сертификатов, может кодировать сообщения и почтовые вложения. На рис. 10.10 представлено окно этой программы, в котором можно установить параметры цифровых сертификатов и шифрования сообщений.

Брандмауэры и прокси-серверы

Чтобы обеспечить большую степень безопасности, иногда требуется изолировать локальную сеть от внешнего мира. Эта задача решается при помощи *брандмауэров* и *прокси-серверов*, работающих как барьер между сетями и Интернетом.

Брандмауэр может быть аппаратным или программным. Более подробное описание этих устройств приведено в следующих разделах.

ПРИМЕЧАНИЕ Пользователи Windows XP могут воспользоваться встроенным программным брандмауэром, что настоятельно советует фирма Microsoft.

Аппаратные брандмауэры

В самом начале компьютерной эпохи безопасность можно было обеспечить при помощи пароля на компьютере и замка на двери вычислительного центра. Но появление компьютерных сетей в корне изменило ситуацию. Внезапно обнаружилось, что старые добрые замки и пароли уже не могут защитить информацию, потенциальные взломщики больше не нуждаются в непосредственном доступе к клавиатуре и экрану. Вместо этого они могут использовать любой компьютер, присоединенный к сети. Появление сетей порадовало также начинающих хакеров и мелких жуликов, изготовляющих устройства, с помощью которых можно обманывать телефонные компании, делая звонки за чужой счет.

Отдельно от этой группы стоят хакеры, извлекающие выгоду из проникновения в конфиденциальные и важные для бизнеса сети. В прошлом большинство пользователей не обращали внимания на эту угрозу. В те благословенные времена сеть Интернет пребывала в зачаточном состоянии, обслуживая немногочисленные научные и учебные учреждения. Несмотря на это некоторые организации, работающие в Сети, решили разработать систему защиты, и одной из них была Bell Labs, установившая шлюз от несанкционированного доступа в свою сеть, объединявшую более 1300 компьютеров.

Пробуждение наступило в 1988 году, когда молодой человек по имени Роберт Моррис, сын компьютерного специалиста, решил продемонстрировать свое умение и запустить в Интернет первого компьютерного червя. Эта программа не была столь уж опасной и не наносила никакого вреда, но когда она начала распространяться через Сеть по всему миру, стало понятно, каков мог бы быть ущерб, будь червь более деструктивным. Этот червь не смог проникнуть в сеть Bell-Labs, но в других местах копии этой программы захватывали все новые и новые системы. Буквально в одночасье появилась новая отрасль, призванная утолить жажду безопасности в корпоративных сетях. Эта отрасль стала заниматься шлюзами, предназначенными для того, чтобы не пускать в сети неавторизованных пользо-

вателей, в том числе хакеров. Такие шлюзы стали называть брандмауэрами (firewall), потому что они останавливают пожар, не позволяя ему распространиться по всему зданию.

Брандмауэр — это регулятор доступа к локальным сетям. Он напоминает охранника, стоящего при входе. Страж останавливает посетителей, по документам устанавливает личность и цель визита, при удовлетворительных ответах пропускает посетителя иначе — блокирует доступ. Часто охранник ведет книгу записи посетителей. Брандмауэр тоже устанавливается у входа в корпоративную или внутреннюю сеть, и все коммуникации проходят через него. Но при этом шлюз становится узким местом, как для обычных пользователей, так и для злоумышленников. Информационный поток между корпоративной сетью и внешним миром неизбежно замедляется, но цена этому — возросший уровень безопасности. При снижении требований злоумышленники могут проникнуть внутрь.

Коммерчески распространяемые брандмауэры различаются как по архитектуре, так и по наборам выполняемых функций. Архитектура в основном представлена двумя типами: *пакетные фильтры* и *брандмауэры прикладного уровня*. Пакетные фильтры анализируют приходящие IP-пакеты и принимают решение об их принятии на основе правил, запрограммированных при их настройке. Брандмауэры, имеющие подобную архитектуру, считаются более быстрыми и более гибкими. Брандмауэры прикладного уровня не пропускают непосредственно ни одного пакета извне. Все пакеты вместо этого направляются специальному приложению, называемому прокси-сервер, который и решает, устанавливать соединение или нет. Брандмауэры этой архитектуры работают медленнее, и они менее гибки.

Брандмауэр Firebox от фирмы WatchGuard Technology основан на смешанной архитектуре динамической фильтрации пакетов и «прозрачного» прокси-сервера. Подобная комбинация обеспечивает оптимальный баланс между безопасностью и производительностью. Динамическая фильтрация пакетов отслеживает состояние соединения, что позволяет не только отфильтровывать пакеты, но и контролировать соединения. Динамические наборы правил должны быть изменены непосредственно во время работы. Прозрачный прокси-сервер анализирует трафик на сетевом уровне.

Такой анализ на высшем уровне позволяет получить более надежную защиту. Правила, по которым ведется защита, могут определяться пользователем самостоятельно исходя из имеющихся потребностей и угрозы безопасности. Кроме того, брандмауэр Firebox может распознавать подмену сервисов и пакетов. В дополнение к этому имеется функция регистрации пользователей, что позволяет не только повысить безопасность, но и вести мониторинг сети на основе имен пользователей. Для регистрации используется URL, имеющийся на самом брандмауэре.

Firebox может работать как с собственным сервером регистрации, так и с сервером доступа домена Windows NT. Он поддерживает функционирование сетей VPN, т. е. позволяет устанавливать безопасный доступ в корпоративную сеть через Интернет для авторизованных удаленных пользователей. Чтобы установить соединение, используется протокол PPTP (Point-to-Point Tunneling Protocol, протокол туннелирования «точка-точка»). Протокол создает в общей сети безопасный туннель, через который и передается трафик. Адаптированная операционная

система при включении загружается с гибкого диска, на нем же сохраняется конфигурация. Брандмауэр устанавливается в стойку или на стол.

Брандмауэр PIX от Cisco Systems также построен на основе смешанной архитектуры. Основные его возможности — поддержка алгоритма адаптивной безопасности, отслеживающего возвращаемые пакеты и для минимизации риска его атаки меняющего номер последовательности TCP. Он поддерживает трансляцию адресов исходящих пакетов для того, чтобы вовне не были известны внутренние IP-адреса, и трансляцию адресов портов. Также гарантируется поддержка VPN и идентификация пользователей. Идентификация соединения происходит на уровне приложений, а в дальнейшем трафик идет через более быстрый фильтр пакетов. Возможна установка двух брандмауэров, один из которых находится в горячем резерве. Количество одновременно поддерживаемых соединений — более 500. Брандмауэр располагает адаптированной ОС реального времени. Для конфигурации и настройки используется порт RS-232, возможна установка до трех сетевых адаптеров.

Интересное решение нашла компания Bay Networks, применившая в качестве брандмауэров маршрутизаторы собственного производства. В самом деле, уже существует устройство, установленное в сети и выполняющее функции передачи пакетов. Почему бы ему, в таком случае, не поручить задачу сортировки этих пакетов? Вычислительные возможности маршрутизаторов BCN старшей модели производят должное впечатление. В них возможна установка до восьми процессоров (MC68040, MC68060 или PowerPC). Не каждый сервер способен на такое. Учитывая, что маршрутизаторы работают на сетевом уровне модели OSI, они должны иметь высокопроизводительную сетевую ОС, которую вполне можно нагрузить дополнительными приложениями, тем более что полностью загрузить подобное устройство трудно. Таким образом, брандмауэр от Bay Networks, с одной стороны, представляется чисто программным средством (адаптированная система разработки Check Point Software), но с другой стороны, он не использует компьютер общего назначения, устанавливается в стойке и во всем остальном похож на другие брандмауэры, за исключением того, что кроме заботы о безопасности он выполняет еще и некоторые другие функции. Разница состоит только в том, что аппаратные брандмауэры — это специализированные компьютеры, предназначенные для выполнения одной задачи. Маршрутизатор — также специализированный компьютер, но его специализация оказалась гораздо шире, чем было изначально задумано.

Программные брандмауэры и прокси-серверы

Программный маршрутизатор — это специальная программа, которая отфильтровывает вредную и ненужную информацию. Прокси-сервер является посредником при реализации сетевых соединений. Функционирование прокси-серверов аналогично работе программных брандмауэров.

Далее приводится описание двух распространенных программ, которые могут выполнять функции программных брандмауэров.

Программа *GFI LANguard Network Security Scanner (NSS)* изначально предназначалась для проверки локальной сети на предмет выявления возможных уязвимостей в системе безопасности. В результате сканирования локальной сети отобра-

жаются такие сведения, как перечень установленных на компьютере сервисных пакетов, наличие или отсутствие заплат в системе безопасности, открытые порты, а также некоторые другие данные. В случае отсутствия требуемых «заплат» и/или сервисных пакетов обеспечивается их автоматическое развертывание на уровне всей сети.

На рис. 10.11 приведен экран программы GFI LANGuard Network Security Scanner.

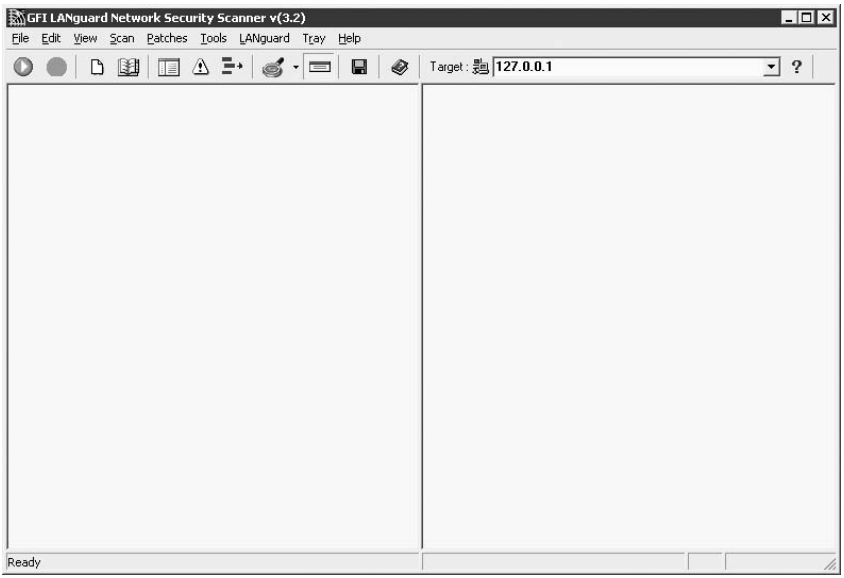


Рис. 10.11. Диалоговое окно программы GFI LANGuard Network Security Scanner

Для установки программы GFI Network Security Scanner требуется операционная система Windows 2000/2003, а также обозреватель Internet Explorer версии 5.1 и выше. В процессе инсталляции потребуется до 10 Мбайт свободного места на жестком диске компьютера.

Чтобы начать новый просмотр состояния сети, достаточно выполнить команду меню File ▸ New (Файл ▸ Новый). В результате выполнения этих действий на экране отображается всплывающее окно, в котором можно указать диапазон просматриваемых IP-адресов. Нужно выбрать параметр Just Scan the Internal Network (Обычный просмотр локальной сети) и нажать кнопку Finish (Готово). На основной панели инструментов GFI LANguard нужно нажать кнопку Play (Воспроизвести). После этого начнется процесс просмотра сети.

После выполнения всех перечисленных ранее действий программа GFI LANguard Network Scanner начинает просмотр локальной сети. Сканирование отдельных узлов/компьютеров, входящих в состав локальной сети, осуществляется с помощью зондов NETBIOS, команд ping или SNMP-запросов.

После завершения сканирования сети на левой панели отобразится список всех сетевых компьютеров. Если щелкнуть мышью на одном из них, отобразится перечень информационных узлов, характерных для данного компьютера. Правее

имени компьютера и связанного с ним IP-адреса находится уровень, соответствующий операционной системе и ее сервисным пакетам. Вполне естественно, что следует устанавливать сервисные пакеты самых последних версий.

Первый узел, изображенный на панели, содержит связанные с протоколом NetBIOS сведения (перечень служб, текущие зарегистрированные пользователи и т. д.).

Второй узел на панели содержит перечень доверенных доменов. Этот перечень формируется только в том случае, если компьютер входит в состав домена. Убедитесь в том, что домены на самом деле являются доверенными, а установленные меры безопасности соответствуют требуемому уровню.

Следующий узел содержит перечень всех общих сетевых ресурсов. Работа с подобными ресурсами чревата определенной степенью опасности, если не обеспечивается адекватный уровень защиты. Именно поэтому администраторы должны убедиться в том, что:

- ни один из пользователей данного компьютера не предоставляет весь свой диск для общего доступа из сети;
- заблокирован анонимный/несанкционированный доступ к общим сетевым ресурсам;
- отсутствует общий доступ к начальным папкам или системным файлам.

Перечисленные соображения играют важную роль, когда для сетевых компьютеров критичным моментом является системная интеграция, например для общих контроллеров доменов (Public Domain Controller). Легко представить себе ситуацию, когда администратор устанавливает общий доступ для начальной папки на компьютере PDC всем пользователям. С помощью соответствующих прав доступа пользователи могут легко копировать исполняемые файлы, и, следовательно, вытворять с ними все что угодно до тех пор, пока администратор повторно не зарегистрируется в системе.

ВНИМАНИЕ Если процесс сканирования сети инициирован владельцем учетной записи администратора, на экране отображаются административные сетевые ресурсы, например «C$ — сетевой ресурс, определенный по умолчанию». Эти ресурсы недоступны пользователям с обычными полномочиями.

Следующие два узла отображают локальных пользователей и группы, которые находятся на данном компьютере. Убедитесь в том, что отсутствуют дополнительные пользовательские записи, а также отключите гостевую учетную запись. Нельзя забывать о том, что найдется достаточно много желающих проникнуть в систему с «черного хода»! Если раскрыть узел пользователей, то можно будет проанализировать активность учетной записи. В идеальном варианте пользователь не должен применять локальную учетную запись для регистрации. Также нужно удостовериться, что частота смены паролей достаточно велика.

Необходимо отключить все службы, которые не используются в данный момент! Помните о том, что каждая служба представляет потенциальный ущерб для системы безопасности, поэтому отключение ненужных служб приводит к автоматическому уменьшению степени риска.

В узле общей информации перечислены сетевые устройства, диски, а также выводится общая информация о компьютере. В узле парольной политики отображаются важные настройки. Нужно убедиться в том, что политика паролей защищена, пароли будут меняться со временем, а история паролей хранится в особом журнале.

Легко заметить, что эта программа обладает широким спектром возможностей, в связи с чем может использоваться в локальных сетях для выполнения разнообразных функций.

Программа *Zone Alarm Pro* от фирмы Zone Labs реализует функции программного брандмауэра. Установка ZoneAlarm не составляет труда, а параметры, используемые по умолчанию, сразу обеспечивают два уровня защиты — средний для локальной сети и высокий для работы в Интернете. При этом весь трафик будет заблокирован до тех пор, пока не будут изменены установки. Это значит, что как только какое-либо приложение попытается осуществить выход в Интернет, ZoneAlarm оповестит об этом пользователя и потребует подтверждения. Специальные установки, правда, позволяют сконфигурировать работу в Интернете более гибко. Можно выбрать приложения (например, Internet Explorer или Outlook), подключение которых не будет требовать авторизации.

Вся текущая информация о блокировке/доступе к Интернету той или иной программы будет отображаться в небольшом окошке, которое располагается в верхней части экрана.

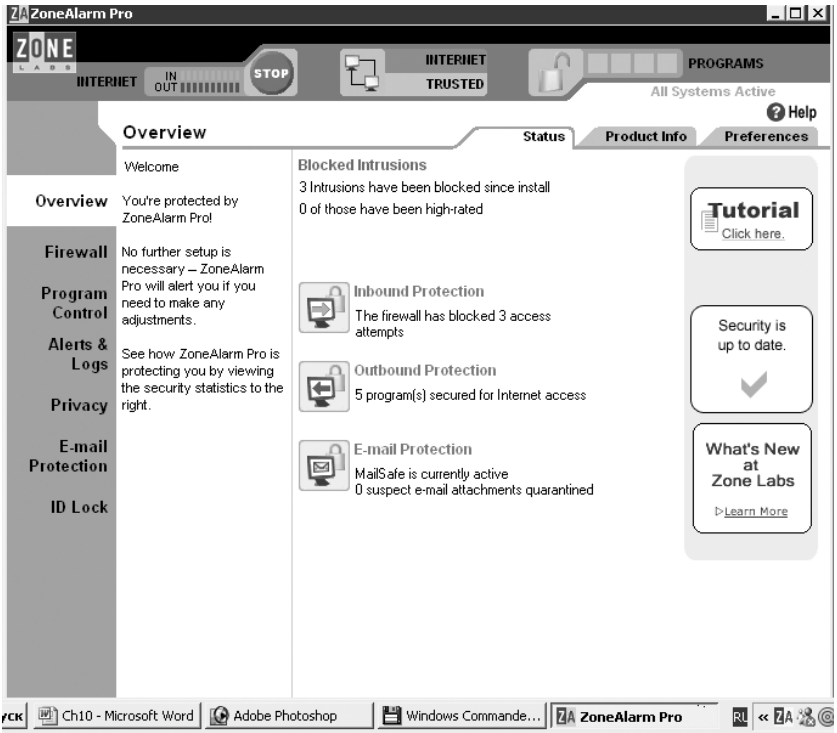


Рис. 10.12. Диалоговое окно программы Zone Alarm Pro

Неплохие возможности предоставляет кнопка Emergency Stop (Срочная остановка). С ее помощью можно немедленно заблокировать передачу любой информации в Интернет, если, например, началась несанкционированная передача данных. С помощью инструмента Automatic Lock можно приостановить связь с Интернетом при активации хранителя экрана либо после заданного периода времени, что поможет предотвратить несанкционированный доступ к компьютеру во время отсутствия пользователя. А одной из самых приятных возможностей ZoneAlarm является его способность автоматически закрывать неиспользуемые и простаивающие порты и даже полностью заблокировать все порты системы.

Хотя ZoneAlarm не антивирусная программа, она может отфильтровать входящие сценарии на Visual Basic. Кроме того, ZoneAlarm может самостоятельно обновляться через Интернет, что позволит поддерживать средства защиты на должном уровне.

Программу ZoneAlarm по праву можно назвать одним из лучших персональных брандмауэров как с точки зрения обширности инструментария, так и с точки зрения эффективности работы (рис. 10.12).

Возможно, одним из наилучших брандмауэров на сегодняшний день является Microsoft AntiSpyware. Я использую в работе тестовую бесплатно распространяемую версию (Beta 1). Эта программа автоматически находит и загружает из Интернета обновления, позволяет защищать компьютер в режиме реального времени, блокируя возможные хакерские атаки из Интернета, а также активизацию различных «вредоносных» программ, которые проникают в систему или принимаются в качестве почтовых вложений. Возможно также провести сканирование системы в заданный промежуток времени согласно заранее составленному календарному графику.

Диалоговое окно программы показано на рис. 10.13.

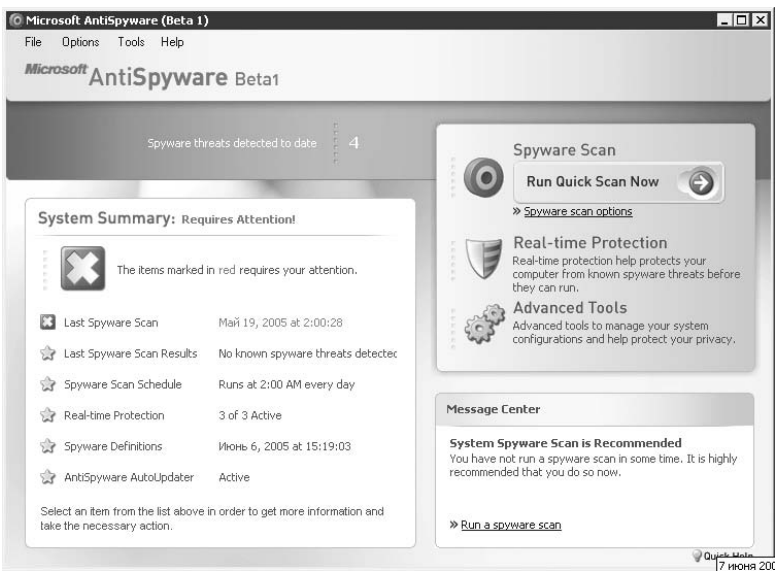


Рис. 10.13. Наилучший программный брандмауэр в своем классе

Физические способы обеспечения безопасности

Хорошо продуманная стратегия обеспечения сетевой безопасности должна предусматривать блокирование *физического доступа* к сети. К сожалению, этому важному фактору не всегда уделяется должное внимание.

К серверам и соединительным устройствам предъявляются высокие требования по обеспечению безопасности, поэтому их следует размещать в комнатах, запираемых на замок. Если же сервер находится в общей комнате, следует контролировать доступ к нему при помощи различных систем программной и аппаратно реализованной сигнализации. Сетевые кабели следует прокладывать в коробах, что затруднит доступ к ним потенциальных злоумышленников.

Осторожнее с ноутбуками

Как известно, недостатки — обратная сторона достоинств. Вот и достоинства портативных компьютеров оборачиваются недостатками,— ноутбуки очень часто пропадают. Иногда их где-то забывают, но еще чаще крадут. Причем убытки от кражи могут многократно превышать стоимость украденного компьютера. Неудивительно, что многие компании пытаются найти способы обезопасить пользователей от утечки данных и вернуть украденный компьютер. Очередной такой способ предложен совместно компаниями Phoenix Technologies и Softex.

Созданная ими небольшая программа TheftGuard работает подобно совершенным противоугонным системам для автомобилей. Утилита скрытно выполняется на ноутбуке и всякий раз, когда компьютер подключается к Интернету, подает сигнал серверу TheftGuard. Начиная с этого момента владелец компьютера (если, конечно, не он сам работает на своей машине) может отдать через Сеть команду удалить данные с жесткого диска и/или полностью отключить питание, сделав украденный ноутбук неработоспособным. Можно даже отследить сетевой адрес и попробовать поймать злоумышленника.

В принципе, подобных программ немало. Новизна TheftGuard заключается в том, что одна часть программы записывается в BIOS, а другая — на жесткий диск, в области? Которые не используются операционной системой. Как утверждает Phoenix, злоумышленникам не поможет даже установка в систему нового винчестера, поскольку часть программы, записанная в BIOS, проверяет целостность исходного состава аппаратуры. Перепрошивка BIOS также не снимет защиту.

Программа TheftGuard использует технологию Core Managed Environment, которую Phoenix представила в начале 2003 года. По сути, она является отдельной защищенной операционной системой, которая позволяет запускать заранее определенные приложения, причем их целостность гарантирована цифровой подписью. В числе таких приложений могут быть средства восстановления основной операционной системы, антивирусные программы и иные приложения.

Защита сети от разрушения

К потере ценных данных могут привести отказы оборудования, стихийные бедствия, а также технические ошибки персонала. Поэтому стратегия, предусматривающая защиту сети, должна учитывать необходимость резервирования данных.

В частности, защита от краха и восстановление предусматривает выполнение следующих действий:

- резервирование энергоснабжения;
- резервное копирование данных;
- обеспечение отказоустойчивости дисков;
- повышение отказоустойчивости серверов (кластеризация).

А теперь рассмотрим каждый из этих вопросов немного подробнее.

Резервирование энергоснабжения

Достаточно часто происходят потери ценных данных из-за нестабильности сети энергоснабжения. Действие этих факторов можно свести к минимуму, если воспользоваться специальным оборудованием. Бороться с нестабильным энергоснабжением можно при помощи фильтров электропитания, источников бесперебойного питания или автономных электрогенераторов.

