Криста Андерсон
с Марком Минаси

Локальные сети

ПОЛНОЕ РУКОВОДСТВО

Проектирование, создание и обслуживание сетей, удовлетворяющих вашим требованиям

Разнообразныесредства для любого, кто создаёт сеть или управляет сетями

Жизненно необходимая информация о сетях, включающая всестороннее рассмотрение плана восстановления

Это Ваш путь к успеху

NETWORK PRESS
SYBEX

Криста Андерсон
с Марком Минаси

ББК 32.973-01
А65 УДК
681.3.06

Локальные сети. Полное руководство.

Перевод с английского

Криста Андэрсон с Марком Минаси

Локальные сети. Полное руководство: Пер. - К.: ВЕК+, М.: ЭНТРОП, с англ.-СПб.: КОРОНА принт, 1999.— 624 с., ил.

ISBN 5-88547-067-7

Эта книга представляет практический, систематизированный взгляд на компоненты сети, их взаимодействие и роль в вашем бизнесе. Независимо от того, собираетесь ли вы строить свою сеть "с нуля" или хотите модернизировать уже созданную ранее, эта книга поможет вам выбрать технологию, которая сделает эту модернизацию наиболее эффективной. Если вы хотите создать сеть самостоятельно, книга ознакомит вас со всеми концепциями и методиками, необходимыми для того, чтобы сделать всю работу правильно с первого раза. Если сеть уже работает, то наша книга поможет вам решить задачи, стоящие как перед администраторами сетей, так и перед аналитиками, озабоченными проблемой повышения производительности сетей, оптимизацией ее характеристик и снижением трафика.

Скотту, который сочетает в себе любимую мной комбинацию сетевого пользователя и фанатика. Видишь, я, наконец, написала книгу, как ты и предлагал мне три года назад. Пообещав тебе, я стала к этому стремиться

Благодарности

Любая книга — итог усердной работы многих людей. Выражаю особую благодарность моим коллегам.

- Скотту Андерсену (Scott Anderson) за поздние обеды, поглаживание по плечу и периодические побеги от компьютера, чтобы поиграть в поселенцев и собрать граблями листья. Как всегда, его поддержка была бесценна — я не смогла бы работать без нее.
- Терезе Вэйджмен (Teresa Wagamon) за большую поддержку издалека (экстремальные условия стимулируют работу; спасибо за запросы), а также за множество предложений и консультаций.
- Марку Минаси (Mark Minasi) за то, что много лет назад вовлек меня в дело и особо — за предложение приступить к работе именно над этим проектом. Как и все остальное, над чем мне довелось с ним работать, работа над этой книгой была захватывающей и перспективной.
- Джиму Куперу (Jim Cooper), который снова показал себя лучшим в мире техническим редактором. Технический редактор — либо огромная помеха, либо огромная помощь. Джим был техническим редактором нескольких моих книг и всегда был помощником. Мне хотелось бы и впредь работать с ним.
- Всему редакционному и производственному персоналу издательства Sybex, который внес вклад в эту книгу: Рэкуэлу Бейкеру (Raquel Baker) управление сложным проектом, Валери Перри (Valerie Perry) за тщательное редактирование, Бонни Биллсу (Bonnie Bills) за помощь в разработке структуры книги, Бренде Фринк (Brenda Frink), которая помогала разрабатывать структуру книги в отсутствие Бонни, Ниле Николе (Nila Nichols) за квалифицированную и быструю разработку схемы проекта, а также Сьюзен Берг (Susan Berg) и Катарине Моррис (Catherine Morris) за безукоризненную корректуру.

Выражаю самые глубокие благодарности всем, кто делился со мной своими замыслами и предположениями. Я с большим удовольствием полагалась не только на собственный опыт, но и опыт моих коллег, чтобы сделать книгу полезной как можно большему числу читателей.