Фильтр электропитания предназначен для подавления скачков напряжения, которые могут возникать во время грозы или из-за банального сложения трех фаз, когда напряжение в сети может достигать 380 В. Последствия подобного происшествия нетрудно себе представить. Поэтому применение подобных фильтров — это тот минимум, который должен быть предусмотрен при эксплуатации локальной сети, хотя они и не защищают от понижения напряжения или полного его пропадания.

В этом случае применяются источники бесперебойного питания, которые позволяют поддерживать энергоснабжение компьютеров в течение 5–20 минут после пропадания питающего напряжения. Этого времени обычно достаточно для корректного завершения выполнения программ и отключения компьютера. Поэтому подобный блок бесперебойного питания следует использовать, как минимум, для файл-сервера. Экономить на этом устройстве не следует, так как пропажа ценных данных обойдется гораздо дороже!

Если же напряжение в сети пропадает часто и надолго, либо к надежности энергоснабжения компьютерного оборудования предъявляются особо высокие требования, следует воспользоваться автономным генератором. Цена этих устройств достаточно высока, поэтому их применение должно быть обоснованным.

Резервное копирование данных

Иногда все же происходит непоправимое, и ваш сервер или даже вся сеть выходит из строя. И в этом случае должны помогать резервные копии. Перед разработкой плана резервного копирования следует ответить на следующие вопросы.

- Какие файлы нужно выбрать для копирования?
- Когда следует выполнять резервное копирование?
- Каким образом выполняется копирование?
- Зачем его нужно выполнять?

От успешного ответа на эти вопросы зависит успех всего мероприятия.

Естественно, что следует копировать только рабочие файлы. Файлы приложений и системы копировать не следует, поскольку их всегда можно установить с дистрибутивов. Резервные копии необходимо хранить в одном хорошо защищенном месте.

Резервное копирование должно быть регулярным. Расписание резервного копирования следует составить таким образом, чтобы эта операция выполнялась в нерабочее время. В расписание, как правило, включаются три основных вида резервного копирования.

- *Полное резервное копирование*. Копирование всех файлов из указанных дисков независимо от того, когда выполнялось копирование в последний раз, а также были ли с тех пор какие-либо изменения.
- *Разностное резервное копирование*. В данном случае копируются все файлы, которые были изменены с момента последнего полного копирования.
- *Добавочное резервное копирование*. Этот метод предусматривает копирование всех файлов, которые изменялись с момента любого последнего копирования, а не только со времени последнего полного копирования.

Полное резервное копирование занимает больше всего времени и места на носителях резервных копий, но зато гарантирует сохранность всех данных.

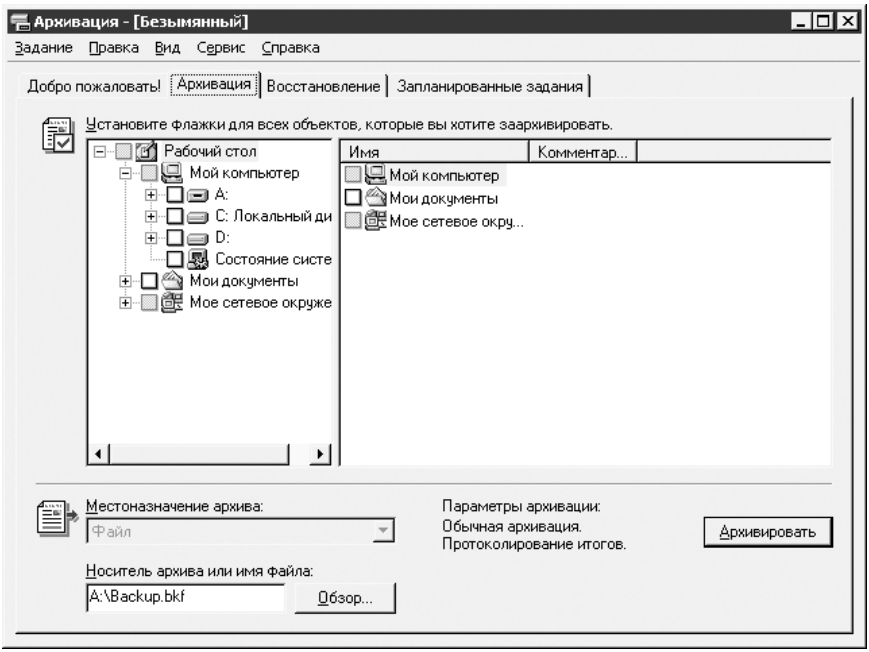


Рис. 10.14. Эта программа предназначена для выполнения резервного копирования (восстановления) данных

Разностное резервное копирование выполняется быстрее, но требует больше времени на восстановление данных. Это связано с тем, что восстановление данных выполняется с последней полной и последней разностной копий. Оптималь-

ный план резервного копирования предусматривает проведение полного копирования раз в неделю, а разностного — ежедневно.

Самым быстрым является добавочное резервное копирование, но для восстановления данных в этом случае нужна одна полная резервная копия и все добавочные копии, созданные с момента формирования последней полной копии.

План резервного копирования должен предусматривать выбор носителей резервных копий, программ резервного копирования, назначение ответственных лиц. В качестве носителей можно использовать традиционные магнитные ленты, а также многие другие носители (диски MO, CD-RW, Zip и т. д.). В качестве программ резервного копирования можно выбирать стандартные системные утилиты, входящие в комплект поставки сетевых ОС, либо программы от независимых поставщиков.

На рис. 10.14 показано окно программы резервного копирования, входящей в комплект поставки Windows 2000 Server.

Следует назначить ответственное лицо, выполняющее резервное копирование. В ОС Windows 2000 даже предусмотрена специальная учетная запись, называемая *оператор архива*. Особо ценные данные следует резервировать многократно, а копии хранить в надежных местах.

Особенности резервирования и восстановления данных в Windows XP

В Windows XP имеется собственная программа архивации (Все программы ▸ Стандартные ▸ Служебные ▸ Программа архивации). Программа архивации состоит из трех компонентов — мастер архивации, мастер восстановления и мастер аварийного восстановления системы. Каждый компонент следует рассмотреть подробнее.

Мастер архивации

Как и следует из названия этого мастера, его назначение заключается в подготовке и выполнении резервного копирования. После щелчка на значке мастера отображается диалоговое окно выбора архивируемых файлов, в котором пользователь может выбрать один из трех вариантов:

- архивировать все данные на этом компьютере;
- архивировать выбранные файлы, диски или сетевые данные;
- архивировать только данные состояния системы.

После щелчка на кнопке Далее появляется окно выбора носителя архивной копии. После завершения выбора щелкните на кнопке Далее, после чего начнется процесс архивирования. В диалоговом окне настройки параметров архивации (рис. 10.15) можно выбрать архивируемые данные, тип архива (команда Сервис ▸ Параметры).

В частности, можно выбрать следующие типы архивации (резервного копирования):

- обычный;
- копирующий;
- разностной;
- добавочный;
- ежедневный.

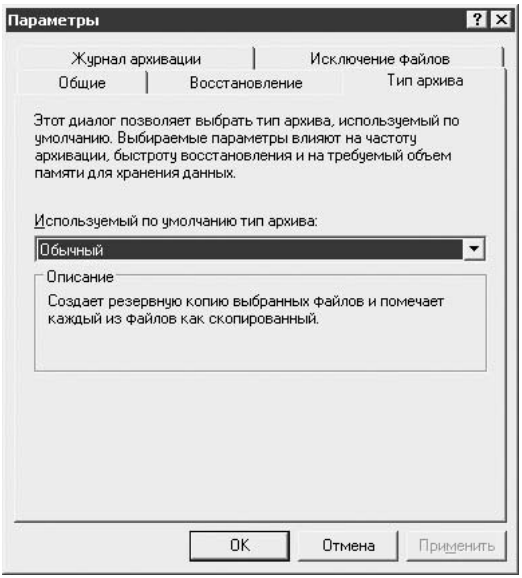


Рис. 10.15. В этом диалоговом окне указываются параметры резервного копирования

Мастер восстановления

Благодаря *мастеру восстановления* (рис. 10.16) можно восстановить заархивированные данные.

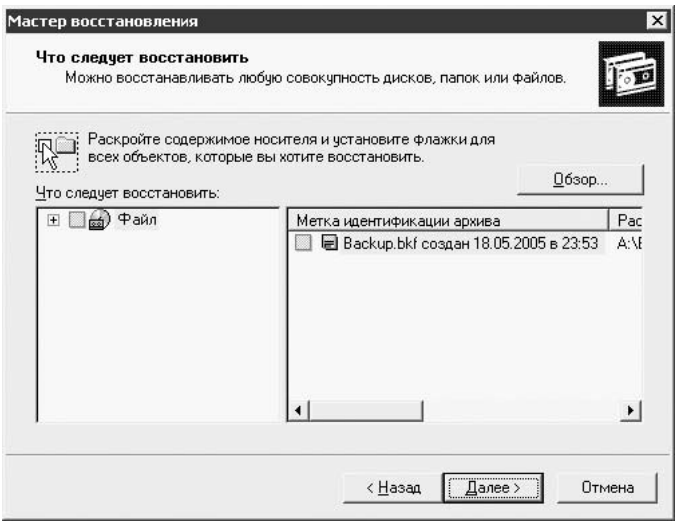


Рис. 10.16. Мастер восстановления данных

Мастер аварийного восстановления системы позволяет создать дискету аварийного восстановления системы (рис. 10.17).

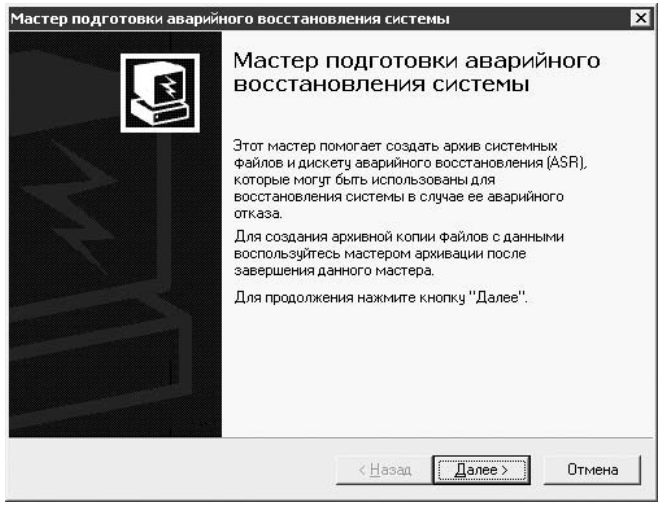


Рис. 10.17. Окно мастера аварийного восстановления системы

Восстановление системы

В Windows XP существует очень полезная *утилита восстановления системы.*

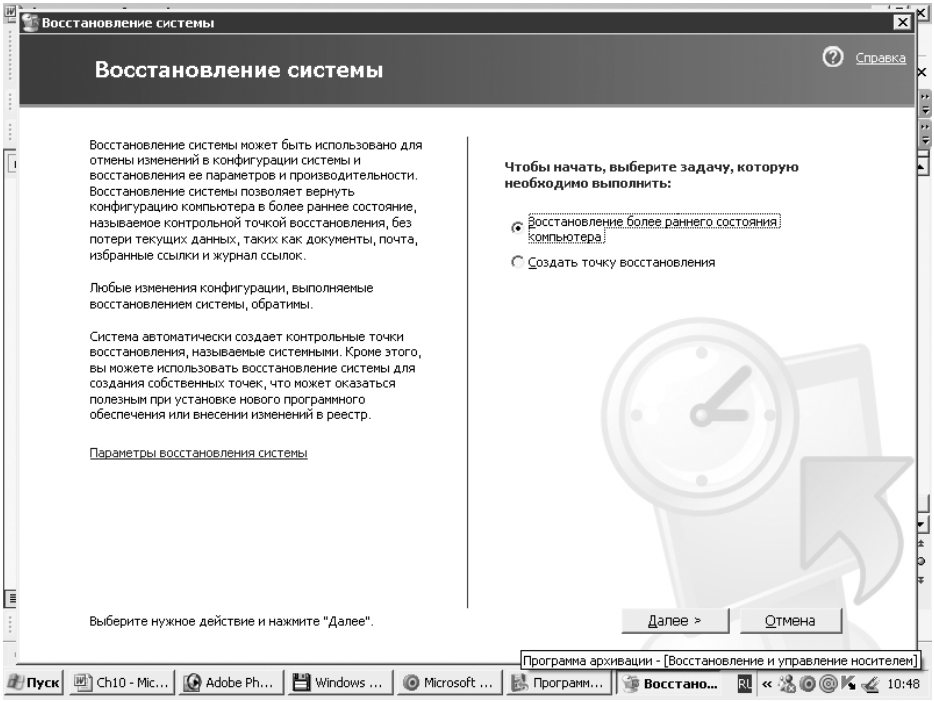


Рис. 10.18. Диалоговое окно утилиты восстановления системы

Утилита позволяет восстановить систему в случае каких-либо неполадок (аналог Last Known Good Configuration в Windows 2000 Server, но с удобным графическим интерфейсом и с большими возможностями). Команда запуска – Пуск ▸ Все программы ▸ Стандартные ▸ Служебные ▸ Восстановление системы. После запуска программы можно выбрать одну из следующих возможностей:

- Восстановление более раннего состояния компьютера;
- Создание точки восстановления.

Точки восстановления создаются по заранее разработанному расписанию, хотя возможно выполнение этой операции вручную. Диалоговое окно этой утилиты показано на рис. 10.18.

Обеспечение отказоустойчивости дисков

Обеспечение отказоустойчивости дисков повышает надежность хранения данных в сети. Для этого диски следует объединять в RAID-массивы.

ПРИМЕЧАНИЕ Вообще говоря, существует пять уровней RAID, причем современные системные платы часто снабжаются встроенными контроллерами RAID, вплоть до уровня 5.

Необходимо также производить мониторинг состояния дисков, используя сведения системы S.M.A.R.T.

Повышение устойчивости серверов

Один из методов повышения устойчивости серверов к сбоям — кластеризация. Этот метод описан в главе 6. Здесь следует отметить, что *кластеризация* предусматривает объединение нескольких серверов, в результате чего повышается степень отказоустойчивости всей системы.

На этом можно завершить большую главу, посвященную описанию средств и методов обеспечения безопасности локальных сетей. Следует отметить, что обеспечение безопасности системы — это комплексная проблема, требующая выполнения целого ряда мер, которые должны осуществляться последовательно и неукоснительно.

Поиск и устранение неисправностей

Хорошо, когда все идет хорошо и жизнь сетевого администратора не нарушают нештатные ситуации. Но на практике часто бывает иначе. В большой сети ежедневно и ежечасно могут возникать различные неисправности, и в задачи сетевого администратора входит своевременное их обнаружение и устранение. Описание соответствующих методик и инструментов находится в главе 11.

11 ГЛАВА Методики и инструменты, применяемые для поиска и устранения неисправностей

Сетевой администратор имеет дело не только с оборудованием, которое может выходить из строя в любое, порой самый неподходящее время, но и с нерадивыми пользователями, которые так и норовят запутаться ногами в сетевых кабелях или выдернуть из розетки шнур питания магистрального маршрутизатора. Естественно, что профилактика всегда лучше лечения, но следует знать, что же делать в том случае, когда сеть «заболела» и требует лечения.

Все не так уж и страшно, как может показаться с первого взгляда. Предположим, что вы прокладываете новую сеть, и нужно отобрать и протестировать кабели, а также продумать схему их расположения в офисе.

Проверяем кабели

Любая локальная сеть состоит из рабочих станций, соединенных с серверами с помощью множества кабелей. На самом деле хаос — кажущийся, за всем этим стоит хорошо организованная иерархическая структура. К тому же в настоящее время довольно часто используются беспроводные подключения, благодаря которым существенно уменьшается количество кабелей в локальной сети.

На первом этапе формирования любой локальной сети производятся работы по прокладке кабелей между рабочими станциями, серверами и другими сетевыми компонентами. Обычно этот этап выполняется на этапе строительства здания. Если же в силу каких-либо причин кабели заранее проложены не были, то рабочим придется вооружиться перфоратором и заняться подготовительными работами — пробиванию дырок в стенах и перекрытиях, а также созданию каналов, предназначенных для прокладки кабелей.

Затем следует подготовиться к этапу проверки кабелей. Инструменты, используемые для тестирования кабелей (как медных, так и оптоволоконных), бывают самые разные — от дешевых малогабаритных, при помощи которых сетевой администратор может выполнить простое тестирование кабеля, до очень сложных и дорогих устройств, применяемых опытными специалистами для выполнения тестирования и оценки полученных результатов. Проверяемые параметры сетевых кабелей приведены в следующем списке.

- *Длина кабеля*. Применяемая топология физической сети ограничивает длину используемого сетевого кабеля. При самостоятельном прокладывании кабелей попытка выйти за ограничения, накладываемые топологией, и проложить кабель хоть на несколько метров длиннее может привести к возникновению проблем.
- *Электрическое сопротивление*. От величины этого параметра напрямую зависит такая важная характеристика сетевого сигнала, как величина затухания. Если электрическое сопротивление слишком велико, следует задуматься о том, чтобы перейти со стального кабеля на медный, либо просто увеличить сечение применяемого кабеля. В крайнем случае, если сопротивление слишком велико, а поменять кабель не удастся, можно воспользоваться усилителем сигнала.
- *Электрические помехи*. Причины появления электрических помех могут быть самые разные. Так, причиной появления сильных электрических помех может служить некачественное заземление или полное отсутствие последнего, сильный «электрический смог», вызванный работой такого мощного оборудования, как прокатный стан или радиолокатор. В любом случае следует выявить причину появления электрических помех и предпринять меры для ее устранения. В частности, можно убрать кабели подальше от источников помех либо вместо неэкранированной витой пары (UTP) воспользоваться экранированной витой парой (STP).
- *Перекрестные помехи на ближнем конце (NEXT, Near-end cross-talk)*. Согласно законам физики, наиболее сильное излучение проводника, по которому проходит переменный ток, наблюдается на конце кабеля. Поэтому ни в коем случае не следует оставлять чрезмерно длинные оголенные жилы кабеля. Их следует обрезать до необходимой минимальной длины, а затем вставить каждую жилу до упора в контактный разъем.

В процессе проверки электрических и физических параметров кабелей используются два основных типа приборов — кабельные пробники и кабельные тестеры. Здесь напрашивается аналогия с радиоэлектроникой, где пробник позволяет «прозвонить» цепь, а с помощью тестера можно определить такие нетривиальные характеристики, как емкость и индуктивность контура. Ну а теперь остановимся подробнее на описании этих двух категорий приборов.

Приборы, применяемые для тестирования кабелей

Кабельный пробник обычно имеет небольшие размеры, использует автономный источник электропитания, а применяется он для проверки на предмет обрыва

кабелей витой пары. При помощи этого устройства можно быстро определить механические повреждения кабелей, возникающие в процессе их прокладки.

Если кабель уже подсоединен к сетевому устройству, необходимо отсоединить его и подключить к пробнику. Кабельный пробник работает при подаче напряжения на провод с последующим его детектированием на противоположном конце. Эта процедура используется для обнаружения разрывов кабеля по всей его длине, а также для определения одинаковых жил кабеля. Большинство кабельных пробников имеют два зонда, подключаемые к противоположным концам кабеля.

Кабельный тестер является достаточно сложным устройством и применяется для измерения таких параметров, как показатель NEXT, величина затухания, полное сопротивление, а также шум в кабеле. Некоторые модели кабельных тестеров позволяют оценить такие параметры, как общая длина кабеля и расстояние до поврежденного участка кабеля, например места перегиба. Этот же прибор позволяет проверить корректность подключения кабельных жил к соответствующим контактным выводам соединительного устройства, прикрепленного к концу кабеля. Скажем, в кабелях UTP, применяемых в сетях 10BASE-T, стандартом определены пары кабельных жил, которые должны использоваться для передачи и приема данных. Фактические решения о том, какие контакты выбираются для того или иного соединительного устройства, принимаются произвольно. Если провода неправильно подсоединены к выводам соединительного устройства, то кабель может создавать ошибки из-за шума или перекрестных помех.

Простейшие кабельные тестеры, как правило, снабжены светодиодными индикаторами, которые отображают результаты тестирования. Некоторые из этих устройств снабжены небольшим жидкокристаллическим дисплеем, на котором отображаются несколько текстовых строк, описывающих характер ошибок. Большинство устройств этой категории имеют универсальное электропитание — от аккумуляторов или от сети, благодаря чему они являются весьма полезными как при прокладке кабелей, так и при поиске и устранении повреждений ранее установленного кабеля.

Некоторые кабельные тестеры могут выполнять расширенные функции мониторинга, как, например, отображение коэффициента использования сети и частоты коллизий в сети Ethernet. Данные измерений могут обрабатываться компьютером, отображаться на экране или выводиться на печать. Благодаря этому можно организовать непрерывный мониторинг сети.

Стоимость кабельного тестера может варьироваться от нескольких сотен до нескольких тысяч долларов, в зависимости от характеристик того или иного конкретного устройства. При оценке различных тестеров нужно сравнивать их технические характеристики. Цена не всегда отражает качество товара. Поэтому при покупке всегда следует тщательно изучить прилагаемые к этим устройствам инструкции. Несмотря на то, что некоторые из характеристик, например возможность создания отчетов, могут выглядеть довольно привлекательно, стоит задуматься над тем, действительно ли они необходимы. Если вы имеете дело с большими сетями, то, возможно, вам это и пригодится, в противном случае — вряд ли.

Тестеры BERT позволяют оценить долю ошибочных фреймов по отношению к общему количеству фреймов. Эти тестеры обычно применяются при установке

соединения с провайдером сетевых услуг, и используются для демонстрации качества услуг предоставляемых провайдером для вашего канала связи.

В процессе измерения генерируется специальный битовый шаблон в одном месте линии, затем выполняется контрольный замер в другом ее месте, после чего сравниваются результаты измерений. При генерировании шаблона формируется псевдослучайная последовательность двоичных цифр, имитирующая случайную выборку данных. Если показатель количества ошибок чрезмерно высок, может быть полезно снижение скорости передачи данных.

Принцип действия *рефлектометров TDR* напоминает принцип действия радиолокаторов. Электрический сигнал характеризуется постоянной скоростью распространения в кабеле, если, конечно, проводник является однородным по всей своей длине. В месте повреждения часть мощности сигнала отражается обратно и улавливается приемником прибора. Зная скорость распространения сигнала в кабеле, нетрудно оценить расстояние до места повреждения.

Используя рефлектометр TDR, можно определить следующие виды повреждений кабеля:

- плохо скрученные или непропаянные жилы;
- повреждение кабеля влагой;
- обрыв или перегиб кабеля;
- короткие замыкания;
- проблемы с оплеткой кабеля;
- неплотное соединение и отсутствие контакта.

Рефлектометр TDR может также использоваться при измерении длины неповрежденного кабеля, в том числе намотанного на катушку. Подобная процедура обычно производится перед началом выполнения основных работ по прокладке кабеля, чтобы оценить, достаточен ли имеющийся его запас. Рефлектометр TDR может использоваться для измерения кабелей витой пары, коаксиальных кабелей и даже волоконно-оптических кабелей. Поскольку кабели из третьей категории являются наиболее дорогостоящими и обеспечивают при этом наибольшую скорость передачи данных, весьма желательно, чтобы рефлектометр TDR поддерживал работу с ними. В процессе прокладки кабелей следует проверять их пропускную способность, которая может снижаться по причине различных помех, например от расположенного рядом силового оборудования. Если зафиксировано снижение пропускной способности, возможно, благоразумнее будет просто проложить кабель в другом месте.

Более дорогие модели рефлектометров TDR оснащаются дисплеями, на которых визуально представлен излучаемый или отраженный сигнал. Этот прибор чем-то напоминает электронный осциллограф. В более простых моделях определяется расстояние до конца кабеля или повреждения, а также предусмотрен индикатор, отображающий информацию о типе повреждения.