Содержание

Глава 4

УСТАНОВКА СЕТЕВЫХ ПЛАТ И КАБЕЛЕЙ

Глава 5

ДОПОЛНИТЕЛЬНОЕ СЕТЕВОЕ ОБОРУДОВАНИЕ

Глава 6

ОБЩИЕ СВЕДЕНИЯ О ГЛОБАЛЬНЫХ СЕТЯХ

ЧастьII. Детали головоломки

Глава 7

ПОСТРОЕНИЕ СЕРВЕРА

Глава 8

СЕРВЕРЫ И ДОПОЛНИТЕЛЬНОЕ ОБОРУДОВАНИЕ

Глава 11

ПРИЛОЖЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ И ИХ ЛИЦЕНЗИРОВАНИЕ

Глава 12

ТОНКАЯ КЛИЕНТНАЯ СЕТЬ

Глава 13

СОЗДАНИЕ КОРПОРАТИВНОЙ WEB-СЕТИ

Часть IV. Распределение ресурсов, защита и аварийное восстановление

Глава 14

ПРИНЦИПЫ УПРАВЛЕНИЯ СЕТЯМИ

Глава 15

ЗАЩИТА СЕТЕЙ

Глава 16

ВОССТАНОВЛЕНИЕ ПОСЛЕ АВАРИЙ

Приложения

ПРИЛОЖЕНИЕ А

РЕСУРСЫ INTERNET

ПРИЛОЖЕНИЕ В

СЕТЕВЫЕ ФОРМЫ

ПРИЛОЖЕНИЕ С

ОБРАЗЕЦ ПЛАНА ВОССТАНОВЛЕНИЯ СЕТИ

ПРИЛОЖЕНИЕ D

ОТВЕТЫ НА УПРАЖНЕНИЯ

СЛОВАРЬ ТЕРМИНОВ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Введение

Добро пожаловать в книгу "Локальные сети. Полное руководство". Цель книги - прорваться через жаргон, принятый в сетевых технологиях. Независимо от того, начинаете вы работать с локальными сетями или уже приобрели некоторый опыт, изучаете новые технологии либо просто освежаете старые познания, этот подход будет вам полезен.

Чего ожидать от этой книги?

Полки книжных магазинов переполнены книгами по сетям. Зачем же нужна эта? Главным образом потому, что она с самого начала создавалась как учебное пособие, адресованное сотням или даже тысячам людей таких же, как вы - людей, которые хотят углубить знания по сетям. После нескольких лет преподавания и живой "обратной связи" с посетителями курсов, безусловно, можно довести до совершенства, как содержание книги, так и подход к его изложению. За основу книги принят курс лекций, в который включены дополнительные сведения. Конечный результат предполагает систематический подход к изучению компонентов локальных сетей и их взаимодействия.

В книге последовательно рассмотрены этапы создания локальной сети, начиная от разработки структурной схемы и заканчивая конфигурированием средств управления ресурсами с установкой системы защиты, обеспечивающей целостность и безопасность сетевых данных. Однако этим ее содержание не исчерпывается: в ней изложена методика документирования и устранения неисправностей, которая позволит (или, по меньшей мере, поможет) вам устранять различные нарушения работоспособности. Далее кратко рассмотрены некоторые технологии, которые в настоящее время еще не получили широкого распространения, но пригодятся вам в недалеком будущем. Наконец, вы изучите приемы, которые помогут вам обойти или преодолеть затруднения, встречающиеся при установке и обслуживании локальных сетей.

В общем, прочитав эту книгу, вы познакомитесь как с теорией, так и с практикой работы с сетями, приобретете теоретические знания и научитесь применять их на практике. Закончив чтение, вы обнаружите, что процесс создания сети, удовлетворяющей большинству запросов ваших руководителей и пользователей, на самом деле не так уж и сложен.

Кому предназначена книга?

Эта книга написана как для тех, кто просто изучает локальные сети так и для тех, кто систематически их разрабатывает. В книге я не углублялась именно в эти вопросы (которые лично меня просто очаровывают). Основное внимание уделялось локальным сетям. Таким образом, вы изучите несколько сетевых протоколов. Эта информация будет полезна при выборе протокола для вашей сети. Однако я не описывала специально, например, структуру пакета DLC, если только это не касалось непосредственно того, что вы должны знать. Основной упор сделан на практические вопросы сетевых технологий.

Что вы найдете в книге?

Основной стимул при создании сети заключается в желании избавиться от забот, связанных с дискетами. Разумеется, сети создаются не только для этого, но сама идея сети подразумевает совместное использование информации и ресурсов. Сети предназначены для выполнения множества задач, том числе:

- организации совместного использования файлов для повышения целостности информации;
- организации совместного использования периферийных устройств, таких, например, как принтеры;
- обеспечения централизованного хранения данных с целью облегчения их защиты, управления ресурсами и архивирования.

Чтобы пояснить, каким образом все это достигается, книга разделена на четыре части, каждая из которых описывает отдельный аспект работы в сети.

В ч. I "Каналы - нервная система сети" я расскажу о теоретических и физических аспектах построения схем локальных сетей. В гл. 1 рассматриваются основные элементы сетей, включая типы плат, выбор кабелей и юн; описывается модель OSI, которая крайне важна для понимания сетевых протоколов. На этом фундаменте строится гл. 2. В ней описывается сетевая архитектура, т.е. физическая и логическая топология сети, с которыми вы, вероятно, уже встречались, и поясняется их смысл. В гл. 3 рассматриваются| сетевые протоколы, на которых базируется транспортная система II гл. 4 рассказано об установке плат и кабелей, которые вы должны выбирать опираясь на знания, полученные в предыдущих главах. Если же вы собираетесь создать многосегментную сеть, приступайте к гл. 5, чтобы ознакомиться с устройствами, необходимыми для этого: повторителями, коммутаторами, маршрутизаторами, мостами и прочим оборудованием. И, в завершение ч. I, в гл. 6 рассматриваются некоторые параметры совместимости, которые необходимо знать для выхода в глобальные сети и организации доступа.

Оставив в сторону собственно сетевые вопросы, в ч. II "Детали головоломки" рассматриваются отдельные части сети, которые, организуя связи, загружают ее каналы и ресурсы: серверы, клиентные машины и соответствующие периферийные устройства. Начав в гл. 7 с описания оборудования. Необходимого для поддержки сетевого сервера, в гл. 8 изложены специфические требования к этим серверам. Кроме того, вам необходимо еще к ним и подключиться, поэтому в гл. 9 описывается оборудование, необходимое для поддержки клиентных машин.

Итак, у вас есть каналы связи и оборудование. Что теперь делать с этой сетью? Часть III "Сетевые операционные системы и приложения LAN" начинается с обзора сетевых операционных систем как одноранговых, так и клиент/сервер. Но сети никому не нужны, пока в них не запущены приложения, поэтому в гл. 11 рассматриваются типы приложений, которые вам необходимо использовать в сети, а также ,то, о чем вам следует побеспокоиться с точки зрения лицензирования этих приложений. Эта часть завершается описанием основных сетевых проблем, число которых непрерывно возрастает, так что вы не сможете их обойти. Одно из решений этих проблем - создание тонких клиентных сетей (гл. 12) и Web-узлов (гл. 13).

Итак, сеть установлена и запущена, но как гарантировать ее успешную работу в дальнейшем? В части IV "Распределение ресурсов, защита и аварийное восстановление" рассматриваются средства, гарантирующие, что ваш напряженный труд не пропадет даром. В гл. 14 рассматриваются принципы администрирования сети: аудит, инструменты управления и методы устранения неполадок. Если вас интересует защита данных от несанкционированного доступа или повреждения, прочитайте гл. 15, где рассматривается защита сетей. Ну, а если сеть разрушится полностью, для восстановления после аварии обратитесь к гл. 16.

Вы подавлены обширностью тем? Чтобы ободрить вас, я включила в книгу несколько дополнительных разделов. В приложении A "Ресурсы Internet" содержится список материалов, доступных как из этой книги, так и на Web-узле www.sybex.com издательства Sybex. Чтобы найти Web-страницу этой книги, щелкните на каталоге, затем введите цифры 2258 в поле поиска и нажмите клавишу <Enter>. В приложение B "Сетевые формы" включено несколько форм, которые помогут вам задокументировать сеть и составить расписание для архивирования. В приложении C "Пример плана восстановления сети" приведены подробности, которые пригодятся вам при составлении собственного плана. Наконец, в приложение D "Ответы на упражнения" содержатся ответы на упражнения, находящиеся в конце каждой главы. Кроме того, в книгу включен список использованных в ней терминов. Читатели, знакомые с терми-

нологией, могут опустить его, новичкам же полезно заглядывать в него по ходу чтения. (Когда термин появляется в книге впервые, ему немедленно дается определение, однако если вы забудете термин или читаете книгу выборочно, то можете найти его значение в словаре.)

Особенности и соглашения

Эта книга содержит огромный объем информации, поэтому, кроме упомянутых приложений, в текст включены некоторые дополнительные элементы, которые помогут вам усвоить информацию и запомнить особо важные моменты.

Во-первых, обратите внимание на упражнения, которые расположены в конце глав. Они разработаны для того, чтобы помочь вам закрепить знания. Никто не собирается заставлять вас выполнять их: эта книга - не руководство желающим получить сертификат MCSE. Однако если вы сможете правильно ответить на вопросы в упражнениях, значит, вы вполне освоили прочитанный материал.

Во-вторых, обратите внимание, как выглядит текст. Когда какой-либо 1 мин встречается впервые, он выделяется курсивом и ему дается определение. Кроме того, чтобы привлечь ваше внимание к разнообразной I ной или (надеюсь) полезной информации, которая несколько отклоняется от основной темы, в текст включены Примечания (Notes), Советы (Tips) и Предупреждения (Warnings). Например:

Примечание

В примечаниях содержатся интересные сведения о работе сети или его отдельном компоненте или инструменте.

Совет

В советах приводится информация об использовании инструментов для улучшения работы или защиты вашей сети.

Предупреждение

Предупреждения привлекают ваше внимание к той информации, которая поможет избежать сбоев и возможной потери данных. Если что-либо является достаточно важным, чтобы поместить его в предупреждение, значит, это действительно весьма неприятная вещь.

И, наконец...

Пора закончить болтовню и приступить к делу, поэтому я закругляюсь. Хочу только добавить, что, когда пишешь книгу подобного рода, объем информации, который необходимо усвоить и включить в текст, обычно огромен. (Да, именно так - приступите к чтению и вы увидите сами, насколько я права.) Сделано все возможное, чтобы материал был изложен упорядоченно, связно и, по возможности, доступно. Однако, как вы понимаете или вскоре поймете, тема книги представляет собой невероятно динамичную область знаний и не всегда возможно обсудить все темы так подробно, как, возможно, вам того хотелось. Если у вас появятся вопросы и комментарии, пожалуйста, не стесняйтесь, и направляйте их мне электронной почтой по адресу: candersn@adelphia.net. Время от времени я путешествую, поэтому не беспокойтесь, если не получите ответ сразу. Обещаю: по возвращении в офис я пошлю ответ.

Итак, представление начинается...

Криста Андерсон (Christa Anderson).