Рефлектометр TDR позволяет также установить величину отклонения величины импеданса от характеристики, определенной стандартом. Кабели, используемые в локальных сетях, должны производиться в соответствии с характеристиками, гарантирующими постоянство характеристик применяемого изоляционного

материала, разделяющего жилы в кабеле. Если имеют место непроизвольные отклонения от заданных характеристик из-за производственного брака, то могут возникнуть проблемы с кабелем, что отобразится на производительности сети. Таким образом, рефлектометр TDR позволяет убедиться в том, что приобретенный кабель соответствует заявленным характеристикам.

Высококлассные рефлектометры TDR позволяют выбирать длительность импульса, которая обычно указывается в наносекундах. Чем больше длительность импульса, тем больше энергии, которая передается от устройства, из-за чего растет «дальнобойность» прибора.

При настройке длины импульса рекомендуется начать с наименьшей допустимой величины, а затем постепенно увеличивать длительность импульса. Если повреждение кабеля находится недалеко от измерительного прибора, короткого импульса будет достаточно для его обнаружения. Изменяя длительность импульса, а также выполняя несколько измерений, можно более точно локализовать место повреждения кабеля.

Как известно, скорость света постоянна и составляет 300 000 км/с (в вакууме). Скорость распространения электрического сигнала обычно меньше этой величины. Например, кабель витой пары со значением VOP (Velocity Of Propagation, скорость распространения сигнала), равным 0,65, будет передавать электрический сигнал со скоростью, равной 65 % скорости света в вакууме.

Покупателям обычно сообщается значение, которое зачастую можно найти среди технологических характеристик приобретаемого кабеля. Поскольку рефлектометр TDR измеряет время прохождения сигнала по кабелю и обратно, то, прежде чем приступать к точным измерениям, необходимо знать значение VOP для тестируемого кабеля.

Если вы не уверены в качестве тех или иных кабелей, следует сначала их протестировать для определения значения VOP. Это можно сделать при помощи измерения заранее определенной длины кабеля, а затем можно применить рефлектометр TDK, протестировать длину кабеля, изменяя показатель VOP до тех пор, пока тестер не укажет правильную длину. Подразумевается, конечно, что сегмент кабеля, используемого для тестирования, находится в хорошем состоянии.

Сетевые и протокольные анализаторы

Если при проверке кабелей повреждений не обнаружено, это гарантирует, что физическая кабельная структура, лежащая в основе сети, функционирует в нормальном режиме. Следующий уровень обследования предполагает проведение мониторинга и тестирования сетевого трафика и сообщений, генерируемых сетевыми протоколами в целях подтверждения нормального функционирования сети. Программы сетевых анализаторов отслеживают сеть на канальном и транспортном уровнях в эталонной модели OSI.

Анализатор локальной сети позволяет перехватывать сетевой трафик при его прохождении по кабелю в режиме реального времени и сохранять данные в целях их дальнейшего анализа. Хороший анализатор должен уметь генерировать

значимую статистику сетевого трафика, декодировать используемые протоколы, а также обеспечивать хорошую фильтрационную способность, чтобы пользователю не пришлось выполнять лишнюю работу, самостоятельно обрабатывая такое огромное количество данных.

При покупке сетевого анализатора следует учитывать множество факторов.

- *Цена.* Этот фактор всегда следует учитывать при покупке сетевого оборудования.
- *Аппаратные и программные средства.* Требуется ли покупать аппаратно реализованное устройство, которое может выполнять полный анализ или подключаться к многочисленным сегментам, или для этих целей достаточно специальной программы, которая выполняется на существующей сетевой рабочей станции?
- *Сетевой интерфейс.* Примите решение, будете ли вы работать в сети 100BASE-T (Gigabit Ethernet или даже 10Gigabit Ethernet), или же вы нуждаетесь в устройстве, которое может подключаться к сетям FDDI либо Token-Ring?
- *Поддержка стека протоколов.* Определитесь с тем, однородна ли ваша сеть, или же она поддерживает многочисленные сетевые протоколы?
- *Статистика.* Определитесь с типом статистической информации, выводимой анализатором. Одним из наиболее важных показателей является количество фреймов в секунду. Другая статистическая информация включает коэффициент использования и загрузки сети. Первый показатель измеряется как фактическая скорость передачи данных для вашего сетевого устройства. Коэффициент загрузки позволяет определить, каким образом используется полоса пропускания, — от статистики протокола до таких показателей, как количество коллизий в совместно используемом сегменте сети Ethernet.
- *Память и буферные устройства.* Снабжен ли анализатор буфером памяти достаточного объема, который позволяет накапливать сетевые фреймы в современных высокоскоростных сетях, таких как Gigabit Ethernet (или даже 10Gigabit Ethernet)?
- *Фильтры.* Обеспечивает ли анализатор достаточный уровень фильтрации, позволяющий просматривать большие объемы данных с тем, чтобы «вылавливать» нужные фреймы?
- *Операции импорта и экспорта.* Позволяет ли устройство сохранять файлы на диске или на другом устройстве, чтобы можно было копировать их на другие рабочие станции для дальнейшего анализа?

Хороший анализатор локальной сети позволяет контролировать сетевой трафик в режиме реального времени, используя при этом фильтры для сужения области просмотра. Можно установить фильтры сбора, хранить некоторые или все подходящие кадры в буфере для выполнения дальнейшего анализа.

Выборка базовых данных

Прежде чем приступать к выполнению мониторинга или анализа использования сети, необходимо создать набор базовых данных. Для интерпретации статистических данных, которые можно собрать с помощью анализаторов локальной сети,

требуется определить эталон, с которым будут сравниваться результаты будущих измерений. Базовые данные используются для определения обычной операционной среды системы и обеспечивают ссылки на функции мониторинга, они также полезны при поиске и устранении неисправностей.

Кроме того, базовые данные нужны для планирования мощности и оценки эффективности модернизации. При внесении записей в документацию, связанную с базовыми данными, кроме значений, получаемых с помощью анализатора локальной сети, необходимо учитывать следующие факторы:

- расположение оборудования в сети;
- тип используемого оборудования;
- количество и распределение пользователей;
- используемые протоколы.

Осведомленность о типе оборудования особенно важна, поскольку различные модели сетевых адаптеров, концентраторов и других устройств могут значительно отличаться друг от друга по своим параметрам. Зная, где располагается то или иное оборудование, можно создать контрольный журнал поиска и устранения неисправностей.

Перемещение нескольких рабочих станций или серверов, если оно заранее не согласовано, может привести к нежелательному изменению топологии. Предположим, что необходимо перенести два сервера из отдела в центральный вычислительный центр. Раньше, когда серверы были размещены в том же сегменте, что и большинство пользователей, трафик носил локальный характер. После того как серверы окажутся в другом сетевом сегменте, может оказаться недостаточной скорость передачи данных в магистрали или в коммутаторах/маршрутизаторах, соединяющих два сетевых сегмента. Отслеживая статистическую и аппаратную информацию, характеризующую использование и функционирование сетевых устройств, можно предотвратить подобные неприятности. По крайней мере, можно воспроизвести прежнюю ситуацию и локализовать проблему.

Этот же принцип применим и к проблеме с расположением пользователей в сети. Различные пользователи могут предъявлять совершенно разные требования к одной рабочей станции или серверу. Нужно составить список пользователей и приложений, с которыми они работают, а в случае необходимости отмечать даже время суток, когда ими выполняется сменная работа.

Также не помешает понимание сути работы используемых протоколов. Зачастую бывает непросто локализовать проблему, возникающую при перемещении устройства в другой сетевой сегмент, не ведая о том, что он использует немаршрутизируемый протокол. Конфигурация многих маршрутизаторов предусматривает использование немаршрутизируемых протоколов (например, NetBEUI). Об этом следует знать при необходимости соответствующего конфигурирования маршрутизатора до того, как выполнять какое-либо перемещение.

Наконец, базовые данные постоянно изменяются. Если ваша сеть расширяется или изменяется, модифицируйте документацию соответствующим образом, чтобы данные могли использоваться в дальнейшем.

Статистика

Несмотря на то, что большая часть анализаторов предоставляет широкий спектр статистических данных, анализатор должен отображать некоторые общие значения.

Необходимо удостовериться в том, что анализатор может собирать статистические данные об использовании сети. Кроме графического отображения нагрузки в режиме реального времени, следует также использовать возможность мониторинга сети, чтобы определять момент максимальной степени использования. Итоговая степень использования сети, вычисленная в течение обычного рабочего дня, может быть не столь полезной, как определение наиболее напряженных периодов работы пользователей, когда они сталкиваются со значительной перегрузкой сети. С помощью статистики по максимальной степени использования можно разрешить проблемы трафика перераспределением ресурсов.

Применяя сетевые анализаторы можно также оценивать количество фреймов, передаваемых в секунду (FPS, Frames Per Second). Само по себе значение FPS не является определяющим, однако в сочетании с данными, отображающими размер сетевых пакетов, оно может быть полезным. Чем больший размер пакета используется протоколом, тем более эффективным может оказаться протокол. Такая закономерность объясняется тем, что каждый пакет должен обладать дополнительными свойствами, требуемыми для реализации протокола, например адресацией и возможностью мониторинга ошибок. При наличии пакета большого размера соотношение дополнительных свойств и рабочей нагрузки можно сократить.

Фильтрация

Фильтрацию пакетов может осуществлять любой сетевой анализатор. При этом можно устанавливать критерии, используемые анализатором при сборе фреймов, или производить выборочный поиск в буфере собранных данных для выборки только тех кадров, которые необходимы при поиске и устранении неисправностей. Обычно фильтры настраиваются на выборку кадров по типу протокола и кадра, адресу протокола или MAC-адресу. Некоторые фильтры позволяют производить поиск определенных шаблонов данных во всем пакете.

Программные анализаторы

Программные анализаторы входят в класс наиболее дешевых инструментальных средств, предназначенных для больших и сложных сетей. Поскольку мощность современных процессоров очень велика, а сетевые карты могут захватывать пакеты даже в высокоскоростных локальных сетях, возможности программных анализаторов в настоящее время соответствуют возможностям аппаратных анализаторов. В Интернете можно найти бесплатно распространяемые программные анализаторы, реализующие большинство функций, присущих небольшим сетям.

Версии ОС от Windows NT 4.0 Server до Windows 2003 Server снабжены средствами сетевого мониторинга, позволяющими локальной рабочей станции или серверу контролировать сетевой трафик, который генерируется компьютером или отсылается ему. Версия, поставляемая в комплекте с сервером управления

системами (SMS, Systems Management Server), позволяет сетевому администратору контролировать трафик в локальной сети. Программу сетевого монитора для Windows 2000 Server/Windows 2003 Servers можно найти в папке Administrative Tools.

Оба этих программных продукта позволяют собирать данные в локальной сети, фильтровать и исправлять множество ошибок. Поскольку эти программы предназначены для рабочих станций, можно использовать их для сбора и хранения больших объемов информации в целях выполнения немедленного анализа, а также для генерирования отчета в долгосрочном плане. На рис. 11.1 изображено главное окно сетевого монитора Capture Window (Окно сбора данных) для Windows 2000 Server.

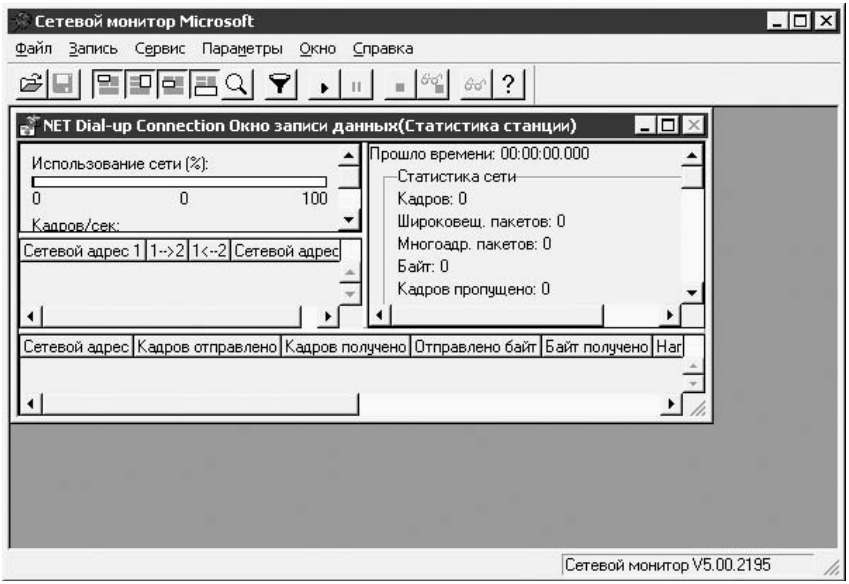


Рис. 11.1. Окно сетевого монитора Windows 2000 Server

ПРИМЕЧАНИЕ Если в папке Administrative Tools отсутствует инструмент Network Monitor, необходимо установить этот компонент. Для этого нужно запустить оснастку Add/Remove Programs (Установка и удаление программ) из панели управления. В ней нужно выбрать категорию Add/Remove Windows Components (Добавить/Удалить компоненты Windows), а затем группу Management and Monitoring Tools (Инструменты управления и мониторинга). После этого - останется лишь нажать кнопку Details (Подробно) и выбрать сетевой монитор.

Чтобы начать сбор кадров в сети, нужно выполнить команду Capture ▸ Start (Сбор данных ▸ Начать). Можно также воспользоваться меню Capture для приостановки или прекращения процесса сбора данных. В процессе сбора кадров монитором можно получить представление о том, что происходит в сети, при помощи постоянно обновляемых диаграмм в окне Capture Window. Чтобы остановить сбор дан-

ных, нужно выполнить команду меню Capture ▸ Stop (Сбор данных ▸ Остановить), Затем команду Capture ▸ Display Captured Data (Сбор данных ▸ Отобразить собранные данные) для просмотра собранных фреймов данных.

При просмотре данных видно, что каждый фрейм снабжен итоговой строкой. Собранные кадры хранятся во временном буфере. Если требуется сохранить данные для их дальнейшего анализа, то следует выполнить команду меню File ▸ Save As (Файл ▸ Сохранить как). Для просмотра данных из сохраненного файла нужно выполнить команду File ▸ Open (Файл ▸ Открыть), чтобы считать данные файла во временный буфер.

Для проверки любого фрейма достаточно дважды щелкнуть на итоговом окне. После этого открывается панель Detail (Подробно), где отображаются данные, передаваемые в этом фрейме.

Объем трафика, проходящего даже через небольшие сети, может быть достаточно большим, хотя благодаря программе сетевого монитора с ним вполне можно справиться. В процессе поиска и устранения неисправностей полезно иметь возможность отфильтровать несущественную информацию, чтобы просматривать только те фреймы, которые имеют отношение к решаемой проблеме.

Фильтр сбора используется для создания критериев выбора фреймов, которые будут храниться во временном буфере, в то время как фильтр отображения может использоваться для дальнейшей выборки кадров из набора данных. Для создания фильтра достаточно просто выполнить команду меню Capture ▸ Filter (Сбор данных ▸ Фильтр). После создания фильтра сбора данных можно начинать сбор данных, выполнив команду Capture ▸ Start (Сбор ▸ Начать). Используя узкополосный фильтр при поиске специфической проблемы, можно задать событие, которое будет уведомлять об обнаружении подходящего фрейма. Для установки триггера сбора данных нужно выполнить команду Capture ▸ Trigger (Сбор ▸ Триггер).

Программа сетевого монитора позволяет контролировать весь трафик в сети при помощи графиков, отображаемых в окне Capture Window. Эта же программа обеспечивает обнаружение специфических кадров, позволяющих локализовать возникающие проблемы. Хороший программный анализатор локальной сети может быть ценным инструментом, позволяющим оценить степень загрузки сети или найти и устранить специфические проблемы, связанные с протоколом. Однако чтобы просматривать весь сетевой трафик, потребуется другой сетевой монитор, например, поставляемый в комплекте с Microsoft SMS, или какая-либо программа от независимого производителя.

Иные программные анализаторы

Быстродействующие микропроцессоры, используемые в современных настольных и портативных компьютерах, привели к тому, что появилось семейство программных анализаторов, свойства которых вплотную приблизились к свойствам аппаратных анализаторов. В предыдущем разделе рассматривались встроенные инструменты мониторинга локальной сети, входящие в комплект поставки операционной системы Windows. Однако на рынке в огромном количестве представлены программные анализаторы локальной сети, которые намного дешевле, чем их аппаратные аналоги.

Прежде чем приобретать анализатор локальной сети, следует его испытать. Ниже приведен список некоторых программ, доступных в виде демо-версий либо пробных оценочных версий. Следует проверить качество документации, наличие хорошей технической поддержки, а также практические свойства каждого программного анализатора.

- *Ethertest LAN Analyzer for Windows.* Этот анализатор локальной сети, разработанный фирмой Frontline Test Equipment, Inc. (FTE), существует в виде версий для ряда операционных систем, от Windows 95 до Windows 2000. Демоверсию этой программы можно загрузить с веб-сайта, расположенного по адресу www.fte.com. Если в локальной сети применяется технология Bluetooth, не помешало бы также загрузить демо-версию FTE SerialBlue Bluetooth.
- *Observer, Expert Observer и Observer Suite* от компании Network Instruments. Эти программные продукты обеспечивают выполнение всех функций — от простого анализа сети и функций консоли SNMP (Simple Network Management Protocol, простой протокол сетевого управления) и RMON (Remote Monitoring, удаленный мониторинг) до формирования отчетов на основе тестирования сети. Существуют версии этих программ для различных платформ — от Windows 95 до Windows 2000. Кроме того, программа Observer поддерживает беспроводные сети, функционирующие в соответствии со стандартом IEEE 802.11a и 802.11b. Демо-версию этой программы можно загрузить с веб-сайта, расположенного по адресу www.netinst.com.
- *Wildpackets.* На соответствующем веб-сайте (www.wildpackets.com) доступны демо-версии всего набора инструментов сетевого анализа (от высококачественных инструментальных средств анализа локальных сетей (EtherPeek) до анализаторов беспроводных сетей (AiroPeek)).

Выбор необходимых средств анализа среди перечисленных продуктов должен определяться потребностями администратора и структурой сети. Тем не менее, рекомендуется загрузить демо-версии вышеупомянутых программ, с тем чтобы получить общее представление о программном анализаторе локальной сети.

Аппаратные анализаторы

Подобные инструментальные средства могут стоить десятки тысяч долларов. Но зато они предоставляют администратору намного больше возможностей, чем любой программный анализатор. Аппаратный анализатор локальной сети может применяться либо непосредственно у рабочей станции, на которой была зафиксирована та или иная проблема, либо подключаться к сети для штатного выполнения своих функций. Аппаратно реализованный инструментарий может намного успешнее применяться в такой среде, чем программный анализатор, который ориентирован на сбор трафика с помощью сетевых карт. Аппаратные анализаторы содержат специальную схему, которая используется для более быстрого выполнения многих функций. Поэтому считается, что аппаратные анализаторы намного надежнее, чем соответствующие им программные анализаторы.

Другим фактором, который следует учитывать при сравнении программных и аппаратных анализаторов, является то, что при использовании компьютера или

рабочей станции, выступающей в роли анализатора локальной сети, его функции могут ограничиваться возможностями сетевой карты. Например, встроенное ПО некоторых сетевых адаптеров обладает функциями, которые реализуют автоматическое отклонение определенных видов пакетов, содержащих ошибки. В этом случае выявить ошибки программным способом будет просто невозможно.

Кроме того, хотя сетевые адаптеры могут в буквальном смысле «просвечивать» каждый пакет, циркулирующий в сети, это не означает, что адаптеры могут собирать данные и передавать их протоколам высшего уровня. Когда адаптер собирает все фреймы и передает их стеку протоколов, он работает в *беспорядочном режиме*. В некоторых сетевых адаптерах подобный режим блокируется, поэтому при выборе адаптера для рабочей станции, на которой выполняется мониторинг локальной сети, не забудьте ознакомиться с соответствующей документацией.

ПРИМЕЧАНИЕ Во многих стандартных ситуациях функции, выполняемые большинством аппаратных анализаторов, реализованы даже в программных анализаторах. Однако при использовании высокоскоростных каналов связи глобальных сетей или когда сложная сетевая топология содержит множество протоколов и служб, лучше было бы вложить средства в покупку аппаратного анализатора.

Большинство аппаратных анализаторов снабжено встроенными дисками для хранения собранных данных, включая дисковод для дискет, который может использоваться при обмене данными с рабочими станциями. Нужно удостовериться в том, что анализатор имеет достаточный объем памяти для хранения огромных объемов информации. Другим важным критерием, на который следует обратить внимание, является хороший дисплей, который позволит наглядно видеть степень загрузки сети, а также отображать содержимое отдельных кадров.

Возможно также использование гибридных устройств, сочетающих в себе свойства программных и аппаратных анализаторов. При этом функции сбора и фильтрации информации выполняются аппаратным компонентом, который подключается к рабочей станции, обеспечивающей функции отображения и хранения данных. Аппаратный компонент снабжен выделенной схемой, а также имеет производительность, позволяющую собирать данные в сети. Программа, выполняемая на компьютере, используется для фильтрации, вычислений и отображения данных.

Простой протокол сетевого управления

Формирование современной локальной среды предусматривает интеграцию компонентов от различных производителей. Поэтому требуется постоянный мониторинг физических сетевых компонентов и сетевых протоколов.

Все подобные инструментальные средства ориентированы на выполнение специфических задач, поэтому каждое из них реализовано в виде отдельного модуля. При разработке *простого протокола сетевого управления (SNMP, Simple Network Management Protocol)* преследовалась цель создания простого метода, применяемого

для централизации управления сетями на основе набора протоколов TCP/IP. В частности, на «повестке дня» были следующие основные задачи:

- минимальный уровень расходов, связанных с разработкой протокола;
- обеспечение удаленного управления устройствами;
- создание гибкого протокола, способного адаптироваться к новым технологиям;
- создание протокола, не зависящего от основных свойств эксплуатируемых устройств;
- предельное упрощение.

Особенно важным является соответствие последнему критерию. Поскольку протокол SNMP предназначен для реализации во многих типах сетевых устройств, то в процессе его разработки нужно было избежать больших накладных расходов. Благодаря этой идее стало возможным создание таких простых устройств, как мост или концентратор, которыми можно управлять при помощи протокола SNMP, а также более сложного устройства наподобие маршрутизатора или коммутатора. Другие ключевые факторы, связанные с применением протокола SNMP, — использование протокола пользовательских дейтаграмм (UDP, User Datagram Protocol) для обмена сообщениями и архитектура типа «менеджер-клиент». С точки зрения реализации и применения, протокол UDP проще, чем, TCP. К тому же он обладает достаточными функциональными свойствами, позволяющими главному менеджеру поддерживать связь с удаленным агентом, выполняемым на эксплуатируемом устройстве.

Двумя основными компонентами протокола SNMP являются *менеджер* и *агент*. В качестве менеджера обычно выступает программа, выполняемая на рабочей станции или более мощном компьютере, поддерживающем связь с процессами агента, выполняющимися на каждом отслеживаемом устройстве. Агенты могут выполняться мостами, маршрутизаторами, концентраторами и даже рабочими станциями пользователей. Менеджер опрашивает агентов, отсылая информационные запросы, а агенты отвечают на них.

Приложения, исполняющие роль менеджеров SNMP, отличаются как с точки зрения расходов, так и по своим функциональным свойствам. Некоторые из них — это простые приложения, осуществляющие запросы и позволяющие администратору просматривать информацию, поступающую от устройств, и составлять отчеты. Кроме того, приложение консоли управления может осуществлять следующие функции:

- формирование топологии сети;
- мониторинг сетевого трафика;
- перехват избранных событий и генерирование оповещений;
- составление отчета о значениях переменных.

Некоторые консоли управления, называемые также станциями управления сетью (NMS, Network Management Stations), могут генерировать отчеты, содержащие анализ тенденций в долгосрочной перспективе. Администратор может формировать содержательные отчеты, облегчающие решение тех или иных проблем.

Агенты управления устройствами и программами поддерживают между собой связь, используя ограниченный набор операций, именуемых *элементарными*

действиями. Благодаря им обеспечивается составление запросов, а также обмен информацией между двумя сторонами канала связи. Элементарные действия инициируются программами и приведены в следующем перечне:

- *get* — это элементарное действие применяется менеджером для получения от агента однократного сообщения;
- *get-next* — данное элементарное действие применяется в том случае, когда данные, ожидаемые менеджером от агента, состоят из нескольких фрагментов;
- *set* — это элементарное действие применяется менеджером в том случае, когда формируется запрос для агента, выполняемого на удаленном устройстве. Результатом является то, что определенной переменной присваивается то или иное значение.

Для управляемого устройства агент использует следующие примитивы:

- *get-response* — данное элементарное действие генерирует ответы на запросы `get` или `get-next`, поступающие от менеджера;
- *trap* — хотя обмен данными протокола SNMP обычно выполняется программой менеджера, данное элементарное действие используется в том случае, если агенту необходимо сообщить менеджеру об определенном важном событии.

Указанные элементарные действия выполняются менеджерами (агентами) в процессе обмена данными между ними. При этом типы данных определяются в *базе данных управляющей информации (MIB, Management Information Base)*. Первоначальное определение объектов, хранящихся в этой базе данных, было приведено в документе RFC 1066, «Management Information Base for Network Management of TCP/IP-based Internets: MIB-II». Затем появился документ RFC 1213, «Management Information Base for Network Management of TCP/IP-based Internets: MIB-II», в который были внесены некоторые поправки. В частности, там содержатся более четкие определения некоторых объектов, представленных в оригинальном документе, а также некоторые новые определения. Два документа RFC 2011 и RFC 2012 содержат расширенный набор данных об информационной базе данных MIB-II.

База данных MIB организована как «информационное дерево». Эта иерархическая база данных установлена на компьютере агента, который также ответственен за ее своевременное пополнение. Каждый объект MIB представляет некий аспект устройства. Например, в концентраторе полезные объекты могут накапливать информацию, отображающую количество пакетов, поступающих концентратору, тогда как другой объект может отслеживать сетевые адреса.

При определении типов объектов, принимаемых в качестве стандарта, учитывались следующие факторы:

- объект должен быть полезен в процессе управления конфигурацией либо устранения неисправности;
- объект должен устранять только небольшие повреждения, если имел место случай вторжения. Не следует забывать о том, что кроме считывания значений, хранящихся в MIB, управляющая программа может выполнять запросы, результатом которых является присваивание объекту определенного значения;
- не допускается простое получение объектов на базе ранее существующих.

Первое определение стандартной базы MIB содержало меньше ста объектов, что позволяло упростить процесс ее развертывания. В настоящее время это ограничение уже не актуально.

Поскольку схема управления SNMP может расширяться, разработчики часто создают свои собственные объекты, которые можно добавлять к программе консоли управления, чтобы пользователь мог их применять.

Объект содержит специфическую синтаксическую структуру, имя и связанный с ним метод шифрования. Имя состоит из идентификатора объекта, уточняющего его тип, к которому добавляется специфический экземпляр такого вида объекта. Идентификатор объекта — это строка десятичных цифр, разделяемых точками, например .3.6.1.2.1.1.1. Экземпляр объекта содержит дополнительное десятичное число, которое следует после идентификатора оригинального объекта. Дескриптор объекта для удобства пользователя определяется в формате читаемого текста.

Доступ к объекту может определяться в режиме только чтения, режиме чтения и записи или в режиме только записи. Кроме того, объект может быть недоступен в конкретное время.

В первых документах RFC, описывающих базу MIB, объекты разделялись лишь на несколько групп высокого уровня:

- *System*. Эта группа состоит из объектов, идентифицирующих тип системы (применяемые аппаратные или программные средства);
- *Interfaces*. Объект из этой группы может представлять номер или тип интерфейса. Другая информация о сетевых интерфейсах, таких как самая большая IP-дейтаграмма, которая может быть отправлена или получена, представлена в этой группе в качестве объектов;
- *Address Translation*. Объекты этой группы используются для хранения информации относительно трансляции адреса, такой как кэш протокола ARP;
- *IP*. Объекты из этой группы поддерживают информацию, относящуюся к протоколу IP, включая время существования, количество дейтаграмм, полученных от интерфейсов, ошибок и т. д.;
- *ICMP*. Данная группа включает статистику входных и выходных данных протокола контроля сообщений в Интернете;
- *TCP*. Объект из этой группы используется для хранения информации относительно соединений TCP. Экземпляры этих объектов существуют только при наличии соединения. Данные, содержащиеся в этих объектах, отображают, например, количество полученных или отправленных сегментов или режим определенного соединения TCP;
- *UDP*. Объекты из данной группы представляют статистику по протоколу UDP, как количество доставленных или полученных UDP-дейтаграмм, для которых отсутствует соответствующее приложение для порта назначения;
- EGP. Эти объекты используются протоколом внешней маршрутизации (EGP).

В базе данных MIB-II была исключена группа трансляции адресов. В MIB-II были добавлены также новые объекты и функциональные свойства, которые могут быть использованы для осуществления функций, выполняемых этой группой.

Кроме того, появились новые объекты в составе ранее существующих групп. Например, информация, которая в настоящее время считается необходимой для системной группы (контактное лицо, расположение системы и службы системы), теперь может храниться в объектах этой группы.

Ниже представлены новые группы, появившиеся в базе MIB-II.

- *Transmission*. Как и группа *Interface*, эта группа используется для объектов, имеющих отношение к специфическим средствам передачи данных.
- *SNMP*. Это группа, добавленная для объектов, необходимых ориентированной на приложения рабочей группе для сбора полезной статистической информации.

Не все устройства имеют возможность использовать протокол SNMP. В этом случае аналогичные функции может выполнять другое устройство, выступающее в роли *прокси-агента* и управляемое с консоли управления SNMP. Например, протокол SNMP может не поддерживаться сетевым адаптером, но на узловом компьютере выполняется процесс, позволяющий отслеживать сетевой адаптер, а также выступать в роли прокси-агента, передающего информацию на станцию управления. Прокси-агенты могут также выполнять функции трансляции между лицензионной управляющей программой и SNMP. В этом случае прокси-агент использует собственное управляющее программное обеспечение и поддерживает, в случае необходимости, связь с управляющей станцией SNMP.

Модуль удаленного мониторинга

Модуль удаленного мониторинга (RMON) представляет собой инструмент для сбора данных и анализа, призванный устранить недостатки, присущие протоколу SNMP. Принцип работы RMON аналогичен принципу действия SNMP, причем соответствующие объекты тоже определены в базе MIB. В основе проектирования данного инструмента лежал принцип работы анализатора локальной сети, о котором упоминалось в этой главе. Определения базы данных MIB для RMON в сетях Ethernet и Token-Ring, соответственно, описаны в документах RFC 1757, «Remote Network Monitoring Management Information Base» и RFC 1513, «Token-Ring Extensions to the Remote Network Monitoring MIB».

В протоколе SNMP функции менеджера и агента аналогичны функциям клиента и сервера, где агент является клиентом консоли программного управления. В модуле RMON агенты, часто называемые *зондами*, являются активной стороной (серверы), тогда как одна или более консолей управления могут быть их клиентами.

Агенты RMON производят интеллектуальный анализ и посылают ловушки SNMP консоли управления в случае возникновения важного события.

Применяя модуль RMON, администратор может осуществлять сквозной обзор сети. Типы собранных данных, оповещения и действия, связанные с RMON, отличаются от своих прототипов в стандартных типах SNMP. Объекты RMON делятся на следующие MIB-группы:

- *Statistics*. Эта группа регистрирует данные о сетевых устройствах. Таблица EtherStatsTable содержит по одной записи для каждого интерфейса. Статистика отображает сведения об объеме трафика, размерах пакета и ошибках;
- *History*. Функция управления этой группы отвечает за статистическую выборку данных. Она контролирует частоту выборки данных в сети и формирует таблицу historyControlTable. Эта группа объектов позволяет архивировать данные, в результате чего происходит регистрация статистических данных и их перенос в таблицу etherHistoryTable;
- *Hosts*. Эта группа отслеживает сетевые узлы, основываясь на соответствующих MAC-адресах. Информация в таблице hostControlTable определяет параметры для операций мониторинга, а таблица hostTimeTable регистрирует время обнаружения сетевого узла;
- *HostTopN*. Эта группа используется для классификации узлов в соответствии со статистическими показателями, например количеством генерируемых ошибок. Таблица TopNControlTable содержит параметры управления для этой группы, а таблица hostTopNTable отслеживает данные;
- *Matrix*. Данные, фиксируемые этой группой, содержат сведения о передаче фреймов между сетевыми узлами. Здесь хранятся статистические сведения о передаче данных между узлами в обоих направлениях;
- *Filter*. Эта группа определяет типы пакетов, которые собирает зонд модуля RMON, например размер фрейма;
- *Capture*. В то время как группа Filter определяет параметры, необходимые для сбора пакетов, эта группа отвечает за сбор пакетов на основании этих параметров;
- *Alarm*. Эта группа используется для установки оповещений в ситуациях, описанных в следующей группе Event. Здесь пользователь может установить периоды проведения выборок и пороговые величины, при которых выдается оповещение. Эта группа считывает собранные статистические данные, а когда они превышают пороговую величину, генерируется соответствующее событие;
- *Event*. Когда переменная величина превышает пороговое значение, определенное оповещением, генерируется событие. Эта группа может формировать ловушку SNMP для уведомления станции управления сетью или регистрации информации в журнале. Таблица Event Table используется для определения способа уведомления, применяемого для события, а таблица Log Table — для записи информации.

Приведенный перечень групп свидетельствует, что модуль RMON обладает расширенным набором разнообразных функций и предусматривает сбор статистических данных на всех уровнях эталонной модели OS1.

Поскольку сеть Token-Ring обладает некоторыми присущими ей особенностями, в состав модуля RMON были включены дополнительные группы, предназначенные для сетей этого типа.

- *Token-Ring Statistics*. Данная группа предназначена для хранения информации о поведении кольца, от объема трафика до количества встречающихся источ-

ников сигнала, очистки кольца и другой служебной информации сети Token-Ring.

- *Token-Ring History*. Аналогично группе History (в сетях Ethernet), эта группа отслеживает события, поддерживая соответствующий архив.
- *Token-Ring Station*. Здесь можно найти подробную информацию о каждой станции, входящей в кольцо.
- *Station Order*. Физический порядок расположения станций в кольце может определяться информацией, хранящейся в этой группе.
- *Station Config*. Здесь хранится информация о конфигурации станций.
- *Source Routing*. В этой группе производится контроль информации по маршрутизации от источника в Token-Ring для трафика между кольцами.

Агенты RMON могут быть запрограммированы для реагирования на специфические ситуации, возникающие в сети. Выбор конфигурации оповещения зависит от определения переменной величины для наблюдения, периода выборки и события, которое будет выполняться при достижении пороговой величины. Например, можно установить оповещение для информирования пользователя о нежелательном ходе событий или об улучшении ситуации.

Событие, формируемое оповещением, может быть сконфигурировано таким образом, чтобы была возможность отправки сообщения о ловушке SNMP на одну или более консолей управления и хранения события в таблице регистрации. Станция управления может предпринять необходимые меры, включая удаление информации из таблицы регистрации.

В процессе принятия решения о принципе установки оповещений и событиях, генерируемых ими, пользователю следует помнить о нормальном функционировании сети. Сначала мониторинг сети нужно осуществлять при помощи агентов RMON. При этом отмечаются изменения в трафике или возникшие ошибки. Нужно обратить внимание на любые отклонения, происходящие на регулярной основе в определенные дни или в определенное время суток.

Для различных сетевых сегментов могут потребоваться различные периоды выборок или пороговые величины. Например, локальный сегмент сети может иметь различные отклонения даже при малом количестве пользователей, тогда как основная сетевая магистраль может быть подвержена менее значительным изменениям при смешивании трафика от многих сегментов. При определении периодов выборки рекомендуется придерживаться следующего правила: более короткий промежуток — для сегмента, имеющего частые отклонения, и более длинный — для сегмента с более стабильными показателями.

Ответ на оповещения может быть либо в форме немедленного корректирующего действия, например, в случае с неисправным устройством, либо в форме долгосрочного решения, такого как выделение дополнительной мощности или установка оборудования. Проверка значений базовой линии, установленной пользователем, проводится на регулярной основе, производятся их изменения при смене режима пользования сетью или топологии. Если конфигурацией оповещений и событий не предусмотрено реагирование на проблемные варианты, сетевые операторы будут игнорировать их.

Утилиты мониторинга сети в Windows XP

В среде Windows XP мониторинг сети может осуществляться с помощью утилит Просмотр событий и вкладки Сеть диспетчера задач Windows.

ПРИМЕЧАНИЕ Обратите внимание, что утилита Просмотр событий осталась практически неизменной по сравнению с Windows 2000 Server, а вот вкладка Сеть появилась в диспетчере задач Windows XP.

Просмотр событий

В окне консоли управления утилиты Просмотр событий (рис. 11.2) находятся три записи, соответствующие трем *журналам — безопасности*, *приложений* и *системы*.

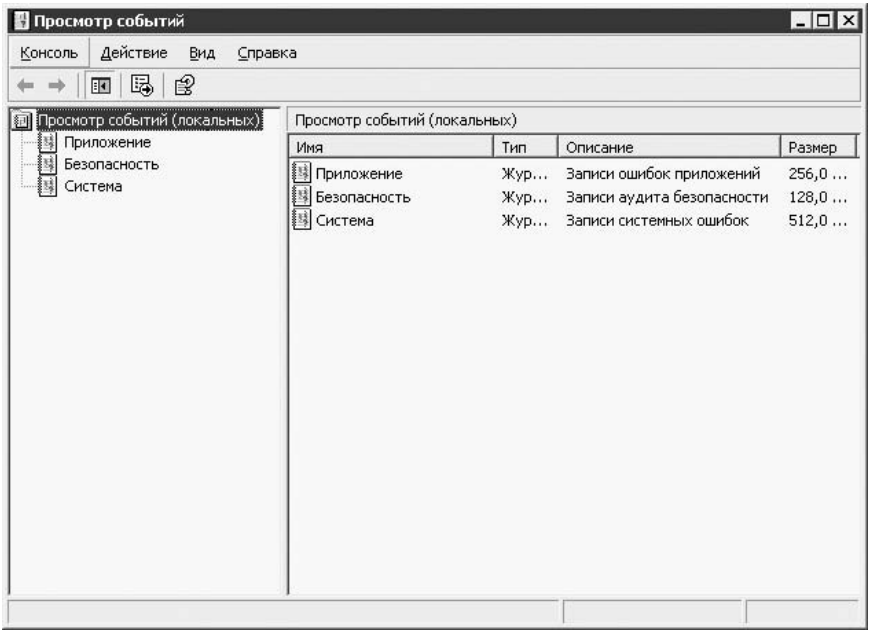


Рис. 11.2. Окно консоли управления просмотром событий

В журнале приложений (рис. 11.3) содержатся данные, относящиеся к работе различных приложений и программ. Записи этого журнала создаются самими приложениями. События, регистрируемые в журнале приложений, определяются разработчиками соответствующих приложений.

Журнал безопасности (рис. 11.4) содержит записи о таких событиях, как успешные и безуспешные попытки регистрации в системе, а также о событиях, относящихся к использованию ресурсов, например о создании, открытии и удалении файлов и других объектов. Решение о событиях, сведения о которых заносятся в журнал безопасности, принимает администратор. Например, после разрешения

аудита входа в систему сведения обо всех попытках регистрации будут вноситься в журнал безопасности.

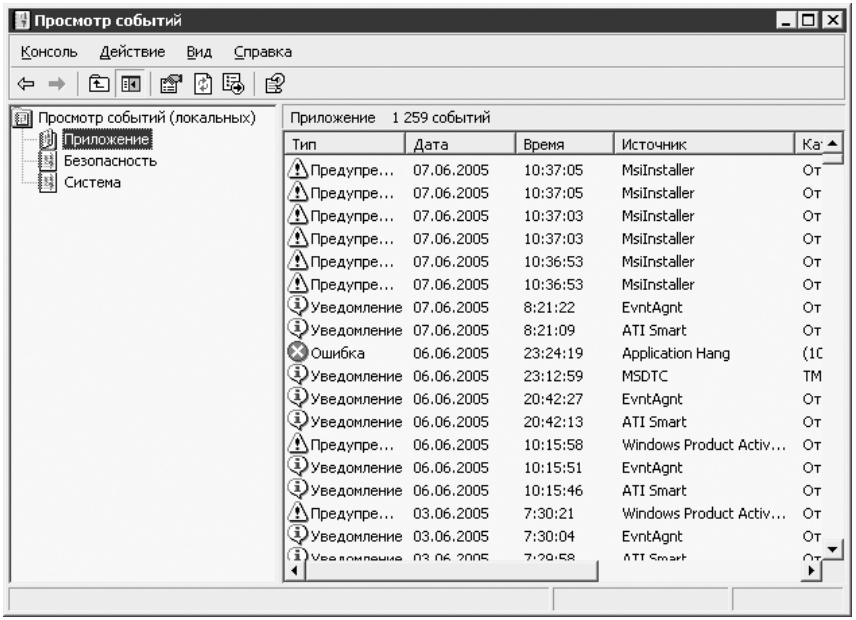


Рис. 11.3. Окно журнала приложений

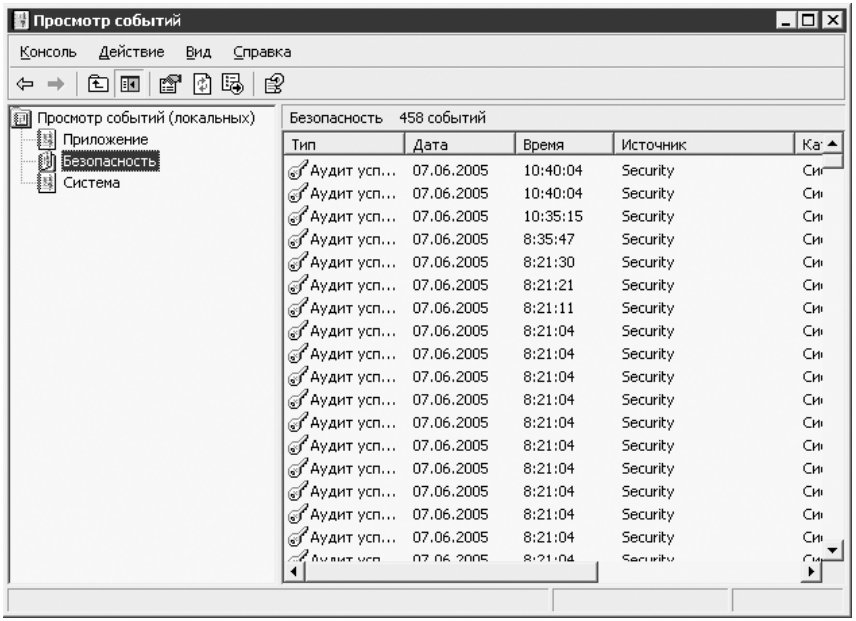


Рис. 11.4. Окно журнала безопасности

Журнал системы (рис. 11.5) содержит записи о событиях, сгенерированные системными компонентами Windows. Например, в журнале системы регистрируются сбои при загрузке драйвера или других системных компонентов при запуске системы. В операционной системе Windows XP жестко зафиксированы типы событий, заносимых в системный журнал.

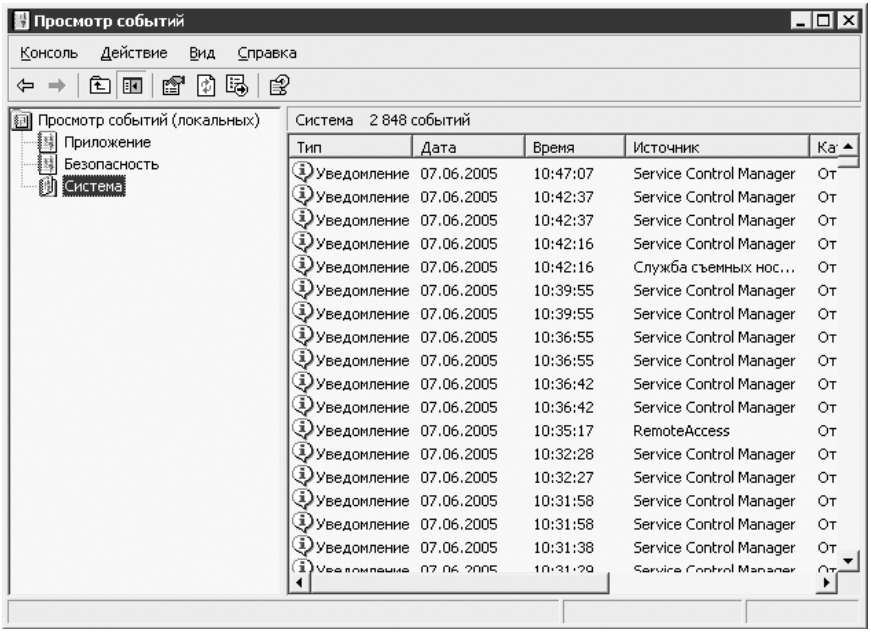


Рис. 11.5. Окно журнала системы

Если компьютер исполняет роль контроллера домена, создаются два дополнительных журнала:

- журнал службы каталогов, в котором регистрируются все события, связанные со службой каталогов;
- журнал службы репликации файлов, который содержит записи о событиях, внесенные службой репликации файлов Windows.

Если компьютер исполняет роль DNS-сервера, то поддерживается журнал DNS-сервера, в котором регистрируются события, связанные со службой DNS.

Все события, регистрируемые утилитой, делятся на следующие категории:

- *Ошибка*. Серьезные проблемы, такие как потеря данных или функциональности. Например, если происходит сбой при запуске загруженной службы, в журнал заносится сообщение об ошибке.
- *Предупреждение*. События, которые в момент записи в журнал не были существенными, но могут привести к осложнениям в будущем. Например, если на диске осталось мало свободного места, в журнал заносится соответствующее предупреждение.

- *Уведомление*. Событие, описывающее удачное завершение действия приложением, драйвером или службой. Например, после успешной загрузки драйвера в журнал заносится событие уведомления.
- *Аудит успехов*. Событие, соответствующее успешно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае успешной регистрации пользователя в системе, в журнал заносится событие с меткой «Аудит успехов».
- *Аудит отказов*. Событие, соответствующее неудачно завершенному действию, связанному с поддержкой безопасности системы. Например, в случае неудачной попытки доступа пользователя к сетевому диску в журнал заносится событие с меткой «Аудит отказов».

Для просмотра любого события достаточно щелкнуть правой кнопкой мыши на соответствующей записи в журнале, затем в контекстном меню выбрать пункт Свойства. После этого будет отображено окно с информацией о характере события (рис. 11.6).

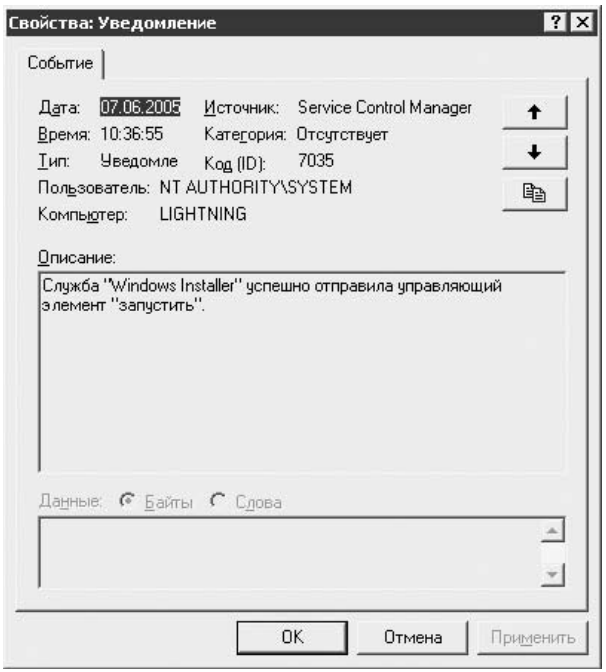


Рис. 11.6. Сведения о характере события

Вкладка Сеть диспетчера задач Windows

На этой вкладке (рис. 11.7) отображается степень загрузки сети, а в строке состояния показаны сведения о сетевых адаптерах, коэффициенте использования сети, быстродействии сетевого соединения и об общем состоянии сети.