Глава 1

Концепция организации сетей и сетевые компоненты

Без тщательного изучения этой главы сложно будет понять дальнейшее изложение. Предупреждаю: глава - не "одноразовая", описывающая мелочи, о которых можно почитать во время авиарейса. Здесь рассматриваются элементы сетевого канала связи, в том числе сетевые платы, кабели, соединители. Рассматриваются также принципы организации сетей (модель OSI). Однако сначала обсудим несколько общих вопросов.

Что такое локальная сеть?

Локальной сетью (LAN - local area network) называют группу связанных друг с другом компьютеров, расположенную в некоторой ограниченной области, например, здании. Размеры LAN могут значительно различаться. Локальная сеть может состоять из двух рабочих станций, работающих под управлением Windows 98, расположенных в одной комнате, либо из нескольких сотен рабочих станций, разбросанных по разным этажам административного здания. Особенность LAN в том, что в такой сети все компьютеры каким-либо образом сгруппированы, тем или иным методом соединены друг с другом, и находятся в одном здании. В большинстве LAN для соединения компьютеров могут использоваться кабели различного типа. Однако, как увидим далее в этой главе, в некоторых LAN применяют и беспроводные каналы.

Примечание

Если сеть выходит за пределы здания, то это уже не LAN, а глобальная сеть (WAN - wide-area network). WAN бывает различных типов. Если сеть достаточно велика, она называется просто WAN. Сеть меньшего размера может носить иное название. Например, WAN, охватывающая основные районы города, может называться MAN (metropolitan area network), а сеть, соединяющая университетские корпуса, может называться CAN (campus area network). Короче говоря, локальная сеть ограничена пределами здания, а глобальная - нет.

Такое определение локальной сети принято в учебной литературе. Однако на практике локальные сети чаще определяют по функциональным, а не по физическим характеристикам. В этом, более общем, смысле, локальные сети являются средством связи компьютеров, которое позволяет им получать доступ к оборудованию. Иными словами, с учетом ограничений системы защиты, компьютеры локальных сетей получают доступ к общему оборудованию (принтерам, сканерам, приводам компакт-дисков, жестким дискам, модемам и т.д.) так, будто оно установлено локально. Разумеется, доступ к оборудованию означает и доступ к данным, хранящимся на этом оборудовании.

Итак, все компьютеры локальной сети могут не только получать доступ к компонентам каких-либо других аппаратных средств (с учетом ограничений систем защиты, рассмотренных далее), но также использовать их так, как если бы они были доступны локально, что предполагает совместное использование данных пользователями компьютеров.

Первые офисные компьютеры - мэйнфреймы и терминалы - были связаны в сеть, однако первые персональные компьютеры (PCs) обычно устанавливались как отдельные устройства. Поэтому старейшая форма сети LAN получила в обиходе название SneakerNet

(игра слов: Sneaker по-английски "тапочки"): пользователь ПК копировал данные с компьютера на дискету, а затем переходил с ней к другому компьютеру, чтобы распечатать данные на принтере, подключенном к этому компьютеру, либо чтобы просто передать коллеге копию данных. Если объем передаваемых данных не слишком велик, это решение не такое уж и плохое (и в некоторых случаях работает великолепно). Однако в нем есть серьезные недостатки:

- высокий риск утраты данных при потере или случайном форматировании дискеты;
- трудность синхронизации различных версий документа, если над ним должны работать одновременно несколько лиц;
- на обычные дискеты помещается не более 1,44 Мбайт данных, а файлы могут иметь значительно большие размеры;
- как быть, если пользователи используют в своих компьютерах разные приложения? Второй пользователь может оказаться не в состоянии открыть данный файл;
- защита данных затруднена - дискету легко украсть;
- копирование файлов, перенос к другой машине, последующее копирование или печать данных отнимает немало времени.

Поэтому сеть SneakerNet годится только для простейших задач. Современные офисные средства должны предоставлять:

- простые методы совместного доступа, передачи и защиты данных;
- средства совместного использования приложений;
- способы взаимодействия пользователей сети друг с другом;
- методы совместного использования периферийных устройств.

Рассмотрим эти вопросы несколько подробнее.

Управление файлами

Совместное использование, передачу и защиту информации сетевых компьютеров обычно называют управлением файлами. Одной из основных целей локальной сети является предоставление области хранении данных в общее распоряжение, для того, чтобы множество пользователей смогли получить доступ к одним и тем же файлам. Персональный компьютер, обеспечивающий совместный доступ к файлам и каталогам, называют *файловым сервером*.

Совместное использование файлов гарантирует, что в работе находится единственная версия файла, и все пользователи работают с новейшими данными. Если вы не хотите, можете не предоставлять общий доступ к файлу, однако, если с ним должен работать кто-либо еще, вы можете передать файл этому лицу - просто перенести его со своего жесткого диска на диск этого пользователя либо переслать как сообщение электронной почты.

Совместное использование файла с помощью сети отнюдь не означает автоматический доступ к нему любого пользователя. В современных операционных системах вы можете ограничить доступ к общим файлам или каталогам. С этой целью используют либо систему паролей, либо учетные записи пользователя. Эти средства предусматривают весьма точную настройку, обеспечивая различные уровни доступа к файлам - от минимального, допускающего только чтение, до полного доступа. Таким образом, вы можете,

например, запретить другим пользователям просматривать вашу работу либо просто не позволять вносить в нее изменения, если это нежелательно.

Как защитить данные от повреждения? Ведь данные - самое ценное имущество вашей фирмы. Они намного ценнее, чем безобразные ящики, называемые компьютерами, которые стоят на столах, поскольку уже устарели со времени покупки и постоянно заменяются. А вот утрата или искажение данных может разорить фирму. Однако сети позволяют легко архивировать данные, причем сделать это намного проще, чем в отдельностоящих компьютерах. Вы можете либо сохранять данные на единственном сервере и регулярно архивировать все его содержимое, либо установить в сети централизованную систему архивирования, с помощью которой каждый пользователь обязан будет скопировать все важные файлы с жесткого диска своего компьютера. При надлежащем управлении локальные сети обеспечивают уровень защиты данных, недостижимый в среде с отдельно стоящими компьютерами. Более подробно архивирование и его стратегия рассматриваются в главе 15 "Защита сетей".

Совместное использование приложений

Одно из крупных достижений локальных сетей - простота распространения приложений между служащими офиса. Многие (хотя и не все) приложения устанавливают на центральном компьютере, называемом сервером приложений, и к ним можно обращаться через сеть. Подобная установка приложений имеет несколько преимуществ. Первое: если на сервере установлено множество приложений, клиентным станциям требуется намного меньшее дисковое пространство по сравнению с установкой приложений на каждом отдельном компьютере. Это немаловажный фактор, поскольку, например, для полной установки типичного набора офисных приложений необходимо почти 2 Гбайта дискового пространства.

Как правило, это в точности соответствует вместимости типичных жестких дисков, и вам нет необходимости устанавливать их на каждый сетевой компьютер. Второе: установка и обновление приложений значительно облегчаются, если программы находятся на единственном компьютере. Таким образом, совместное использование приложений сохраняет немало времени и ресурсов, хотя это возможно не для всех приложений и не во всех ситуациях.

Как работает сеть в этом случае? Когда в клиентном компьютере запускается приложение, установленное на сервере приложений, оно загружается в память клиентного компьютера. Работая с программой, клиент взаимодействует с копией, хранящейся в памяти его компьютера, но не в памяти сервера. Это дает доступ к одному приложению одновременно нескольким клиентам.

Примечание

Известен также более совершенный метод совместного использования приложений, называемый тонкой клиентной сетью, который практически не требует от клиентной машины собственных ресурсов (гл. 12).

Предупреждаем: установка приложения на сервере для использования остальной сетью отнюдь не означает, что вам достаточно единственной лицензии на данное приложение. Как правило, для совместного использования приложения необходимо приобрести либо по одной лицензии для каждого пользователя, либо одну общую лицензию (условия зависят от приложения). Если у вас нет соответствующей лицензии на все ваши приложения, то вы виновны в незаконном использовании программного обеспечения, а это относится к федеральным преступлениям. Думаете, об этом никто не узнает? Ошибаетесь. Основная цель наблюдательной организации, называемой Ассоциацией издателей

программных продуктов (Software Publisher's Association - SPA), как раз и заключается в наблюдении за проблемами пиратского использования программ. SPA преследует в судебном порядке нарушителей законных прав входящих в нее организаций. Если вы не знакомы с вопросами лицензирования, не беспокойтесь об этом, а также о деятельности SPA вы узнаете в гл. 11 ("Приложения локальных сетей и их лицензирование").

Улучшение взаимодействия в офисе

По мере разрастания офиса процесс оповещения сотрудников о важнейших событиях и организации совещаний затрудняется. Некогда групповое планирование доставляло немало забот главе офиса. Сеть поможет согласовать работу офиса с помощью приложений электронной почты или средств группового планирования.

Без этих средств организация собраний учреждения превращается в кошмар, когда организатор пытается рассортировать личные расписания сотрудников, чтобы выбрать подходящее время для встречи. Приложения группового планирования намного упрощают эту задачу. Идея такова: каждый служащий вводит в программу-календарь (calendar program) личное расписание, которое может просмотреть только он сам или избранные сотрудники. Все личные расписания сохраняются в центральной базе данных. Когда вы хотите назначить собрание, вы вводите имена приглашенных сотрудников и время. Если все перечисленные сотрудники в указанное время свободны, программа-планировщик (scheduling software) известит вас об этом. В противном случае, она сообщит о наличии конфликта и укажет, с кем именно. Затем, в зависимости от программы, может предложить первый же интервал времени, когда все необходимые сотрудники будут свободны. После этого, назначив время, вы можете с помощью программы-планировщика разослать всем приглашенным уведомления по электронной почте, указав дату и время совещания.