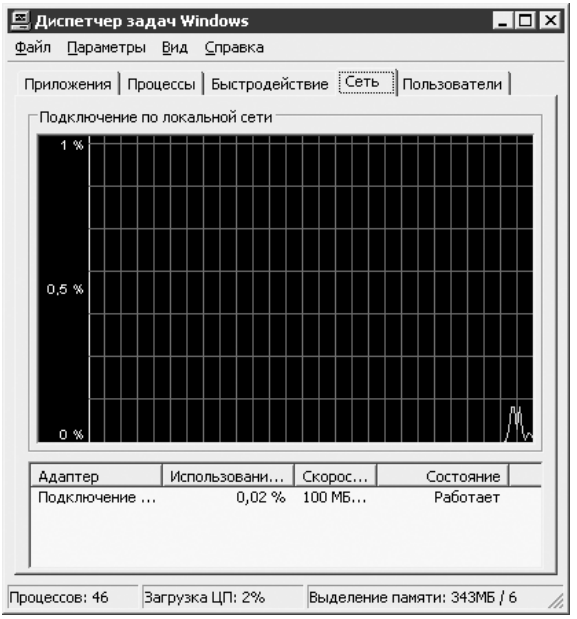


Рис. 11.7. С помощью этого инструмента можно в режиме реального времени отслеживать состояние локальной сети

Вместо послесловия

Вот и перевернута последняя страница книги. Этот труд не претендует на всеобъемлющую полноту, хотя я старался изложить максимум сведений, которые окажутся полезными для администраторов и пользователей локальных вычислительных сетей, развернутых на платформах Windows 2000 Server и Windows XP. В приложении вы найдете словарь сетевых аббревиатур и терминов, имеющих отношение к сетям в широком смысле этого слова. Используйте эту книгу как руководство к действию и не расслабляйтесь, единожды настроив вашу сеть.

Англо-русский толковый словарь сетевых аббревиатур и терминов

В этом словаре вы найдете толкование практически всех аббревиатур и терминов, имеющих отношение к локальным вычислительным сетям и Интернету.

802.3. Стандарт IEEE, определяющий параметры сетей Ethernet.

10BASE-2. Сеть, поддерживающая скорость передачи данных до 10 Мбит/с, в которой используется более тонкий и гибкий коаксиальный кабель, чем в сетях 10BASE-5. Устройства, используемые в этой сети, подключаются с помощью разъемов типа BNC. Также известна под названием *тонкая сеть* (thinnet).

10BASE-5. Сеть, поддерживающая скорость передачи данных 10 Мбит/с, в которой применяется более толстый коаксиальный кабель, чем в сетях 10BASE-2. Для присоединения отводов, к которым подключаются сетевые устройства, производится «прокалывание» жил магистрального кабеля с помощью устройства. Также известна как *толстая сеть* (thicknet).

10BASE-T. Сеть, поддерживающая скорость передачи данных до 10 Мбит/с, в которой используется кабель витой пары (экранированный или не экранированный). Центральным связующим звеном в подобной сети является концентратор либо коммутатор.

100BASE-T. Сеть, поддерживающая скорость передачи данных до 100 Мбит/с, в которой используется кабель витой пары (экранированный или не экранированный). Также известна под названием *Fast Ethernet*. Для объединения устройств в сети применяется концентратор либо коммутатор. Этот вид сетей наиболее распространен в настоящее время.

10Gigabit Ethernet. Сеть Ethernet, поддерживающая скорость передачи данных до 10 Гбит/с. Параметры этой сети определены в стандарте IEEE 802.3a.

AALS (ATM Adaptation Layer 5, протокол адаптации ATM уровня 5). Представитель набора протоколов ATM. Пятый уровень адаптации применяется для передачи данных.

ABR (Available Bit Rate, доступная скорость передачи данных). Эта аббревиатура используется разработчиками протокола ATM и обозначает скорость передачи данных, которая доступна, но не гарантируется.

Accelerated Graphics Port (AGP, ускоренный графический порт). Согласно стандарту, скорость порта AGP варьируется от 2 до 8 (AGP 2x — AGP 8x). Этот порт изначально предназначался для поддержки видеоадаптеров.

Access Point (AP, точка доступа). См. *Wireless Access Point*.

ACK. Эта аббревиатура образована на основе слова «acknowledgment», что означает подтверждение приема сигнала.

Active Directory (активный каталог). Служба каталогов, построенная на основе LDAP, которая включает такие сведения, как учетные записи пользователя, компьютера, а также ссылки на сетевые ресурсы. Обычно применяется в сетях Windows, но может совместно использоваться при работе с другими службами каталогов, основанными на LDAP.

Active monitor (активный монитор). Узел сети Token-Ring, который ответственен за инициализацию и отслеживание трафика в кольце. Он может обнаруживать состояние ошибки, а также переустанавливать состояние кольца. В кольце может одновременно выполняться только один активный монитор. Если происходит сбой, роль активного монитора начинает выполнять другой узел.

Ad hoc wireless network (беспроводная «равноправная» сеть). Беспроводная сеть, не включающая точки доступа (AP, Access Point).

Address Resolution Protocol (ARP, протокол разрешения адресов). Этот протокол определяет физический адрес (MAC-адрес) компьютера в локальной сети на основе его IP-адреса. Команда `arp` может применяться во многих других случаях, например для просмотра и управления текущей таблицей MAC-адресов, которая хранится в локальном кэше ARP.

ADSL (Asymmetric Digital Subscriber Line, асимметричная цифровая абонентская линия). «Асимметричность» проявляется в том, что скорость приема информации выше, чем скорость ее передачи. В современных линиях ADSL скорость приема достигает 8 Мбит/с, а скорость передачи — до 1 Мбит/с.

AGP. См. *Accelerated Graphics Port*.

AH (Authentication Header, заголовок аутентификации). Этот заголовок применяется протоколом IPSec в целях проверки подлинности отправителя дейтаграммы.

ANSI (American National Standards Institute, Американский национальный институт стандартов). Эта организация была основана в 1918 году, в настоящее время представляет собой наиболее крупное учреждение подобного рола в США. Является членом других организаций по стандартизации, например, ISO.

American Standard Code for Information Interchange (ASCII, американский стандартный код обмена информацией). Представление буквенных символов, а также знаков пунктуации в числовом формате. Многие годы стандарт ASCII применялся для кодирования текста в компьютерных системах. В новейших системах этот стандарт был расширен, после чего стал включать дополнительные языки, в которых применяются дополнительные знаки (символы), например Unicode.

American wire gauge (AWG, кабельный калибр). Стандарт, используемый для определения геометрических характеристик кабелей, выпускаемых в США. От размеров кабеля зависит его сопротивление (и некоторые другие параметры), определяемое посредством национального электрического кода (National Electrical Code). Увеличение кабельного калибра соответствует уменьшению диаметра поперечного сечения кабеля.

ANSI. См. *American National Standards Institute*.

APIPA. См. *Automatic Private IP Addressing*.

Arbitrated Loop (управляемая петля). Петлевая топология, используемая при организации сети на основе волоконно-оптических каналов (Fibre Channel). В одной петле может находиться до 126 узлов (или 127, если петля подключена к коммутатору). Каждое устройство в петле конкурирует за право доступа с соседними устройствами; передача данных может осуществляться различными устройствами на поочередной основе.

ARCnet. Старейший протокол локальной сети, напоминающей Token-Ring, количество узлов в которой ограничено до 255. Сети ARCnet по-прежнему широко используются торговыми и промышленными предприятиями. Основное преимущество сетей ARCnet связано с их предельной простотой: после назначения адресов для каждого устройства, требуется выполнить лишь небольшой объем работ по установке. Недостатки связаны с недостаточной «емкостью» сетей — не более 255 сетевых компьютеров и невысокой (по современным меркам) скоростью передачи данных — не более 10 Мбит/с.

ARP. См. *Address Resolution Protocol*.

ARPANET. Первая глобальная сеть, появившаяся в 1969 году. При ее создании использовались автономные коммутаторы пакетов, соединенные между собой выделенными линиями связи. Служила своего рода «полигоном» для обкатки технологических решений, на основе которых был сформирован Интернет.

ARQ (Automatic Repeat Request, автоматический запрос на повторение). Способ повышения надежности передачи данных. Используется в том случае, если протокол поддерживает подтверждение успешной (или неуспешной) передачи данных.

ASCII. См. *American Standard Code for Information Interchange*.

Asynchronous Transfer Mode (ATM, режим асинхронной передачи данных). Сетевой протокол, предусматривающий установку соединения с получателем данных в коммутационной среде, а также передачу пакетов небольшого размера

(53 байта). Пакеты данных в сетях ATM называются ячейками. Поскольку размер ячеек фиксирован и известен заранее, коммутаторы и маршрутизаторы могут работать очень быстро. В этом проявляется основное преимущество сетей ATM по сравнению с сетями Ethernet, где размер фрейма различен и может изменяться в процессе передачи данных.

ATM. См. *Asynchronous Transfer Mode*.

ATMARP. Этот протокол выполняет в сетях ATM функцию, аналогичную функции протокола *ARP* в сетях Ethernet (преобразование IP-адреса в физический адрес).

Attenuation (ослабление). Уменьшение амплитуды сигнала в процессе его прохождения через передающую среду, например медный или волоконно-оптический кабель. Этот показатель рассчитывается как логарифм соотношения между входным и выходным сигналами (или входным и выходным напряжениями в системе). Единица измерения — децибелы (дБ).

Audit trail (контрольный след). Механизм, с помощью которого в операционной системе фиксируются действия пользователя. В большинстве случаев перечень отслеживаемых действий определяется сетевым (системным) администратором.

Automatic Private IP Addressing (APIPA, автоматическая частная IP-адресация). Используя технологию APIPA, компьютеры могут получать IP-адреса автоматически (если, конечно, в локальной сети установлен DHCP-сервер). Компьютер, который нуждается в конфигурационной информации, автоматически выбирает адрес из диапазона от 169.254.0.0 до 169.254.255.255, а затем выполняет широковещательную рассылку ARP-пакета, который включает этот адрес. Если никакой другой компьютер не посылает сообщение о том, что данный IP-адрес уже используется, текущий компьютер выполняет автоматическую конфигурацию с учетом использования данного адреса. Если адрес уже используется, выбирается другой вариант, а затем все повторяется снова.

Autosensing. (автоматическое обнаружение). Способность сетевого адаптера автоматически определять величину полосы пропускания локальной сети (например 10 или 100 Мбит/с).

AWG. См. *American wire gauge*.

Backbone Cabling System Structure (структура магистральной кабельной системы). Каналы связи, объединяющие несколько узлов локальных сетей.

Backup Window (окно резервного копирования). Период времени, требуемый для выполнения резервного копирования в компьютерной системе. Как правило, пользователи не могут получить доступ к серверу в этот период времени. Эта концепция безнадежно устарела после появления центров обработки данных, функционирующих 24 часа в сутки. Резервное копирование, не блокирующее доступ пользователей, может осуществляться в сетях SAN наравне с использованием некоторых технологий RAID.

Bandwidth (пропускная способность). Диапазон частот, применяемых для передачи сигнала в сетевой среде.

Bindery (подшивка). Серверная база данных, используемая клиентами NetWare для идентификации и обеспечения доступа к ресурсам на сервере. В новых версиях NetWare (начиная с 5.0) заменена службой NDS (или eDirectory).

Bit Error Rate (BER, показатель количества ошибочных битов). Вычисляемое значение, которое представляет собой отношение количества ошибочных битов к общему числу битов, находящихся в текущей статистической выборке.

Bit Error Rate Tester (BERT, измеритель коэффициента ошибочных битов). Диагностический прибор, позволяющий определить показатель количества ошибок в канале связи.

Bluetooth («Голубой зуб»). Беспроводная связь «ближнего радиуса действия». Используется несущая частота 2,4 ГГц, область применения — обеспечение связи между компьютерами, мобильными телефонами, клавиатурами и прочими периферийными устройствами. Дальность действия не превышает несколько десятков метров.

BOOTP (протокол начальной загрузки). Этот протокол используется для загрузки бездисковых рабочих станций и прочих сетевых устройств, которые могут получать от сервера собственные IP-адреса и другую конфигурационную информацию.

Bridge (мост). Это устройство можно рассматривать в качестве «продвинутого» повторителя, снабженного набором дополнительных функций. Обычно мосты обладают встроенной памятью, в которой хранятся MAC-адреса. После приема данных, отправленных определенным компьютером, мост перенаправляет их не во все доступные сегменты, а только в тот физический сегмент, в котором находится компьютер-получатель. Благодаря описанной методике снижается широковещательный трафик, а также уменьшается коэффициент использования полосы пропускания. Существуют и другие типы мостов, которые могут обеспечивать такие функции, как трансляция различных сетевых протоколов, в результате чего осуществляется передача данных между разнородными сетями. Имеется также категория устройств, называемых беспроводными мостами. Они служат для поддержки беспроводного канала связи между отдельными сегментами кабельных сетей.

Bus (шина). Применительно к сетевым технологиям, шина представляет собой единственный кабель, объединяющий несколько компьютеров (или других сетевых устройств). Применительно к аппаратным компонентам компьютеров, шина является физическим путем, объединяющим ЦПУ, оперативную память, а также периферийные устройства (например, PCI-адаптеры).

Cable modem (кабельный модем). Используется для подключения клиентских компьютеров к кабельным телевизионным сетям. При этом параллельно с передачей сигнала кабельного ТВ передаются сетевые пакеты.

CAP. См. *Carrierless Amplitude Phase modulation*.

CardBus. Дальнейшее развитие семейства адаптеров PCMCIA. Устройства CardBus обладают несколькими замечательными свойствами, а именно, обеспечивают прямой доступ к памяти, снабжены 32-разрядной шиной данных, а также являются более быстродействующими, чем адаптеры PCMCIA. Устройства CardBus также потребляют меньше энергии, чем их предшественники, что играет большую роль для ноутбуков, питающихся от аккумуляторов в автономном режиме. В большинстве случаев устройства CardBus обладают обратной совместимостью с адаптерами PCMCIA.

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA, множественный доступ к среде с контролем несущей частоты и избеганием конфликтов). Метод, применяемый в беспроводных сетях клиентами, ожидающими получения доступа к совместно используемой полосе пропускания. Небольшой пакет, который передается сначала, содержит сведения о данных, передаваемых в остальных пакетах. Эта технология не исключает коллизии, вследствие чего ее применение связано с дополнительными издержками. Используется устаревшими сетями AppleTalk, а также некоторыми беспроводными сетями. См. также *Carrier Sense Multiple Access/Collision Detect*.

Carrier Sense Multiple Access/Collision Detect (CSMA/CD, множественный доступ с контролем несущей частоты и обнаружением конфликтов). Метод, применяемый ранними устройствами Ethernet для получения доступа к сетевой среде. Термин «контроль несущей частоты» означает, что узел, намеревающийся передать данные, сначала прослушивает сетевую среду для определения факта передачи данных другим устройством. Термин «множественный доступ» означает, что несколько компьютеров одновременно пытаются получить доступ к сетевой среде. Если два узла в сети начинают передачу данных приблизительно в одно и то же время, то возникает состояние конфликта. Термин «обнаружение конфликтов» означает, что узел может обнаруживать факт передачи данных, осуществляемой другим узлом. Каждый узел, вовлеченный в конфликт, ожидает в течение случайного периода времени, затем снова прослушивает сетевую среду и пытается передавать данные.

Carrierless Amplitude Phase (CAP) modulation (амплитудно-фазовая модуляция без использования несущей частоты). Методика, применяемая в линиях xDSL для приема-передачи данных. В технологии CAP используется широкий спектр частот для приема данных, а также более узкий спектр — для передачи данных.

Channel Service Unit (CSU, устройство обслуживания канала). Применяется в выделенных линиях для выполнения основных функций, необходимых для передачи данных по линии.

CIDR. См. *Classless Interdomain Routing*.

CIFS. См. *Common Internet File System*, а также *Server Message Block*.

Cladding (плакирование). Обозначение материала, применяемого в волоконно-оптических кабелях для отражения световых импульсов в направлении прозрачного сердечника.

Classless Interdomain Routing (CIDR, бесклассовая маршрутизация между доменами). Благодаря технологии CIDR устраняются ограничения, присущие основным маршрутизаторам Интернета. Это достигается путем отказа от традиционной системы, основанной на классах и использующей IP-адреса. Вместо традиционных адресов подсети (например, 255.255.0.0), значения суффиксов CIDR (такие как /18) указывают на количество битов, используемых сетевым адресом, в то время как остальные цифры определяют адрес узла. Таким образом, адреса класса A или B, поддерживающие большое количество узловых компьютеров, могут использоваться для поддержки многих сетей, а также обеспечивают сохранение ограниченного пространства адресов, поддерживаемого традиционным протоколом IPv4.

Client (клиент). В компьютерных сетях этот термин относится к компьютеру, получающему доступ к ресурсам другого компьютера, называемого *сервером*.

Coaxial cables (коаксиальные кабели). Кабели этого типа применялись в устаревших сетях для объединения компьютеров в единое целое. Кабели, применяемые в компьютерных сетях, существенно отличаются от телевизионных кабелей своим волновым сопротивлением и диаметром.

Collision domain (область конфликтов). Совокупность сетевых устройств в сети Ethernet, которые совместно используют сетевую среду. Каждый сетевой компонент «конкурирует» с другим компонентом за получение доступа к среде, в результате чего возникает конфликт (в случае, если несколько устройств пытаются начать передачу данных в одно время). Эта проблема практически исключена в современных сетях Ethernet, использующих *коммутаторы*.

Common Internet File System (CIFS, общая файловая система Интернета). Серверный протокол файлов/печати, который пришел на замену протоколу блока серверных сообщений (SMB, Server Message Block). Как и SMB, протокол CIFS использует набор протоколов TCP/IP в качестве транспортного протокола, служащего для обмена сообщениями и данными с другими компьютерами.

CRC. См. *Cyclic redundancy check*.

Cross-talk (перекрестные помехи). Электрический сигнал в медном кабеле распространяется не только по одной жиле, но может расходиться в перпендикулярных направлениях, вызывая наводки в соседних жилах. Подобное явление называется *перекрестной помехой*.

CSMA/CD. См. *Carrier Sense Multiple Access/Collision Detect*.

CSU. См. *Channel Service Unit*.

Cut-through switch (небуферизующий коммутатор). Коммутатор, который начинает передачу полученного фрейма в направлении порта вывода после получения заголовочной информации (около 20 или 30 байтов от входящего порта). В этом случае коммутатор нуждается в определении порта, передающего фрейм, то есть физического адреса компьютера-получателя, который заключен в заголовке фрейма.

Cyclic redundancy check (CRC, циклический избыточный код). Значение, вычисляемое в соответствии со специальным математическим алгоритмом. Значение CRC может быть получено на основе информации заголовка или раздела данных сетевого фрейма. При помощи кода CRC проверяется целостность передаваемых данных.

Data Over Cable Service Interface Specification (DOCSIS, спецификация интерфейса услуги передачи данных по кабелю). Эта спецификация разработана фирмой CableLabs и обеспечивает стандартизацию услуг кабельных модемов. Фирма CableLabs также сертифицирует аппаратное обеспечение, благодаря чему устройства с меткой DOCSIS могут взаимодействовать между собой.

Data Service Unit (DSU, модуль обслуживания данных). Это устройство применяется в выделенных линиях для выполнения преобразований между применяемыми кодировками данных. Устройства DSU также выполняют другие функции, например коррекцию ошибок. Обычно они снабжены соединителями RS-232C или RS-449, применяемыми для подключения к терминальному оборудованию (DTE), обеспечивающему физическое подключение к локальной сети. Используемые в выделенных линиях устройства CSU и DSU часто комбинируются в виде единого блока.

DECnet. Набор патентованных сетевых протоколов, разработанных компанией Digital Equipment Corporation.

Demilitarized zone (демилитаризованная зона). Сегмент сети, подключаемый к Интернету при помощи брандмауэра, изолированный от внутренней сети другим брандмауэром. Компьютеры, находящиеся между двумя брандмауэрами, относятся к так называемой демилитаризованной зоне, и они менее защищены, чем те компьютеры, которые находятся во внутренней локальной сети. Описанная методика часто применяется для обеспечения доступа к веб-серверам (или к другим подобным серверам), которые нуждаются в обеспечении некоторой степени безопасности. Благодаря второму брандмауэру обеспечивается дополнительная степень безопасности для клиентов локальной сети.

Denial-of-service attack (атака отказа в обслуживании). Тип атаки, суть которой заключается в выводе из строя маршрутизаторов, серверов, компьютеров или других компонентов путем массированного потребления ресурсов со стороны другого компьютера или сети. В этом случае атакованные устройства не могут функционировать в обычном режиме.

DFS. См. *Distributed File System*.

DHCP. См. *Dynamic Host Configuration Protocol*.

Dialectic (изолятор). Изоляционный материал, в который заключаются проводники тока. Обычно изготавливается из пластика или другого непроводящего материала и применяется для разделения проводов в кабеле.

Digital subscriber line (DSL, цифровая абонентская линия). Линия DSL предполагает использование полосы частот, значительно превышающей стандартную полосу частот 4 МГц, выделенную для передачи речи в обычных телефонных

линиях. Иногда эта технология называется xDSL, поскольку многие провайдеры предлагают услуги, которые достаточно сильно варьируются в заданной полосе пропускания для передачи/приема данных. Для передачи сигналов в DSL-линиях применяются несколько методов, например, CAP (Carrierless Amplitude Phase, амплитудно-фазовая модуляция без передачи несущей) и DMT (Discrete MultiTone, цифровая мультитональная модуляция).

Digital Subscriber Line Access Multiplexer (DSLAM, мультиплексор доступа к цифровой абонентской линии). Устройство, объединяющее несколько абонентских линий, которое мультиплексирует сигналы в соответствии с одним или большим количеством интерфейсов с большей полосой пропускания, например, ATM или Frame Relay.

Directory (каталог). Совокупность файлов и каталогов, которые могут включать другие каталоги. Применительно к Active Directory или к другой базе данных LDAP каталог будет обозначать базу данных, в которой хранятся объекты, управляемые службой каталогов.

Directory services (службы каталогов). Набор программ, управляющих базой данных каталогов, таких как Active Directory или eDirectory, разработанных фирмой Novell.

Discrete MultiTone (DMT, цифровая мультитональная модуляция). Технология xDSL, которая предусматривает разделение частот, выходящих за пределы канала передачи речи шириной 4 МГц, на 256 каналов. Именно метод DMT чаще всего применяется DSL-технологиями. Также см. *Carrierless Amplitude Phase*.

Disparity (несоответствие). Термин, применяемый в сетях Fibre Channel для описания количества нулей и единиц, переданных в сетевой среде. Если при оценке передачи данных, осуществляемой в течение короткого периода времени, количество нулей превышает число единиц, определяется *отрицательное несоответствие*. Если же передается больше единиц, значит, речь идет о *положительном несоответствии*. Когда количество нулей примерно равно количеству единиц — это случай *нейтрального несоответствия*.

Distributed Coordination Function (DCF, распределенная координирующая функция). Альтернативное название метода CSMA/CA.

Distributed denial-of-service attack (DDoS, распределенная атака отказа в обслуживании). Эта атака осуществляется одновременно с нескольких десятков или даже тысяч компьютеров. В результате становятся практически неэффективными защитные мероприятия, осуществляемые путем простой блокировки IP-адресов или портов.

Distributed File System (DFS, распределенная файловая система). Как и в случае с NFS от Sun, этот метод обеспечивает использование компьютерами Windows общих файловых систем путем монтирования части или всей файловой системы на удаленном компьютере. При этом создается впечатление, что файлы, находящиеся на удаленных компьютерах, являются частью локальной файловой системы.

DMT. См. *Discrete MultiTone*.

DMZ. См. *Demilitarized zone*.

DNS. См. *Domain Name System*.

DOCSIS. См. *Data Over Cable Service Interface Specification*.

Domain Name System (DNS, система имен доменов). Иерархическая система, обеспечивающая преобразование имен узлов и сетей в IP-адреса. Система DNS является «сердцем» Интернета, которое ответственно за преобразование имен. Каждый домен включает два (или больше) DNS-сервера, которые относятся к определенному домену. Для преобразования сетевого имени DNS-серверы запрашивают другие DNS-серверы, которые находятся ниже в иерархии, до момента нахождения соответствующего DNS-сервера или до тех пор, пока не находится другой DNS-сервер, который хранит в оперативной памяти расположение преобразованных имен. Обратите внимание на различия между приведенным определением и определением DNS-сервера, который поддерживает базу данных DNS.

DSL. См. *Digital subscriber line*.

DSLAM. См. *Digital Subscriber Line Access Multiplexer*.

DSU. См. *Data Service Unit*.

Dynamic DNS (динамический DNS). Сервер DNS, который может принимать обновления, поступающие в динамическом режиме от сетевого клиента. Динамический DNS работает совместно с DHCP для включения сетей, которые часто изменяются в целях поддержки обновленной информации. Также см. *Dynamic Host Configuration Protocol*.

Dynamic Host Configuration Protocol (DHCP, протокол динамической конфигурации узла). Протокол, используемый для получения клиентским компьютером необходимых адресов, а также другой конфигурационной информации, принимаемой с центрального сервера DHCP. Благодаря этому сетевой администратор может вручную конфигурировать каждый сетевой клиент. Используя последний, клиент сразу же получает конфигурационную информацию от сервера DHCP, требуемую для обновления DNS-сервера. См. *Dynamic DNS*.

Dynamic packet filter (динамический фильтр пакетов). См. *Stateful Inspection*.

E_Port (порт расширения). Этот порт применяется для подключения коммутатора Fibre Channel к другому такому же коммутатору.

EBCDIC. См. *Extended Binary-Coded Decimal Interchange Code*.

EDirectory. Расширенная версия службы каталогов Novell (NDS, Novell Directory Services). Эта служба поддерживает обратную совместимость с NetWare 5. Многие свойства eDirectory могут использоваться другими операционными системами, например UNIX и Windows. Также см. *Novell Directory Services*.

EISA. См. *Extended Industry Standard Architecture*.

Electromagnetic interference (EMI, электромагнитные помехи). Наводки между соседними жилами в медном кабеле. Высокочастотные сигналы, передаваемые по медному кабелю, распространяются в тонком внешнем проводящем слое, излучая помехи в окружающее пространство.

EMI. См. *Electromagnetic interference*.

Encryption (шифрование). Процесс, реализующий выполнение некоторых функций по отношению к набору данных, в результате чего производится их преобразование в формат, который непонятен и не может быть прочитан кем-либо, кроме адресата. См. *Single key* и *Public key encryption*.

Ethernet. Наиболее распространенный тип локальных сетей. Изначально Ethernet основывалась на результатах исследования Роберта Меткальфа. Затем эта технология получила развитие силами фирм Digital Equipment Corporation, Intel и Xerox (DIX). В настоящее время Ethernet-технология развилась до такой степени, что стала практически универсальной. В частности, она обеспечивает поддержку коммутаторов, повышенной полосы пропускания, а также некоторых других свойств, благодаря чему становится привлекательной для бизнеса, корпораций, а также домашних пользователей. Технология Ethernet поддерживается и в беспроводных сетях.

Extended Binary-Coded Decimal Interchange Code (EBCDIC, расширенный двоично-десятичный код обмена информацией). Метод, применяемый для шифрования алфавитных, цифровых и других символов с помощью 256 двоичных чисел. Код EBCDIC изначально предназначался для операционных систем мэйнфреймов IBM. Позднее фирма IBM разработала архитектуру PC, где использовалась кодировка ASCII или Unicode. Код EBCDIC в настоящее время используется исключительно мэйнфреймами IBM, в связи с чем не столь широко распространен, как раньше.

Extended Industry Standard Architecture (EISA, расширенная стандартная архитектура для промышленного применения). Шина, совместимая с патентованной шиной от IBM, называемой MicroChannel. Шина EISA функционирует на тактовой частоте 8 МГц, как и шина ISA, но ее разрядность составляет 32 бита, благодаря чему обеспечивается большее быстродействие.

F Port. Порт коммутатора Fibre Channel, используемый для подключения к устройству.

Far-end cross-talk (перекрестные помехи на дальнем конце). Передающий конец кабельной пары, генерирующий сильный электрический сигнал. Вследствие затухания сигнала по мере прохождения по медному или волоконно-оптическому кабелю наводки между жилами кабеля в конечной точке могут привести к искажению сигнала.

Fast Ethernet. См. *100BASE-T*.

FDDI. См. *Fiber Distributed Data Interface*.

FEXT. См. *Far-end cross-talk*.

Fiber Distributed Data Interface (FDDI, распределенный интерфейс передачи данных по волоконно-оптическим каналам). Топология с двойным кольцом, в которой сетевой трафик передается от одного узла к другому. И хотя эта технология используется по-прежнему, она начинает вытесняться более новыми технологиями. Одно из преимуществ FDDI заключается в том, что в случае возникновения неполадки в одном из двух колец (например, разрыв кабеля или выход узла из строя) обмен данными может продолжаться по другому кольцу, в результате чего обеспечивается эффективная изоляция проблемы вплоть до ее полного устранения. В сетях FDDI могут применяться одно- и многомодовые оптоволоконные кабели. Скорость передачи данных варьируется в диапазоне от 10 до 100 Мбит/с.

Fiber-optic cable (волоконно-оптический кабель). Кабель, который состоит из стеклянного (пластикового) сердечника, окруженного материалом, отражающим свет в обратном направлении, то есть в направлении сердечника. Одномодовые кабели снабжены тонким сердечником (от 9 до 12,5 мкм), а многомодовые кабели имеют более толстый сердечник (обычно от 50 до 62,6 мкм). Одномодовые кабели лучше работают на больших расстояниях, но достаточно дороги, в то время как многомодовые кабели лучше использовать на небольших расстояниях вследствие их дешевизны.

Fibre Channel (волоконно-оптический канал). Коммуникационный протокол, который в настоящее время преимущественно используется в сетях SAN. При этом между двумя устройствами устанавливаются два канала связи — один для передачи данных, а второй — для приема данных. Эти кабели соединяются таким образом, что передатчик одного устройства подключается к приемнику, находящемуся на противоположной стороне канала связи. В сетях SAN протокол Fibre Channel применяется для ускорения доступа (обычно с помощью волоконно-оптических кабелей) к хранилищам данных на больших расстояниях, когда исключено применение стандартной архитектуры SCSI. Протокол Fibre Channel может также применяться другими технологиями для обеспечения передачи данных.

File Transfer Protocol (FTP, протокол передачи данных. Протокол, при помощи которого сетевые устройства могут отсылать и принимать данные, а также получать список файлов, размещенных на другом устройстве.

Firewall (брандмауэр). Устройство, которое было разработано в целях обеспечения защиты сети от доступа, осуществляемого из другой сети. Например, брандмауэр может находиться между вашей сетью и Интернетом, либо между отделами, подключенными к внутренней сети. Эти устройства применяют такие технологии, как фильтрация пакетов, проверка изменяемого в процессе выполнения состояния, прокси-серверы и фильтрация содержимого.

FireWire. Описанная в стандарте IEEE 1394 высокоскоростная последовательная шина (скорость передачи данных обычно варьируется в диапазоне от 100 до 400 Мбит/с), предусматривающая подключение к компьютеру до 63 устройств. Подобно USB, шина FireWire поддерживает «горячее» подключение,

благодаря чему пользователь может подключать/отключать устройства, не выполняя перезагрузку компьютера.

FL_Port. Порт, через который петля с арбитражной логикой (Arbitrated Loop) подключается к коммутатору Fibre Channel.

Frequency (частота). Единица измерения, позволяющая количественно оценить периодическое действие, которое выполняется в течение выбранного временного интервала. Альтернативное определение частоты — количество циклов за одну секунду. Как правило, частота измеряется в герцах (Гц).

Frequency Hopping (девиация частоты). Передача данных путем быстрого изменения несущей частоты на заранее определенную величину. Используется некоторыми протоколами беспроводных сетей во избежание помех, возникающих при работе устройств, которые используют один и тот же диапазон частот.

FTP. См. *File Transfer Protocol*.

Full-duplex (дуплексный режим). Коммуникации между двумя сетевыми узлами, которые одновременно осуществляются в обоих направлениях. Также см. *Half-duplex*.

GID. Числовое значение, применяемое в системах UNIX/Linux, с помощью которого идентифицируется группа пользователей, к которой относится учетная запись. Файл `/etc/group` включает перечень пользовательских групп, а также связанные с ними числа. Группы могут применяться для управления доступом к системным ресурсам, например к файлам и каталогам, что значительно проще в реализации, поскольку доступ может предоставляться группе в целом, а не отдельным пользователям.

Gigabit Ethernet. Разновидность сети Ethernet, данные в которой передаются со скоростью 1 Гбит/с, определенная стандартом IEEE 802.3.

Half-duplex (полудуплексный режим). Коммуникации между двумя сетевыми узлами, причем одновременная передача данных невозможна.

HBA. См. *Host Bus Adapter*.

HomeRF. Эта спецификация изначально предназначалась для использования в домашних беспроводных сетях. Позднее она была расширена в целях включения некоторых функциональных свойств, которые уже поддерживаются стандартами 802.lib и 802. В настоящее время на рынке активно продаются устройства, совместимые с HomeRF, но их следует рассматривать в контексте упомянутых стандартов IEEE.

Hop (переход). Термин, определяющий количество маршрутизаторов, через которые проходит сетевой пакет, прежде чем достигает цели. Это значение может изменяться для форсирования сетевого трафика при использовании специального маршрута. Также см. *метрика* и *затраты*.

Horizontal Cabling System Structure (структура горизонтальной разводки кабелей). Система кабелей, которая соединяет коммуникационное подключение в рабочей области с аппаратной.

Host Bus Adapter (HBA, адаптер главной шины). Этот термин обозначает плату адаптера, которая подключает компьютер к интерфейсу Fibre Channel сети SAN. Адаптер HBA отличается от адаптера Ethernet тем, что выполняет больше функций, благодаря чему разгружает центральный процессор.

Hostname (имя узла). Имя сетевого узла, которое можно определить с помощью команды `hostname`.

HOSTS (файл HOSTS). Файл, используемый для преобразования имен узлов в IP-адреса. На практике применяется редко, поскольку существует более прогрессивная система имен доменов (DNS, Domain Name System). Файлы HOSTS по-прежнему используются для выполнения трансляции, отличной от осуществляемой DNS-сервером.

HTML. См. *Hypertext Markup Language*.

HTTP. См. *Hypertext Transfer Protocol*.

Hub (концентратор). Устройство, в котором «концентрируются» кабели витой пары локальной сети, образуя звездообразную структуру. При этом каждое сетевое устройство подключается к отдельному порту концентратора. Сами концентраторы напоминают многопортовые повторители, отличаясь от них тем, что изначально рассчитаны на сеть 10BASE-T, в то время как повторители подключаются к «тонкой сети» (10BASE-2). В процессе дальнейшей эволюции концентраторов они «научились» изолировать сетевые сегменты, передающие поврежденные данные, а также работать с протоколом SNMP. В настоящее время вместо концентраторов в корпоративных и SOHO-сетях используются коммутаторы.

Hypertext Markup Language (HTML, язык гипертекстовой разметки). Язык программирования, применяемый для разработки веб-страниц. Предусматривается использование набора определенных символов, с помощью которых описывается, каким образом текст, изображения, а также другие данные отображаются для пользователя, получающего доступ к веб-сайту при помощи браузера.

Hypertext Transfer Protocol (HTTP, протокол передачи гипертекста). Протокол, использующий TCP/IP для получения и ответа на запросы данных, использующих World Wide Web. Хотя большая часть данных, передаваемых HTTP, включает HTML-страницы, могут передаваться и другие объекты.

ICMP. См. *Internet Control Message Protocol*.

ICMP redirects (перенаправления ICMP). Протокол управляющих сообщений Интернета (Internet Control Message Protocol) может применяться для манипуляции таблицами маршрутизации, которая обычно осуществляется при помощи отсылки маршрутизатору сообщений, говорящих о невозможности соединения с компьютером-получателем данных. Этот тип атаки может привести к затруднениям обмена данными между вашей сетью и другими сетями, поскольку «портится» информация в таблице маршрутизации.

IEEE (Institute of Electrical and Electronics Engineers, Институт инженеров по электротехнике и электронике). Профессиональная организация, которая отвечает за разработку многих стандартов, включая сетевые.

IEEE 802 LAN/MAN Standards Committee (Комитет IEEE по разработке стандартов для локальных/городских сетей). Комитет IEEE, который занимается разработкой стандартов для локальных/глобальных сетей. Этот комитет был сформирован в 1980 году, причем изначально он назывался комитетом по разработке стандартов для локальных сетей (Local Network Standards Committee).

IEEE 802.11a. Беспроводной сетевой протокол, разработанный Институтом IEEE. Предусматривается работа с использованием несущей частоты 5 ГГц и поддерживается скорость передачи данных до 54 Мбит/с.

IEEE 802.11b. Беспроводной сетевой протокол, разработанный Институтом IEEE. Предусматривается работа с использованием несущей частоты 2,4 ГГц и поддерживается скорость передачи данных до 11 Мбит/с.

IEEE 802.11g. Беспроводной сетевой протокол, разработанный Институтом IEEE. Предусматривается работа с использованием несущей частоты 2,4 ГГц (как и 802.11b), скорость передачи данных — до 54 МГц. Большинство устройств, совместимых с 802.11g, могут одновременно работать с устройствами, совместимыми с протоколом 802.11b, поэтому они будут преобладать на рынке по сравнению с устройствами 802.11a. Большая скорость передачи данных на несущей частоте 2,4 ГГц обеспечивается благодаря более изощренной методике кодирования данных.

IEEE 1394. См. *FireWire*.

Ifconfig. Эта команда используется системами UNIX/Linux и подобна Windows-команде ipconfig. Данная команда может применяться не только для отображения сведений о конфигурации, но и для конфигурирования сетевых интерфейсов.

iFolder. Технология, используемая в NetWare для обеспечения доступа и синхронизации между данными, полученными от удаленных клиентов и серверов. Обычно используется мобильными клиентами для обеспечения синхронизации данных, размещенных на серверах/клиентах.

IMAP. См. *Internet Message Application Protocol*.

Industrial, Scientific and Medical (ISM, Radio Frequency Band). Полоса радиочастот, используемых промышленными, научными и медицинскими организациями. Использование этого диапазона частот не требует специального разрешения. Она была выбрана для беспроводных сетей, основанных на стандартах IEEE 802.11b и IEEE 802.11g.

Industry Standard Architecture (ISA, стандартная промышленная архитектура). Название оригинальной шины PC, разработанной в 1980-х годах. Эта компьютерная шина работала с тактовой частотой 8 МГц, используя 16-разрядный канал данных для подключения компонентов к оперативной памяти и центральному процессору компьютера.

Integrated Services Digital Network (ISDN, цифровая сеть связи с комплексными услугами). Цифровой канал связи, который состоит из B-канала (передача речи и данных), а также одного или большего количества D-каналов, передающих управляющую и сигнальную информацию. Интерфейс основного уровня (PRI, Primary Rate Interface) включает один D-канал, а также два 65-килобитовых B-канала (в результате получается общая полоса пропускания в 128 Кбит/с). Службы интерфейса основного уровня могут поддерживать до 23 B-каналов (или 30 B-каналов для Европы), что приводит к значительному увеличению скорости передачи данных.

Internet (Интернет). Объединение многих сетей во всемирном масштабе, которому предшествовала сеть ARPANET.

Internet Control Message Protocol (ICMP, протокол управляющих сообщений Интернета). Протокол, в котором предусматривается использование UDP-пакетов для проведения диагностики при функционировании набора протоколов TCP/IP.

Internet Message Application Protocol (IMAP, протокол доступа к сообщениям в Интернете). Благодаря этому протоколу пользователи могут просматривать, загружать или удалять сообщения электронной почты с почтового сервера. В то время как протокол POP3 загружает все сообщения электронной почты с почтового сервера на клиентский компьютер, протокол IMAP позволяет оставлять сообщения на сервере, просматривать заголовки, сообщения и вложения. Пользователь также может явным образом удалять сообщения с сервера.

Internet Printing Protocol (протокол печати Интернета). Используя этот протокол, пользователи Интернета могут подключаться к любому доступному в Интернете принтеру.

Internet Protocol (протокол Интернета). Основа набора протоколов TCP/IP. Протокол IP не ориентирован на установку соединений, не является надежным, а также обеспечивает передачу данных из одного места в другое с наименьшими затратами. Этот протокол поддерживает иерархическое адресное пространство, которое делает возможной маршрутизацию между сетями. Протоколы TCP, UDP, а также некоторые другие из набора TCP/IP используют IP-протокол для маршрутизации данных во внутренних сетях, а также в Интернете. Протоколы верхнего уровня, использующие IP, отвечают за поддержание механизмов, гарантирующих надежность доставки данных.

Internetwork Packet Exchange (обмен пакетами в объединенной сети). Протокол NetWare, применяемый для передачи данных между несколькими сетями NetWare. Также см. *Sequenced Packet Exchange*.

Interrupt Request (IRQ, запрос прерывания). Запрос прерывания (IRQ) может использоваться устройствами для отсылки сигнала прерывания центральному процессору с целью «привлечения его внимания». Это достигается с помощью линии запроса прерывания, подключенной к процессору. Несмотря на то, что многие устройства используют собственные значения прерывания (числовые

значения), некоторые устройства могут совместно использовать один и тот же номер прерывания.

Intranet (внутренняя сеть). Набор сетей, подключенных с помощью маршрутизаторов, в результате чего образуется частная сеть.

IP. См. *Internet Protocol.*

ipconfig. Эта команда может применяться компьютерами Windows (от Windows NT и выше) для просмотра текущих IP-настроек, а также других конфигурационных установок. Другие свойства этой команды могут использоваться для освобождения/обновления конфигурационной информации DHCP, а также некоторых других настроек.

IPP. См. *Internet Printing Protocol.*

iPrint. Реинкарнация протокола Internet Printing Protocol в NetWare. Также см. Internet Printing Protocol.

IPX. См. *Internetwork Packet Exchange.*

IRQ. См. *Interrupt Request.*

ISA. См. *Industry Standard Architecture.*

ISDN. См. *Integrated Services Digital Network.*

ISO. Официальное название Международной организации стандартизации (International Organization for Standardization).

LAN (ЛВС). См. *Local area network.*

LDAP. См. *Lightweight Directory Access Protocol.*

LED (Light-emitting diode, светодиод). Экономичное полупроводниковое устройство, излучающее свет после подачи на него напряжения (с соблюдением полярности). Обычно светодиоды используются в сетевых адаптерах, а также других сетевых устройствах (концентраторы или коммутаторы) для индикации корректного функционирования устройств. Светодиоды могут также использоваться вместо лазеров для передачи данных по волоконно-оптическим кабелям.

LIFA. См. *Loop Initialization Fabric Address.*

Lightweight Directory Access Protocol (LDAP, упрощенный протокол службы каталогов). Каталоги и службы каталогов, основанные на протоколах X.500. Клиенты могут получать доступ к LDAP-совместимым каталогам из разных операционных систем. Протокол LDAP использует структуру каталогов, описанную протоколом X.500, но службы, поддерживаемые протоколом X.500, были «облегчены» в целях снижения уровня издержек для клиента и сервера.

LIHA. См. *Loop Initialization Hard Address.*

LILP. См. *Loop Initialization Loop Position.*

LIP. См. *Loop Initialization Primitive.*

LIPA. См. *Loop Initialization Previous Address*.

LIRP. См. *Loop Initialization Report Position*.

LISA. См. *Loop Initialization Soft Address*.

LISM. См. *Loop Initialization Select Master*.

LMHOSTS. Также см. файл HOSTS. Этот файл применяется в устаревших операционных системах Windows, где используются имена NetBIOS, в целях выполнения преобразования между именами узлов и IP-адресами. Для автоматизации этого процесса была разработана служба имен Интернета для Windows (WINS, Windows Internet Name Service). Служба DHCP может назначать IP-адреса клиентам Windows, а служба WINS может в динамическом режиме выполнять трансляцию пар «имя/адрес». В большинстве современных операционных систем Windows используются DNS-серверы.

Load coil (нагрузочная катушка). Устройство, применяемое в аналоговых телефонных схемах для усиления речи. Поскольку эти устройства могут вызывать взаимные наводки с частотами около 4 МГц, соответствующими речевому диапазону обычных телефонных линий, это может препятствовать нормальному функционированию службы DSL.

Local area network (LAN, локальная сеть). Небольшая сеть, используемая для соединения сетевых устройств, находящихся недалеко друг от друга, например в офисе.

Logical topology (логическая топология). Логический путь в сети, определяющий порядок передачи данных из одного места в другое. Также см. *Physical topology*.

Loop Initialization Fabric Address (LIFA, «зашитый» адрес, используемый при инициализации петли). Первый фрейм, используемый для назначения адресов в сети волоконно-оптических каналов с арбитражной логикой (Fibre Channel Arbitrated Loop). Устройства, которым назначаются адреса коммутаторами Fibre Channel, могут их регистрировать с помощью этого фрейма.

Loop Initialization Hard Address (LIHA, физический адрес, используемый при инициализации петли). Третий фрейм, применяемый для назначения адресов в сети волоконно-оптических каналов с арбитражной логикой (Fibre Channel Arbitrated Loop). Устройства, которым назначаются адреса коммутаторами Fibre Channel, могут их регистрировать с помощью этого фрейма.

Loop Initialization Loop Position (LILP, позиция при инициализации петли). Последний фрейм, отсылаемый в сетях Fibre Channel Arbitrated Loop для того, чтобы каждое подключенное устройство «знало» о позициях остальных устройств в петле.

Loop Initialization Previous Address (LIPA, предыдущий адрес, используемый при инициализации петли). Второй фрейм, применяемый для присвоения адресов в сети волоконно-оптических каналов с арбитражной логикой (Fibre

Channel Arbitrated Loop). Устройства, запоминающие предыдущий адрес, могут регистрировать его с помощью данного фрейма.

Loop Initialization Primitive (LIP,. примитив, используемый при инициализации петли). Фреймы, используемые в процессе инициализации в сети волоконно-оптических каналов с арбитражной логикой (Fibre Channel Arbitrated Loop).

Loop Initialization Report Position (LIRP, Отчет о позиции при инициализации петли). Фрейм, используемый в процессе инициализации устройств, поддерживающих петли с арбитражной логикой, для определения их позиции в петле. После получения этих данных мастер-петля отсылает фрейм позиции в петле инициализации (LILP, Loop Initialization Loop Position) по петле. В результате все устройства получают сведения о позициях других устройств в петле.

Loop Initialization Select Master (LISM, выбор мастера при инициализации петли). Эта процедура применяется для выбора временной мастер-петли, которая координирует назначения адресов при инициализации в сети волоконно-оптических каналов с арбитражной логикой (Fibre Channel Arbitrated Loop).