Электронная почта может принести значительно больше пользы, чем планирование совещаний. Пожалуй, в настоящее время она - самое "вездесущее" сетевое приложение. И хотя избыточный сетевой трафик, генерируемый электронной почтой, может вызывать раздражение, она неоценима как быстрый метод принятия оперативных решений и планирования личных встреч. Электронная почта очень проста и удобна. Людям, которые слишком заняты, чтобы выкраивать время для личных встреч, программа-планировщик не нужна. Почта позволяет быстрее рассмотреть проблему и, к тому же конфиденциальна. Если босс зайдет в вашу комнату, это заметит каждый, но если он пошлет вам сообщение по электронной почте, в котором просит зайти для оценки ваших успехов, об этом никто не узнает. Таким образом, офисная электронная почта удобна для любых сообщении, требующих относительной конфиденциальности распространения, либо краткости.

Другое преимущество электронной почты перед телефонной связью и личными встречами заключается в том, что большинство приложений электронной почты позволяют вкладывать в сообщения бинарные файлы. Например, вы можете послать кому-нибудь файл для просмотра со своими комментариями, причем отдельно от самого документа. Получатель сообщения может просто открыть файл и прочитать его, либо отредактировать содержимое файла. Такой метод рассылки бинарных файлов подобен совместному использованию файла в сети, однако имеет преимущества.

- В сообщении электронной почты вы можете указать на какие-либо неточности в данных или указать на важность передаваемой информации.
- Вы можете убедиться в приеме получателем необходимого файла и не беспокоиться, что он по ошибке откроет не тот файл.

- Вам нет нужды заботиться об установке соответствующих разрешений на доступ к файлу или назначать пароли, поскольку копия отосланного файла поступит только к получателю сообщения электронной почты.
- Вы можете отсылать файлы людям, с которыми не поддерживаете связь через локальную сеть, например тем, с кем вы можете связаться только через Internet.

Одним словом, локальная сеть - лучшее, что можно сделать для связи в офисе и совместного использования информации.

Совместное использование периферийных устройств

Первые персональные компьютеры представляли собой, по сути, пустые ящики, в которых находились всего лишь системная плата, память и дисковод. Даже жесткий диск считался дополнительным оборудованием. Так было десять лет назад. Однако по мере совершенствования компьютеров все большее число устройств, до того считавшихся дорогостоящим дополнительным оборудованием, становились частью стандартного профиля аппаратных средств. По мере того, как все большее число устройств начинало входить в стандартную комплектацию компьютера, возникала своеобразная проблема: какие же устройства следует считать периферийными, а какие - нет. Например, принтер - безусловно, периферийное устройство, но к чему отнести привод компакт-дисков? А жесткий диск?

Периферия, или *периферийное устройство* - это просто любая часть оборудования, напрямую или косвенно подсоединенная к системной плате компьютера. Отнюдь не все периферийные устройства расположены вне корпуса компьютера, и не ко всем можно обеспечить общий доступ. Однако совместное использование в сети периферийных устройств, если оно возможно, очень удобно. Во-первых, такое оборудование становится доступным всем пользователям, а во-вторых, его использование упрощается. Например, вместо того, чтобы занимать очередь к компьютеру с подключенным принтером, можно просто послать задание на печать так, как будто принтер подключен к вашей машине, а потом забрать готовую работу.

Совместное использование периферийных устройств помогает пользователям сети сберечь время и деньги. Действительно, даже если в офисе нет сети, необязательно покупать принтер и приводы компакт-дисков для каждого компьютера. Если служащие готовы постоять в очереди при невысокой загрузке сети, одно-два устройства на весь офис могут прекрасно справиться с работой. Однако если служащие, впустую затрачивая время, подолгу ожидают освобождения устройства, экономия на покупке принтеров обернется немалыми убытками.

Общие периферийные устройства, также как и общие папки, не обязательно должны быть доступны всем пользователям сети; кроме того, доступ может предоставляться на разных уровнях. Так, например, вы можете предоставить общий доступ к цветному принтеру, в котором используются дорогостоящие картриджи, но ограничить его таким образом, что доступ смогут получить исключительно художники, но не всякий Дик, Том или Гарри, которым вздумалось напечатать свою мазню.

Таковы основные возможности локальных сетей. Теперь рассмотрим главные компоненты, с помощью которых они реализуется: сетевые платы, кабели и разъемы.

Основные сетевые компоненты

Итак, мы, надеюсь, убедили вас - и ваш офис вступит в двадцать первый век, связав все компьютеры сетью. Вы знаете, что для этого необходимы компьютеры, и уже приобрели их. Какое же оборудование нужно иметь для того, чтобы соединить их и заставить "разговаривать" друг с другом? Для создания простой сети вам потребуются сетевые платы, кабели различных типов и разъемы, для присоединения кабелей к сетевым платам, установленным в компьютерах.

Сетевые платы - дверь во внешний мир

Сетевые интерфейсные платы (NIC - network interface card), которые иногда называют *сетевыми картами (network board)* или *адаптерами (adapter)*, представляют собой дополнительные платы, устанавливаемые на системную плату компьютера для организации сетевого интерфейса. Фактически, нет значительных отличий сетевых плат от прочих плат расширения: они также вставляются в гнездо (slot) системной платы и требуют для своей работы некоторых ресурсов. На краю платы находится разъем, выходящий на заднюю панель компьютера. Разъем предназначен для подключения инструментов, управляющих работой платы. Так, в звуковых платах в разъем подключают колонки для прослушивания звука, а в сетевых платах в него вставляют разъем сетевого кабеля, который и реализует (физически) линию связи.

Сетевые платы (NICs) можно разделить на различные категории по нескольким признакам. Первый: платы различают по типу поддерживаемых сетей. На практике обычно используют два типа локальных сетей: Ethernet и Token Ring. Различия сетей обоих типов подробнее обсуждаются в гл. 2 "Планирование сетевой архитектуры". Пока что достаточно сказать, что ост этих двух типов различаются методами установления связи. Вы не Можете заставить "разговаривать" платы Ethernet и Token Ring без помощи некоторых сетевых устройств, рассматриваемых в гл. 5 "Дополнительное сетевое оборудование".

Второй признак: платы соединяются кабелями разного типа. Разъем на задней стороне платы должен соответствовать применяемому типу кабеля. К счастью, многие современные платы допускают подключение кабелей нескольких типов. Например, к платам Ethernet можно подключать как коаксиальный кабель, так и кабель типа "неэкранированная витая пара" (UTP). Вы можете использовать такие платы, чтобы организовать сеть Ethernet с помощью коаксиального кабеля. Затем, по мере роста сети, вы можете перейти на кабель UTP (в котором используются разъемы RJ-45) без установки новых плат. На рис. 1.1 показана задняя сторона сетевой платы, в которой предусмотрены порты для интерфейсов обоих типов, а также порт интерфейса сетевых устройств (attachment unit interface - AUI).

Рис. 1.1. Сетевая плата с разъемами для подключения коаксиального кабеля и кабеля UTP

Третий признак: платы различаются по типу шины, определяющий скорость обмена данными сетевой и системной плат. В новейших платах персональных компьютеров используют следующие типы шин.

- Industry Standard Architecture (ISA) – стандартная промышленная архитектура.
- Peripheral Connection Interface (PCI) – интерфейс периферийных устройств.

Примечание

Пользователи портативных компьютеров (laptops) должны использовать сетевые платы с интерфейсом PCMCIA (Personal Computer Memory Card International Association - Международная организация производителей плат памяти для персональных компьютеров), называемые также PC-картами. Вы затрудняетесь запомнить эту аббревиатуру? Запомните ее так: "People Can't Memorize Computer Industry Abbreviations" ("Люди не в состоянии запомнить аббревиатуры компьютерной индустрии").

Различие между шинами ISA и PCI в основном заключается в скорости обмена. Скорость обмена данными по шине ISA с системной платой составляет 16 Мбайт/с при тактовой частоте 8 МГц, что в момент принятия стандарта ISA соответствовало скорости работы компьютера. По соображениям обратной совместимости, эти характеристики не изменялись.

Шины PCI, используемые в современных компьютерах, обеспечивают обмен данными с системной платой со скоростью 32 Мбайт/с при тактовой частоте 33 МГц. Эта скорость выше, чем у ISA, так что шина ISA обречена -I ей недостает скорости и других преимуществ PCI (гл. 3). Тем не менее, шина ISA будет применяться достаточно долго, поскольку она установлена в подавляющем большинстве компьютеров. Однако ее смерть неизбежна. Таким образом, рекомендуем выбирать сетевые платы с шиной PCI, несмотря на их несколько большую стоимость по сравнению с платами ISA.

Примечание

Внешняя скорость передачи данных обычно указывается в битах за секунду (бит/с), в то время как внутренняя - в байтах за секунду (байт/с). Один байт равен восьми битам. Много ли это? Один символ ASCII соответствует одному байту.

Четвертый признак: платы различаются по внешней скорости передачи данных, которую принято выражать в миллионах битов за секунду (Мбит/с). Скорость передачи данных, которую может поддерживать выбранная вами Плата - всего лишь один из критериев, определяющих скорость работы сети. Сети Token Ring работают со скоростями 4, 16 и 100 Мбит/с, а сета Ethernet - либо 10, либо 100 Мбит/с. Разумеется, вы можете подключить Компьютер с платой на 10 Мбит/с в сеть, которая работает со скоростью 100 Мбит/с, однако скорость передачи данных из компьютера в LAN будет определяться быстродействием платы.

Примечание

В скоростной версии Ethernet, называемой Gigabit Ethernet, обеспечивается скорость передачи данных до 1 Гбит/с. В настоящее время сетевые платы, поддерживающие подобные скорости, чрезвычайно дороги. В основном они предназначены для I рынка новейших серверов, а не клиентных компьютеров или заурядных серверов.

Серебряная нить, шелковая связь - сетевые кабели

Вероятно, сэр Вальтер Скотт ничего не знал о сетевых кабелях, когда писал об этих "связях", но, в принципе, сказано верно: действительно, сетевые кабели почти невидимы, но они являются весьма важным компонентом всей сети. К решающим факторам, влияющим на выбор типа кабеля можно отнести тип информации, которой обмениваются компьютеры (текст, сложные графические изображения, видео- и аудиоданные), расстояние между ними и среду, в которой должна работать сеть, созданная с их помощью. Поэтому выбор типа кабеля определяется типом создаваемой сети отдельно в каждом конкретном случае.