Loop Initialization Soft Address (LISA, программный адрес, используемый при инициализации петли). Последний фрейм, применяемый для назначения адресов в сети волоконно-оптических каналов с арбитражной логикой (Fibre Channel Arbitrated Loop). Любое устройство, для которого не был назначен адрес с помощью предыдущих фреймов, может выбирать требуемый адрес на основе этого фрейма.

Loop Master (мастер-петля). Устройство в сети волоконно-оптических каналов с арбитражной логикой, которое временно выбирается для координации функций назначения адресов и составления отчетов в процессе инициализации петли.

Lpr/lpd (Line printer remote/line printer daemon, демон удаленного/строкового принтера). Эти утилиты UNIX обеспечивают отсылку заданий на печать удаленным компьютерам. В общем случае для этого применяется современная печать с применением TCP-потоков.

MAC address. MAC-адрес. См. *Media Access Control*.

MAN. ГВС. См. *Metropolitan Area Network*.

Media Access Control (MAC, контроль доступа к среде). Подуровень канального уровня модели OSI. На этом подуровне формируются фреймы, передаваемые в физической сетевой среде. Как правило, MAC-адрес жестко программируется в сетевом адаптере производителем, причем в этом случае формируется одномерное пространство адресов. Обычно MAC-адреса применяются внутри единой локальной сети, а IP-адреса — для взаимодействия между устройствами, находящимися в разных локальных сетях, посредством маршрутизатора.

Media access unit (MAU)/multistation access unit (MSAU) (устройство подключения к сети/устройство многостанционного доступа). Как и в случае с концентратором Ethernet, подобные устройства объединяют кабели в сетях Token-Ring. Возможности устройств MAU/MSAU улучшены по сравнению

с простым концентратором, в частности возможна изоляция «некорректных» портов, благодаря чему восстанавливается передача данных в кольце. Эти устройства блокируют широковещательное распространение трафика, получаемого всеми портами, как это происходит в случае простого концентратора. Устройства MAU/MSAU поддерживают кольцевую топологию, передавая фреймы между соседними портами.

Mesh topology (ячеистая топология). Эта топология определяет сеть, в которой каждое устройство связано с любым другим устройством. На практике применяются коммутаторы и серверы, которые подключают клиентов к сети. Ячеистая топология обеспечивает высокую степень избыточности. Это полезно в том случае, когда сеть должна быть исключительно надежной. Данная топология также пригодна для описания многих беспроводных сетей.

Metric (метрика). Этот термин является синонимом понятия «количество переходов». Это ограничение количества маршрутизаторов, через которые проходит сетевой пакет, прежде чем он будет отменен. Поэтому может применяться альтернативное название «количество переходов» или «цена» маршрута. Это значение применяется протоколами дистанционно-векторной маршрутизации для присваивания значения маршрутизатору. Можно изменять это значение для различных маршрутов в конкретном направлении, форсируя передачу трафика по выбранному маршруту.

Metropolitan Area Network (MAN, городская сеть). Сеть, которая больше локальной сети, но меньше глобальной. Этот термин относится к сети, которая охватывает город или эквивалентную ему по площади географическую область.

MicroChannel (микроканальная архитектура). Эта шина была разработана фирмой IBM.

Microsoft Management Console (MMC, консоль управления Microsoft). Обобщенный интерфейс, появившийся в Windows 2000, предоставляющий доступ ко многим управляющим утилитам. Основные утилиты находятся в папке Administrative Tools.

MMC. См. *Microsoft Management Console*.

Modem (модем). Это слово образовано на базе двух слов, «модуляция/демодуляция». Благодаря модемам компьютеры могут обмениваться цифровой информацией по аналоговым линиям (например, по линиям телефонной связи). Как правило, модемы применяются для подключения к Интернету, хотя иногда могут применяться для формирования подключения удаленного доступа. В настоящее время эти устройства медленно вытесняются широкополосными соединениями, например DSL-линиями.

Multi-mode fiber-optic cabling. (многомодовый оптический кабель). Волоконно-оптический кабель, в котором используется пластиковый или стеклянный сердечник, диаметр которого больше, чем в случае одномодового кабеля. Вместо фиксированной длины световой волны в многомодовых кабелях применяются различные световые волны различной длины, каждая из которых

отражается под своим углом, в результате чего исключается взаимная интерференция между ними.

Multi-Protocol Label Switching (MPLS, многопротокольная коммутация меток). Этот протокол применяется коммутаторами уровня 3. Пакет попадает в сеть MPLS через входной маршрутизатор LSR (Label Switching Router, маршрутизатор с коммутацией меток), который прикрепляет метку к пакету, а выходит за пределы сети MPLS через выходной маршрутизатор LSR. Во входном маршрутизаторе осуществляется необходимая обработка для определения пути передачи пакета в коммутируемой сети. В сети MPLS IP-протокол воспринимается как протокол, ориентированный на установку соединений. Подобные функции обычно поддерживаются протоколом TCP.

NAS. См. *Network Attached Storage*.

NAT. См. *Network Address Translation*.

NDIS. См. *Network Driver Interface Specification*.

NDS. См. *Novell Directory Services*.

Near-end cross-talk (перекрестные помехи на ближнем конце). Наводки, возникающие между двумя кабелями витой пары. Также см. *Far-end cross-talk*.

Negative disparity (отрицательное несоответствие). См. *Disparity*.

NetBEUI (NetBIOS Extended User Interface, расширенный пользовательский интерфейс NetBIOS). Регулирует передачу пакетов данных в локальной сети. Этот протокол был разработан компаниями IBM и Microsoft. Вообще говоря, NetBEUI является немаршрутизируемым протоколом локальной сети, поэтому в настоящее время практически не применяется.

NetBIOS (Network Basic Input/Output System, базовая сетевая система ввода/вывода). Разработана компанией IBM, используется сетевыми операционными системами Microsoft, а также ОС других производителей. Система NetBIOS предоставляет в распоряжение разработчика приложений стандартный интерфейс, называемый блоком управления сетью (NCB, Network Control Block). В то время как TCP/IP использует IP-адресацию, NetBIOS применяет соглашение о наименовании, которое включает уникальные имена или группы имен. Базовый транспортный протокол (обычно NetBEUI или TCP/IP) «прозрачен» для NetBIOS. Используемый многие годы операционными системами Windows, в настоящее время этот протокол поддерживается главным образом в целях обратной совместимости с устаревшими приложениями. В новейших версиях Windows, а также других операционных системах обычно используется TCP/IP. Для выполнения трансляции между именами NetBIOS и IP-адресами применяется служба WINS. Альтернативой этому протоколу служит *SAMBA*.

Netstat. Команда, используемая в системах Windows и в некоторых системах UNIX/Linux для получения статистики о протоколах TCP/IP, применяемых на данном компьютере.

NetWare. Сетевая операционная система, разработанная фирмой Novell.

Network Address Translation (NAT, трансляция сетевых адресов). Благодаря NAT можно использовать один или больше IP-адресов, которые допустимы в Интернете, а для компьютеров в локальной сети резервировать собственное пространство адресов. Сервер NAT (например, маршрутизатор/коммутатор) использует собственный корректный адрес Интернета для осуществления трансляции между адресом частной сети и адресом, допустимым в Интернете.

Network analyzer (сетевой анализатор). Устройство, выполняющее мониторинг сети на канальном и транспортном уровнях модели OSI. С его помощью можно отслеживать ошибки, в том числе связанные с протоколом. Для некоторых операционных систем, например серверов Windows, разработана упрощенная версия этого устройства. В среде UNIX/Linux можно воспользоваться утилитой `tcpdump`, обладающей подобными функциональными свойствами. Хороший сетевой анализатор обладает и рядом других полезных свойств.

Network Attached Storage (NAS, подключаемое к сети устройство хранения данных). Устройства хранения данных (диски/ленты), подключенные к сети, используемой клиентскими компьютерами.

Network Driver Interface Specification (NDIS, спецификация стандартного интерфейса для сетевых карт). Интерфейс сетевых адаптеров, разработанный фирмами 3COM и Microsoft.

Network File System (NFS, сетевая файловая система). Разработанный фирмой Sun Microsystems, этот набор протоколов позволяет сетевому администратору монтировать файловые системы из одного компьютера в точке монтирования на другом компьютере. В результате создается впечатление, что файлы, находящиеся на другом компьютере, являются частью локальной файловой системы. Также см. *Distributed File System*.

Network Information System (NIS, сетевая информационная система). Служба, разработанная Sun Microsystems, с помощью которой клиенты сети могут получать информацию от других компьютеров, используя единый сеанс регистрации. Для увеличения степени безопасности была разработана система NIS+. Код NIS был представлен компанией Sun на общедоступном домене, а также перенесен на многие другие вычислительные платформы.

Network interface card (NIC, сетевой интерфейсный адаптер). Сетевые аппаратные средства, применяемые для связывания компьютера или рабочей станции с сетевой средой.

Neutral disparity (нейтральное несоответствие). См. *Disparity*.

NEXT. См. *Near-end cross-talk*.

NFS. См. *Network File System*.

NIC. См. *Network interface card*.

NIS. См. *Network Information System*.

NL_Port. Порт, который подключает устройство к петле с арбитражной логикой (Arbitrated Loop).

Node (узел). Аппаратный компонент любого типа, подключенный к сети (например: компьютер, мост, сервер или маршрутизатор).

Novell Directory Services (NDS, службы каталогов Novell). Служба каталогов, которая обычно применяется в Novell NetWare. Служба NDS хранит учетные записи пользователей и ссылки на сетевые ресурсы наряду с другими данными. После появления версии NetWare 6.0 служба стала называться NDS и получила дополнительные функциональные свойства. В настоящее время она называется eDirectory.

Nslookup. Используйте эту команду совместно с параметрами «имя узла» или «IP-адрес» для получения информации у сервера DNS относительно узла, имеющегося в вашей сети.

NTFS. Файловая система, применяемая серверными операционными системами Microsoft, начиная с версии Windows NT. Эту файловую систему поддерживают многие современные клиентские операционные системы, например Windows XP. Система NTFS обеспечивает поддержку дисков большого объема, кодирования, расширенного набора разрешений безопасности, а также сжатие данных.

ODI. См. *Open Data-Link Interface*.

Open Data-Link Interface (ODI, открытый канальный интерфейс). Спецификация для сетевых адаптеров, разработанная компаниями Novell и Apple.

Open Shortest Path First (OSPF, открытый протокол SPF). Протокол маршрутизации, который использует объявление о состоянии канала (Link State Advertisements, LSA) для обмена информацией о маршрутах. По сравнению с RIP, протокол OSPF учитывает другие показатели затрат, например скорость передачи данных по маршруту, трафик маршрута, а также его надежность. Для OSPF отсутствуют ограничения в 15 переходов, присущие RIP, и он применяет маски подсети, чего RIP не делает.

Open Systems Interconnection (OSI, взаимодействие открытых систем). Набор протоколов, разработанный в 80-х годах прошлого века и предназначенный для использования компьютерами, которые относятся к различным аппаратным платформам, для обеспечения беспроблемного взаимодействия между ними. Также см. *OSI Reference Networking Model*.

OSI. См. *Open Systems Interconnection*.

OSI Reference Networking Model (модель взаимодействия открытых систем). Семиуровневая модель, разработанная ISO, которая предназначена для описания специфических функциональных модулей и интерфейсов, с которыми работают создаваемые сетевые протоколы. В настоящее время применяется для изучения концепций, связанных с сетями. Существуют и другие модели, например модель DOD (Department of Defense, Министерство обороны) или

модель DARPA, которая была разработана раньше и применяется для описания набора протоколов TCP/IP.

OSPF. См. *Open Shortest Path First*.

Packet filter (фильтр пакетов). Базовый брандмауэр, который фильтрует входящий и исходящий сетевой трафик на основе информации, содержащейся в IP-заголовке.

Patch panels (коммутационная панель). Этот модуль обеспечивает коммутацию электрических цепей, в результате чего облегчается процесс добавления, удаления и изменения рабочих станций. Коммутационные панели представляют собой наборы штырьков, вставляемых в отверстия, и обычно находятся в телекоммуникационных шкафах.

PCI. См. *Peripheral Component Interconnect*.

PCMCIA. Компактные платы расширения, применяемые в ноутбуках и других подобных компьютерах. Расшифровывается PCMCIA как Personal Computer Memory Card International Association (Международная ассоциация производителей плат памяти для персональных компьютеров IBM PC). Именно эта организация разработала данную спецификацию. Также см. *CardBus*.

Peripheral Component Interconnect (PCI, соединение периферийных компонентов). Стандартная шина, используемая в большинстве современных PC и мини-компьютеров. Шина PCI обеспечивает большую скорость передачи данных (с тактовой частотой 33 МГц) и разрядность данных (32 или 64 бита), чем более ранние шины, например ISA и EISA. Устройства, совместимые с PCI, обладают свойством управления шиной. Это означает, что плата контролирует шину и может передавать большие объемы данных непосредственно в системную память, не обращаясь к центральному процессору. Платы PCI обладают меньшим форм-фактором по сравнению со своими предшественниками, платами EISA.

Permissions (разрешения). Во многих компьютерных системах этот термин обозначает предоставление или запрещение доступа к системным ресурсам, например, к файлам или принтерам. Также см. *Share-level permissions* и *User-level permissions*.

Physical topology (физическая топология). Физическая структура сетевой среды (медные, волоконно-оптические кабели или беспроводное оборудование), а также устройства, которые подключаются к сети.

Ping. Утилита TCP/IP, использующая пакеты ICMP ECHO/REPLY для определения факта наличия соединения с тем или иным сетевым устройством. Другим распространенным инструментом, применяемым для поиска и устранения проблем, является утилита TRACEROUTE/TRACERT (в зависимости от вашей операционной системы).

Plain old telephone service (POTS, обычная телефонная сеть). Этот термин обозначает услуги, предоставляемые традиционной аналоговой телефонной сетью.

Point Coordination Function (PCF, функция точечных координат). Метод, применяемый беспроводными клиентами для получения доступа к полосе пропускания сети путем обмена фреймами (RTS/CTS) с точками доступа.

Point-to-Point Protocol (PPP, протокол «точка-точка»). С помощью этого протокола две конечные точки соединения могут устанавливать между собой коммуникационный канал. Протокол PPP обычно используется провайдером услуг Интернета для обеспечения подключения удаленного пользователя или поддержки доступа к Интернету для удаленного клиента.

Point-to-Point Tunneling Protocol (PPTP, протокол туннелирования «точка-точка»). Подобно VPN, в данном случае образуется защищенный «туннель» через Интернет. Компании, имеющие удаленные филиалы, могут воспользоваться PPTP для безопасной передачи данных.

POP3. См. *Post Office Protocol Version 3*.

Positive disparity (положительное несоответствие). См. *Disparity*.

Post Office Protocol Version 3 (протокол электронной почты версии 3). Протокол, который в настоящее время используется многими провайдерами услуг Интернета для передачи сообщений электронной почты с их серверов клиентам. В отличие от протокола IMAP, который позволяет оставлять сообщения на сервере до тех пор, пока пользователь не удалит их, POP3 загружает все сообщения на компьютеры пользователей, после чего они становятся недоступными на сервере POP3.

POTS. См. *Plain old telephone service*.

Power distribution units (распределительные щиты электропитания). Применяются для стабилизации входящего электропитания, подаваемого мини-компьютерам и мэйнфреймам. Обычно устанавливаются два или больше щитов, чтобы в случае выхода из строя одного из них остальные продолжали бы подавать стабильное напряжение на компьютер. Эти устройства применяются для резервирования электроснабжения высокоуровневых серверов, которые подключены к отдельной линии электроснабжения. Благодаря этому выход из строя одного источника электропитания не приводит к отключению сервера, поскольку альтернативные источники продолжают подавать напряжение на другие распределительные щиты.

PPP. См. *Point-to-Point Protocol.*

PPPoE. См. *The Point-to-Point Protocol over Ethernet*.

PPTP. См. *Point-to-Point Tunneling Protocol.*

Pretty Good Privacy (PGP, высокая конфиденциальность). Набор утилит шифрования с открытым ключом, разработанных Филиппом Циммерманом (Philip Zimmerman). Технология PGP широко распространена в Интернете, хотя изначально правительство США ограничивало ее экспорт. Доступны коммерческая и свободно распространяемая версии. Свободно распространяемая версия доступна на веб-сайте, расположенном по адресу http://web.mit.edu/network/pgp.html.

Существует и другой веб-сайт, предназначенный для распространения PGP за пределами США. Его адрес — www.pgpi.org/.

Protocol (протокол). Согласованный набор методов, предназначенных для осуществления коммуникаций между двумя или большим количеством узлов в сети, а также для обмена данными или сообщениями. Во многих случаях, например, в технологии шифрования, протоколы устанавливают согласование на уровне, который понимается обеими сторонами соединения. Наиболее известными и широко используемыми протоколами наших дней являются TCP и IP.

Proxy server (прокси-сервер). Разновидность брандмауэра, устанавливаемого между сетями. Прокси-сервер заменяет IP-адрес клиента своим собственным, а потом отсылает пакет. После получения отклика прокси-сервер заменяет IP-адрес адресом клиента, отсылая пакет по назначению.

PSTN. См. *Public switched telephone network*.

Public key encryption (шифрование с открытым ключом). Метод шифрования, предусматривающий использование открытого и закрытого ключа. Сообщение шифруется с помощью открытого ключа, а дешифруется — посредством закрытого ключа. При этом открытый ключ публикуется в Интернете. Для шифрования и отсылки сообщения владельцу закрытого ключа отправитель нуждается только в открытом ключе. Получатель сообщения может воспользоваться закрытым ключом для его дешифрования. Комбинация ключей является результатом математического вычисления, причем только владелец закрытого ключа может расшифровать сообщение, зашифрованное открытым ключом, доступным каждому пользователю. Сравните с использованием единственного ключа шифрования, который знают отправитель и получатель. Использование шифрования с открытым ключом означает, что оба участника процесса обмена данными не могут использовать другие средства для обмена одним ключом шифрования. Обратите внимание на то, что протокол Secure Sockets Layer (SSL) предусматривает использование открытого ключа шифрования для начала обмена одним ключом шифрования, используемым на остальных этапах процесса коммуникации.

Public switched telephone network (PSTN, коммутируемая сеть общего пользования). Современная телефонная сеть, которая состоит из миллионов устройств, объединяющих многие малые телефонные сети, причем в основном она включает цифровые линии, соединяющие ваш дом или офис с магистральными линиями. В противоположность сети POTS (обычная телефонная сеть), посредством которой была возможной только передача речи, в данном случае пользователь получает дополнительные телекоммуникационные услуги. В некоторых случаях названия этих сетей взаимозаменяемы, хотя это и неверно.

R-utilities (R-утилиты). Набор утилит, разработанных и распространяемых Калифорнийским университетом в Беркли. С их помощью упрощается выполнение многих задач, обычно связываемых с другими утилитами TCP/IP. В настоящее время во многих областях эти утилиты заменены утилитами

SSH, которые обеспечивают те же возможности, но включают механизм обеспечения безопасности, благодаря которому они являются менее уязвимыми, чем традиционные R-утилиты.

RAID. Изначально эта аббревиатура расшифровывалась в виде «Redundant Array of Inexpensive Disks» (избыточный массив недорогих дисков), а в настоящее время она расшифровывается как «Redundant Array of Independent Disks» (избыточный массив независимых дисков). Это связано с тем, что используемые диски вовсе не так дешевы, как это было раньше. Технологии RAID широко распространены в настоящее время. Различные уровни RAID могут обеспечивать высокоскоростной доступ (полосовые наборы) или избыточность (зеркальные наборы или полосовые наборы с проверкой четности). Результатом дальнейшего развития этой концепции явилось объединение полосовых и зеркальных наборов, воплотившее в себе лучшие качества «предшественников». В случае выхода из строя одного диска из этого набора, другие берут на себя выполнение его функций до тех пор, пока поврежденный диск не будет заменен. В случае использования полосовых наборов производительность снижается, поскольку должна быть вычислена полоса четности (проходящая через весь полосовой набор) при каждом факте получения доступа клиента к данным.

Repeater (повторитель). Повторитель объединяет физические сетевые сегменты, а также усиливает полученный с одного порта сигнал перед его передачей другим портам. Поскольку повторитель не проверяет содержимое полученных (ретранслируемых) данных, могут повторяться поврежденные фреймы (из-за шума и некоторых других факторов). Повторитель, объединяющий более двух сетевых сегментов, обычно называется многопортовым повторителем. Усовершенствованные концентраторы заменили многопортовые повторители во многих областях, поскольку могут выполнять аналогичные функции, обладая при этом дополнительными возможностями.

RFI. См. *Electromagnetic interference (EMI).*

Rights (права доступа). В большинстве компьютерных операционных систем этот термин применяется для определения действий, выполняемых пользователем компьютера.

Ring topology (кольцевая топология). Физическая топология, которая предусматривает наличие «соседей» у каждого сетевого узла. Таким образом, каждый узел в сети соединяется с другим узлом, а последний узел в кольце обычно подключается к первому узлу. На практике это достигается путем подключения кабелей к соседним узлам или с помощью кабельного концентратора (например, MAU или MSAU, используемых в сетях Token-Ring), осуществляющего внутренние топологические соединения в кольце. Все коммуникации в кольце проходят через каждый другой узел до тех пор, пока не будет достигнут целевой узел.

RIP. См. *Routing Information Protocol.*

RMON. См. *Simple Network Management Protocol.*

Router (маршрутизатор). Устройство, работающее на уровне 3 модели OSI (сетевой уровень). На сетевом уровне поддерживается логическое пространство адресов, с помощью которого облегчается организация сетей и маршрутизация трафика между ними. Благодаря этому можно отказаться от последовательного пространства адресов, поддерживаемого устройствами низкого уровня, которые используют адреса контроля доступа к среде (MAC, Media Access Control). Каждый маршрутизатор содержит как минимум два сетевых интерфейса. Один (или несколько) из этих интерфейсов может использоваться для подключения маршрутизатора к глобальной сети, а другие интерфейсы — для подключения к локальным сетевым сегментам. Маршрутизаторы принимают входные данные от одного сетевого интерфейса, затем принимают решения о маршрутизации, основываясь на выборе интерфейса, который наилучшим образом доставит пакет по месту назначения. Маршрутизаторы также обеспечивают конфигурирование фильтрации пакетов (применяется брандмауэрами).

Routing Information Protocol (RIP, протокол маршрутной информации). Используемый маршрутизаторами протокол, с помощью которого принимаются решения о том, какой порт используется для отсылки сетевого пакета по назначению. Протокол RIP выполняет дистанционно-векторную маршрутизацию. Он принимает решение о выборе наилучшего маршрута для достижения цели на основе маршрутизации из соответствующей таблицы, которая содержит сведения относительно места назначения, то есть о расстоянии (в ретрансляциях) и векторе (направлении). Маршрутизаторы RIP также обмениваются между собой данными для обновления таблиц маршрутизации.

SAMBA. Реализация протокола блока серверных сообщений (SMB, Server Message Block) в виде открытого исходного кода, который был обновлен для включения общей файловой системы Интернета (CIFS, Common Internet File System), которая является предшественницей SMB. Протокол SAMBA относится к категории свободно распространяемых программ, существуют его реализации для многих операционных систем, в связи с чем облегчаются коммуникации с операционной системой Windows.

SANs. См. *Storage Area Networks*.

Sequenced Packet Exchange (SPX, последовательный обмен пакетами). Протокол NetWare, который обеспечивает доставку в требуемом порядке пакетов, отосланных при помощи протокола IPX.

Serial Line Internet Protocol (SLIP, межсетевой протокол для последовательного канала). Устаревший метод, применяемый для установки соединения между двумя устройствами (обычно между двумя компьютерами). В настоящее время вместо протокола SLIP используется протокол типа «точка-точка» (PPP, Point-to-Point Protocol).

Server (сервер). Компьютер, который выделяет вычислительные ресурсы другим компьютерам, которые в этом случае называются клиентами. Например, сер-

вер может обеспечивать для клиентов совместный доступ к файлам или принтерам.

Server Message Block (SMB, блок серверных сообщений). Протокол, разработанный фирмой IBM и адаптированный Microsoft для обмена сообщениями и поддержки доступа к ресурсам в соответствии с технологией «клиент-сервер». Протокол SMB в настоящее время продолжает использоваться некоторыми приложениями и операционными системами Windows. Система SMB была адаптирована другими операционными системами для поддержки совместимости с операционными системами Microsoft. Протокол SMB был расширен, а затем переименован в общую файловую систему Интернета. Версией этого протокола с открытым кодом является SAMBA.

Shadow Password File (теневой файл паролей). Применяется в операционных системах UNIX/Linux для поддержки файла паролей (в котором хранятся сведения о пользовательской учетной записи). Этот файл защищен, поэтому только учетная запись root (или приложение, которое выполняется под управлением root, например, процесс регистрации) может получать доступ к этому файлу. Благодаря этому файлу становится невозможным получение хакером информации из файла /etc/passwd/, а также применение инструментальных средств для декодирования паролей учетных записей. Во многих системах UNIX/Linux этот файл называется /etc/shadow.

Share-level permissions (разрешения на уровне общего доступа). Разрешения, которые предоставляют доступ ко всем файлам/подкаталогам, где находятся общие сетевые файлы. Обратите внимание, что во многих системах возможна дальнейшая защита выбранных файлов или подкаталогов с помощью разрешений на уровне пользователей. Например, можно применить разрешения на уровне ресурсов по отношению к разделу NTFS на сервере Windows, но ограничить доступ к выбранным файлам и каталогам путем применения разрешений на уровне пользователей.

Simple Mail Transfer Protocol (SMTP, простой протокол передачи почты). Современный метод, применяемый для обмена сообщениями между серверами электронной почты. После завершения передачи данных пользователи могут обратиться к протоколам IMAP или POP3 для просмотра и управления почтовыми сообщениями.

Simple Network Management Protocol (SNMP, простой протокол сетевого управления). Расширенный протокол, применяемый для отслеживания многих сетевых устройств. (Расширением SNMP является протокол RMON (Remote Monitoring Protocol, протокол удаленного мониторинга).)

Single key encryption (шифрование с единственным ключом). Технология шифрования, использующая единственный закрытый ключ для шифрования и дешифрования информации. Эта методика предусматривает обязательное применение механизма, который позволяет получить единственный закрытый ключ сторонами, участвующими в передаче информации.

Single-mode fiber-optic cabling (одномодовые волоконно-оптические кабели). Волоконно-оптический кабель, в котором применяется монохромный луч света

(световая волна фиксированной длины), излучаемый лазером или светодиодом. Благодаря этому отсутствует явление интерференции, наблюдаемое в случае световых волн разной длины, поэтому одномодовые волоконно-оптические кабели обеспечивают передачу сигнала на большие расстояния, чем многомодовые волоконно-оптические кабели. Стеклянный или пластиковый сердечник, используемый в одномодовых кабелях, имеет меньший диаметр, чем его аналог в многомодовых кабелях, обеспечивая передачу данных на большие расстояния.

SLIP. См. *Serial Line Internet Protocol*.

Small Computer Systems Interface (SCSI, интерфейс малых компьютерных систем). Параллельная архитектура, обеспечивающая подключение дисковых и ленточных устройств к серверу или высокоуровневой рабочей станции. Также см. *Storage Area Networks* и *Network Attached Storage*, где применяется последовательное подключение хранилищ данных.

Small office/home office (SOHO, малый офис/домашний офис). Небольшая сеть, которая обычно охватывает один офис или небольшую домашнюю/офисную сеть. В локальной сети SOHO конфигурируется лишь небольшое количество компьютеров, применяются простые маршрутизаторы/коммутаторы наряду с программными маршрутизаторами, блокирующими внешнюю атаку. Также доступны недорогие брандмауэры, которые требуют выполнения небольшого объема управленческих задач.

SMB. См. *Server Message Block*.

SMTP. См. *Simple Mail Transfer Protocol*.

SNIA. См. *Storage Networking Industry Association*.

SNMP. См. *Simple Network Management Protocol*.

Social engineering (социотехника). Простой метод, применяемый для получения относящейся к сети информации (пользовательские учетные записи и пароли). Обычный используемый в этом случае прием заключается в том, что некто звонит пользователю, представляясь сотрудником службы технической поддержки, и просит его сообщить пароль, который якобы необходим для выполнения технического обслуживания. Защита от подобного вида вторжения должна быть определена в политике по обеспечению безопасности.

SOHO. См. *Small office/home office*.

Spread Spectrum (расширенный спектр). Методика передачи данных по беспроводным сетям, которая предусматривает комбинирование псевдошумового сигнала и фактической информации модуляции в виде несущей радиочастоты. Благодаря интерференции двух различных сигналов генерируется один сигнал, в котором передаваемые данные маскируются случайным сигналом. Обратите внимание на то, что вследствие одновременной передачи фактических данных и кажущегося случайным шума используется большая полоса частот, чем в случае передачи единственного сигнала, включающего данные.

Получатель этого сигнала просто маскирует псевдошумовой сигнал для восстановления фактических данных.

SPX. См. *Sequenced Packet Exchange*.

SSH (Secure Shell, безопасная оболочка). Эта технология также известна под названием Secure Socket Shell (оболочка безопасных сокетов). Этот протокол поддерживает более безопасную среду, чем традиционные R-утилиты. В настоящее время к SSH-утилитам относятся slogin, ssh и scp. Обеспечение безопасности передаваемых данных обеспечивается путем поддержания механизма безопасной регистрации, а также с помощью шифрования данных. Последняя версия этих утилит, SSH2, определена группой IETF.

Star topology (звездообразная топология). Сетевая топология, предусматривающая использование центрального кабельного концентратора. Каждый сетевой компьютер подключается к единственному концентратору (или коммутатору). Именно кабельный концентратор обеспечивает обмен данными между устройствами в локальной сети (или в городской/глобальной сети). Примером реализации подобной топологии служит 100BASE-T Ethernet, использующая коммутатор.

Stateful Inspection (проверка состояния). Методика, используемая брандмауэрами для отслеживания исходящих запросов и их сравнения с входящими откликами. Благодаря этому механизму блокируется проникновение в вашу сеть нежелательного трафика.

Storage Area Networks (SANs) (архитектура «сервер — хранилище данных»). Сеть, используемая серверами для получения доступа к хранилищу данных большой емкости на высокой скорости. Сети SAN поддерживают выполнение множества функций. В сети SAN может находиться много дисковых/ленточных устройств, которые подключаются к серверу с помощью SCSI или других протоколов. Помимо этого, доступ к хранилищу данных в SAN может обеспечиваться с нескольких серверов. В этом плане NAS отличается от SAN, поскольку она должна дополняться другими сетевыми клиентами и серверами, находящимися в производственной локальной сети.

Storage Networking Industry Association (SNIA, ассоциация производителей сетевых устройств хранения данных). Промышленная ассоциация, в задачи которой входит разработка устройств хранения данных, например NAS и SAN.

Store-and-forward switch (коммутатор с буферизацией данных). Коммутатор, который буферизует фреймы в памяти перед тем, как отослать их соответствующему порту. Этот коммутатор может объединять две различные сети (в плане применяемой топологии), например 10 Мбит/с и 100 Мбит/с, причем в этом случае не нужно беспокоиться по поводу различных скоростей передачи данных. Коммутаторы этого типа могут проверять целостность фреймов, блокируя поврежденные фреймы и не допуская их распространения в других сетевых сегментах. Также см. *Cut-through switch*.

Subnet (подсеть). Подмножество класса IP-адресов. Например, можно разделить IP-адреса класса C на несколько подсетей путем выделения битов из узлового раздела IP-адреса. В результате становится возможным формирование в сети двух или большего количества подсетей. Для этих целей применяется *маска подсети*.

Subnet mask (маска подсети). 32-разрядный фрагмент, который используется для описания раздела IP-адреса, используемой для идентификации сетевой и узловой части IP-адреса (ваш компьютер или другое сетевое устройство).

Switch (коммутатор). Устройство, которое напоминает концентратор тем, что функционирует подобно кабельному концентратору. Однако вместо широковещательного распространения всех входящих данных в направлении всех остальных портов, коммутатор устанавливает соединение между данными, поступающими на входящий порт, и портом, куда должны доставляться эти данные. В современных сетях коммутаторы полностью вытеснили концентраторы.

SYN flooding (атака с применением бита SYN). Применяемая в прошлом форма атаки по отношению к серверу. Эта атака связана с трехсторонним квитированием, используемым TCP/IP для установки связи. Бит SYN, входящий в состав TCP-пакета, приводит к тому, что сервер выделяет ресурсы памяти для подключения. Отсылая большое количество SYN-пакетов и не отвечая на запросы сервера, можно легко вызвать переполнение памяти сервера, что приведет к его блокированию. Многие современные операционные системы способны блокировать подобные атаки.

Syslog. Демон UNIX/Linux, который регистрирует важные события в форме, выбираемой администратором. Благодаря Syslog поддерживается контрольный журнал, являющийся частью этих операционных систем.

T-carrier (T-носитель). Этот термин применяется для описания цифровых служб, которые ранжируются от линий T1 (1,544 Мбит/с) до линий T4 (274,186 Мбит/с). Линия T1 поддерживает 24 независимых канала связи, которые могут применяться для передачи речи и данных по паре проводов. Каждый из 24 каналов может передавать данные со скоростью 64 Кбит/с. В Европе эта услуга известна как E-носитель. Но в этом случае поддерживается иное количество каналов. Например, линия El поддерживает 30 каналов.

TCP. См. *Transmission Control Protocol.*

Tcpdump. Утилита от независимого производителя, применяемая в операционных системах UNIX/Linux для перехвата и просмотра пакетов TCP/IP, а также статистики. Эта популярная утилита включена в состав многих операционных систем семейства UNIX/Linux. Аналогичная версия для клиентов Windows называется windump.

TDR. См. *Time domain reflectometry.*

Telecommunications closet (телекоммуникационный шкаф). Центральное место, объединяющее все кабели, проложенные на данном этаже. В телекоммуникационном шкафу могут устанавливаться сетевые устройства и концентраторы, а также телефонное оборудование.

Telnet. Протокол/утилита, используемые для установки удаленных терминальных сеансов.

TFTP. См. *Trivial File Transfer Protocol.*

Thicknet («толстая» сеть). Этот термин обычно применяется для обозначения коаксиальных кабелей 10BASE-5, которые использовались в первых сетях Ethernet.

Thinnet. («тонкая» сеть). Коаксиальный кабель (10BASE-2), диаметр которого меньше, чем у коаксиального кабеля 10BASE-5.

Time domain reflectometry (TDR, рефлектометрия временных интервалов). Метод, применяемый для измерения длины кабеля или нахождения мест обрывов путем измерения периода времени, прошедшего между отсылкой тестового импульса и его отражения из-за неоднородности в кабеле. Инструменты, обеспечивающие измерение в соответствии с методом TDR, позволяют примерно определить место обрыва кабеля.

Time to Live (TTL, время существования). Концепция, используемая многими протоколами. Как правило, это значение указывает на количество секунд или переходов, в течение которых сетевой пакет передается по сети, а затем самоликвидируется. Благодаря этому предотвращается бесконечная передача пакета в случае некорректно настроенной топологии маршрутизации.

Token-Bus (эстафетная магистраль). Напоминает Token-Ring, за исключением того, что все рабочие станции подключены к шине, которая может прослушивать все выполняемые передачи данных. Адресация в сетях Token-Bus подобна адресации, принятой в кольцевой топологии, когда между узлами упорядоченным образом передаются фреймы маркера или данных.

Token-Ring (эстафетное кольцо). Сетевая технология, в которой между узлами сети упорядоченным образом передается фрейм маркера. Как только узел в локальной сети испытывает потребность в передаче данных, он ожидает момента получения фрейма маркера, а затем создает фрейм, содержащий передаваемые данные, наряду с информацией относительно адресов компьютера-отправителя и компьютера-получателя. Затем фрейм данных циркулирует по кольцу до тех пор, пока не достигнет получателя. При этом проверяется флаг во фрейме для определения того, смог ли принимающий узел перехватить данные для завершения передачи. В целях разработки стандартов для сетей Token-Ring была сформирована рабочая группа IEEE 802.5. В настоящее время подобные сети практически не применяются.

Traceroute. Утилита TCP/IP, которая использует пакеты ICMP ECHO/REPLY для обнаружения маршрутизаторов (или шлюзов) на пути к устройству-получателю. Эта утилита выполняет приращение значения TTL начиная с единицы, добавляя каждый раз 1 в случае обнаружения очередного устройства. Эта утилита может рассматриваться в качестве усовершенствованного варианта утилиты Ping. В некоторых операционных системах утилита Traceroute называется tracert.

Tracert. Команда Tracert используется в Windows, а также в некоторых других операционных системах, от MS-DOS 6.2 до Windows 2000 и Windows XP. В новейших версиях операционных систем Microsoft используется команда Traceroute.

Transmission character (символ передачи). В контексте Fibre Channel 10-битовый символ, выбранный для передачи данных в целях поддержки нейтрального несоответствия. Для поддержки последнего выполняется кодирование восьмибитовых значений с генерированием одного-двух возможных символов передачи.

Transmission Control Protocol (TCP, протокол управления передачей). Ориентированный на установку соединений надежный протокол, который использует протокол Интернета (IP) для передачи данных в сети. Протокол TCP устанавливает сеансы связи с удаленным узлом, а также использует различные методики, например, подтверждения для гарантии надежной передачи данных между двумя конечными точками канала связи.

Trivial File Transfer Protocol (TFTP, простейший протокол передачи файлов). Упрощенная версия протокола FTP, используемая для выгрузки файлов на маршрутизатор, а также другое подобное оборудование. Здесь не используются какие-либо механизмы аутентификации или коррекции ошибок. Протокол TFTP не может использоваться в производственных сетях.

Trojan horse (Троянский конь). Программа, напоминающая компьютерный вирус. В отличие от последнего, файл троянского коня хранится на инфицированном компьютере до того момента, когда какое-либо событие приведет его в действие. В качестве подобного события может быть определенная дата либо внешний сигнал, отосланный с другого компьютера. Например, программа троянского коня может заражать тысячи компьютеров, не защищенных брандмауэрами или антивирусными программами. После получения определенного сигнала каждая копия этой программы активизируется и начинается распределенная атака отказа в обслуживании другого компьютера. Многие программы троянских коней могут маскироваться, выдавая себя за файлы операционной системы инфицированного компьютера.

TTL. См. *Time to Live*.

Twisted-pair cables (кабели витой пары). Также известны как неэкранированные кабели витой пары, поскольку в этом случае не требуется экран. Благодаря наличию витков для отдельных пар жил кабеля происходит балансировка электромагнитных полей, что позволяет исключить электромагнитные наводки в кабеле.

UDP. См. *User Datagram Protocol*.

UID. Идентификатор, используемый операционными системами UNIX/Linux для идентификации пользователя при выполнении процессов или оценивании доступа к файлам и другим системным ресурсам. Нулевое значение этого поля — признак суперпользователя, или пользователя с привилегиями пользователя root. В некоторых системах значения от 1 до 99 зарезервированы для системных процессов, например для демонов, выполняемых в фоновом режиме.

Unicode. Метод кодирования, применяемый для присвоения числовых значений алфавитным, символьным и числовым символам. По сравнению с ASCII, стандартом, применяющимся с давних времен, Unicode поддерживает множество языков и включает до 34 168 символов. Также см. *American Standard Code for Information Interchange* и *Extended Binary-Coded Decimal Interchange Code*.

Uninterruptible power supply (UPS, источник бесперебойного питания). Источник электропитания, оборудованный аккумуляторами и поддерживающий энергоснабжение устройств в случае отказа основного питающего напряжения. Для поддержки корпоративных серверов ИБП объединяются с дизель-генераторами, что позволяет существенно увеличить надежность автономного электроснабжения. Если же мощность ИБП невелика, аккумулятор может быстро разрядиться. Во избежание этого осуществляется коммуникация ИБП с сервером, поэтому в случае перебоев с электроснабжением выполняется автоматическое отключение последнего в штатном режиме, что позволяет избежать потерь данных.

Universal serial bus (USB, универсальная последовательная шина). Высокоскоростная шина, которая позволяет подключить большое количество периферийных устройств к компьютеру. Начальная спецификация поддерживает скорость передачи данных до 12 Мбит/с (спецификация USB 2.0).

Uplink port (восходящий порт). Порт концентратора, коммутатора, маршрутизатора или другого сетевого устройства, который используется для подключения к другому подобному устройству в целях увеличения плотности портов для локальной сети.

UPS. См. *Uninterruptible power supply*.

USB. См. *Universal serial bus*.

User Datagram Protocol (UDP, протокол пользовательских дейтаграмм). Ненадежный протокол без установки соединений, который использует IP-протокол для отсылки сетевых сообщений. В отличие от него, протокол TCP также использует IP-протокол, но является ориентированным на соединения надежным протоколом.

User-level permissions (разрешения на уровне пользователей). Разрешения для файлов и каталогов, которые позволяют разрешить/запретить доступ отдельным пользователям к сетевым ресурсам. Также см. *Разрешения на уровне совместно используемых ресурсов*.

Virtual LAN (VLAN, виртуальная локальная сеть). Метод, предусматривающий использование сетевых коммутаторов для подключения нескольких устройств к одному или большему количеству коммутаторов. Виртуальная локальная сеть позволяет сетевому администратору выбирать локальную сеть, к которой относится компьютер или другое устройство. Поскольку коммутатор является разновидностью кабельного концентратора, «виртуальность» заключается в том, что невозможно использовать отдельные коммутаторы для каждого сетевого сегмента. Вместо этого можно подключать несколько клиентов к одному и тому же коммутатору, а затем использовать специальную программу для определения виртуальной сети, к которой относится компьютер или другое устройство.

Virtual Private Network (VPN, виртуальная частная сеть). Защищенный путь через общедоступную сеть или глобальную сеть, который объединяет два компьютера или две сети таким образом, что, с точки зрения каждой конечной точки соединения, они находятся в одной и той же сети. Это соединение является частным, поскольку полезные данные, передаваемые через виртуальный туннель, являются защищенными. Для создания сетей VPN используются различные протоколы, поэтому ознакомьтесь с документацией, которая поставляется вместе с операционной системой, либо с VPN-решением от независимого производителя для оценки степени безопасности, обеспечиваемой в данном случае.

Virus (вирус). Подобно вирусу, который поражает человеческий организм (или любую другую живую форму), компьютерный вирус маскируется под полезную программу, нарушает нормальную деятельность компьютера, самостоятельно копируется и инфицирует другие компьютеры. Почтовые вирусы весьма распространены, а защита от них обеспечивается с помощью хорошей антивирусной программы, для которой доступно свойство автоматического обновления, позволяющее загружать из Интернета описания новых вирусов.

VLAN. См. *Virtual LAN*.

VPN. См. *Virtual Private Network*.

W3C. См. *World Wide Web Consortium*.

Wake On LAN (WOL). «Пробуждение» сетевого адаптера после получения соответствующего сигнала.

WAN. См. *Wide area network*.

WEP. См. *Wired Equivalent Privacy*.

Wi-Fi. Альянс, обеспечивающий решение проблем совместимости беспроводных сетей Ethernet (WECA, Wireless Ethernet Compatibility Alliance), был сформирован в целях поддержки продуктов от различных производителей, которые прошли строгие тесты для проверки «гладкого» взаимодействия.

Wi-Fi 5. Термин, применяемый для описания сетевой технологии IEEE 802.11a. Также см. Wi-Fi (термины беспроводных сетей 802.11b).

Wide area network (WAN, глобальная сеть). Сетевая технология, которая объединяет локальные и городские сети на больших расстояниях. В глобальных сетях могут использоваться различные протоколы, например, ATM и Frame Relay.

Windows Internet Naming Service (WINS, служба имен Интернета для Windows). Служба преобразования имен, используемая операционными системами Microsoft для трансляции имен NetBIOS в IP-адреса. Служба WINS актуальна и в настоящее время, поскольку до сих пор используются применяющие ее приложения. Обратите внимание на то, что сервер системы имен доменов

(Domain Name System, DNS) используется большинством операционных систем Windows (и некоторыми другими) для трансляции DNS-имен в IP-адреса. Сервер DNS от Microsoft может конфигурироваться для запроса сервера WINS в случае невозможности разрешения имени.

Winipcfg. Эта команда может использоваться устаревшими операционными системами Windows (например, Windows 95/98) для просмотра параметров IP-протокола, а также других конфигурационных настроек. Напоминает команду ipconfig, применяемую в более современных версиях операционных систем Windows.

WINS. См. *Windows Internet Naming Service*.

Wired Equivalent Privacy (WEP, уровень безопасности, эквивалентный кабельным сетям). Используется ранними реализациями сетей Wi-Fi. Протокол WEP обеспечивает весьма слабые возможности по шифрованию, эквивалентные степени безопасности, достигаемой в обычной кабельной сети. Имейте в виду, что защита кабельных сетей обеспечивается путем внедрения ряда защитных мероприятий на физическом уровне. В настоящее время технология WEP используется только в тех беспроводных сетях, где безопасность не имеет особого значения.

Wired Protected Access (WPA, защищенный кабельный доступ). Спецификация IEEE 802.111, разработанная для усовершенствования протокола Wired Equivalent Privacy (WEP), применявшегося ранее. Протокол WPA использует методики аутентификации, а также постоянно изменяющиеся ключи шифрования, в результате чего обеспечивается более безопасная беспроводная среда.

Wireless Access Point (AC, точка доступа). Беспроводное сетевое устройство, которое может использоваться в качестве «центрального пульта управления» для беспроводных клиентов, ожидающих передачи данных в сети. Точка доступа может использоваться беспроводными клиентами в качестве автономного устройства либо подключаться к кабельной сети. В «равноправной» беспроводной сети точки доступа не применяются.

WLAN (беспроводная локальная сеть). Локальная сеть (обычно небольших размеров), которая включает беспроводные сетевые устройства и может входить в состав обычной локальной сети.

WOL. См. *Wake On LAN*.

Work Area (рабочая область). Место подключения сети к рабочему месту пользователя.

World Wide Web Consortium (W3C, консорциум World Wide Web). Промышленная группа, в задачи которой входит развитие Веб путем разработки стандартов и программ, которые могут использоваться в качестве справочной модели для организации взаимодействия между веб-продуктами.

Worm (червь). Эта вредоносная программа напоминает вирус в том, что инфицирует компьютер, а затем использует его ресурсы (например, адресную книгу) для копирования в других компьютерах. Современные черви могут оставаться резидентными в памяти, а также распространяются в Интернете с очень высокой скоростью.

WPA. См. *Wired Protected Access.*

XDSL. См. *Digital Subscriber Line.*

Алфавитный указатель

Сергеев Александр Петрович

Настройка сетей Microsoft дома и в офисе

Учебный курс

Главный редактор	*Е. Строганова*
Заведующий редакцией	*А. Кривцов*
Руководитель проекта	*И. Шапошников*
Литературный редактор	*И. Шапошников*
Художник	*Л. Адуевская*
Корректоры	*Н. Лукина, И. Смирнова*
Верстка	*Н. Баланина*

Лицензия ИД № 05784 от 07.09.01.

Подписано к печати 12.08.05. Формат 70×100/16. Усл. п. л. 28,38.
Тираж 3500. Заказ
ООО «Питер Принт», 194044, Санкт-Петербург, Б. Сампсониевский пр., д. 29а.
Налоговая льгота — общероссийский классификатор продукции
ОК 005-93, том 2; 95 3005 — 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., д. 15.