Примечание

Медные провода, используемые в витых парах и коаксиальных кабелях, могут быть либо многожильными, либо одножильными. *Многожильный провод* состоит из переплетенных проводов меньшего сечения, а *одножильный* - из единственного провода. По сравнению с одножильными, многожильные провода отличаются гибкостью, поэтому использование последних предпочтительнее в тех местах, где они могут подвергается значительной нагрузке, которая может разрушить одножильный провод. Однако при этом надо учитывать, что скорость затухания сигнала в многожильных проводах выше, чем в одножильных.

Каковы же критерии выбора? Их несколько, относящихся как к медным, так и к оптоволоконным кабелям. Кабель каждого типа спроектирован так, чтобы решить тем или иным методом одну из самых серьезных проблем, стоящих перед любым типом линии передачи: минимизировать внешние помехи, (*радиочастотный шум* или *RF (radio frequency) - шум*). Изначально в качестве среды передачи использовались обычные медные кабели, поскольку они превосходно проводят электрические сигналы. Однако это же свойство делает их восприимчивыми к помехам, созданным другими источниками электрических сигналов, искажающими исходный сигнал. Чтобы решить проблему помехозащищенности, и кабелях используют всевозможные методы защиты сигнальных проводников от внешних помех, в том числе и такие которые делают их совершенно нечувствительными к RF-помехам.

Примечание

Источником RF-шума являются электромагнитные помехи (EMI - electromagnetic interference). Такой шум генерируется не только передающими устройствами. Так, электромагнитные помехи генерируют мощные электромоторы, линии электропередачи, излучения радаров, прочие незащищенные должным образом кабели и, конечно, мощные радиопередатчики.

Чем менее чувствителен кабель к помехам, тем с большей скоростью по нему можно передавать данные, поскольку скорость передачи по аналоговым каналам, таким как медные провода, зависит от частоты. Последнее обстоятельство очень важно при выборе типа кабеля. Нередко медные кабели различают по максимально допустимой частоте сигналов, которые они могут пропускать (при заданной величине ослабления - Прим. ред.). Если вы не понимаете, что это значит, то не сможете разобраться в типах кабелей.

Частота характеризует количество колебаний некоторой величины (например, напряжения) за секунду. Она выражается в герцах, или числе периодов колебаний за секунду. В самом простом случае колебания можно представить как синусоидальные волны (рис. 1.2). Иными словами, синусоидальное колебание, частота которого составляет 8 МГц, в течение одной секунды восемь миллионов раз проходит через максимум. Чем выше частота, тем больше скорость перемещения данных, поскольку в единственную секунду можно "упаковать" большее количество единиц и нулей.

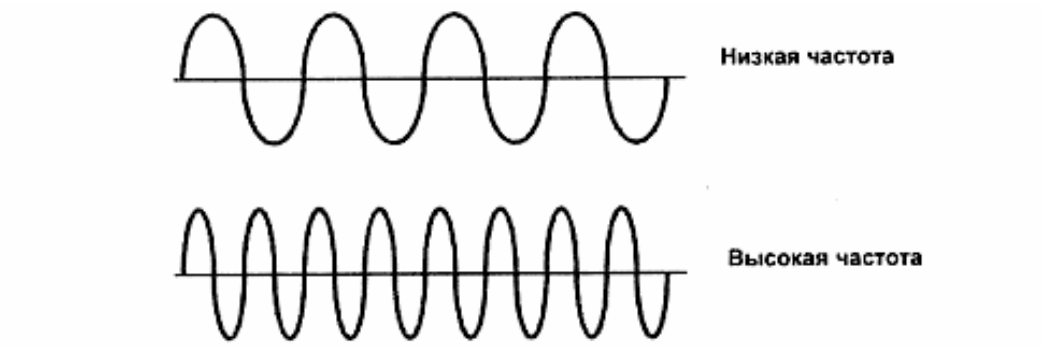


Рис. 1.2. Чем больше колебаний синусоидальной волны за данный период времени, тем выше частота

Высокочастотные сигналы в большей степени подвержены помехам, чем низкочастотные, поскольку за единицу времени они переносят большее число данных. Если это не укладывается у вас в голове, взгляните еще раз на рис. 1.2. Предположим, в течение половины секунды на высоко- и низкочастотные сигналы воздействует какая-нибудь помеха. (Половина секунды - немалое время, но здесь мы собираемся только привести пример и ничего более.) Данные, передаваемые по каналам в эти полсекунды, исказятся и будут отброшены. В случае высокочастотного сигнала, объем потерянных данных будет значительно большим, поскольку за одинаковый период времени он переносит большее количество данных по сравнению с низкочастотным сигналом.

Максимальная частота сигналов в определенной степени характеризует кабель данного типа (это предельное значение не связано с рабочей частотой). Она только указывает, что *теоретически* физическая среда кабеля способна обеспечивать работу на данной частоте, если кабель не поврежден и правильно смонтирован. Например, кабель UTP категории 5 (рассматриваемый в следующем разделе), имеет максимальную частоту передачи 100 МГц, однако для передачи данных со скоростью 100 Мбит/с достаточно частоты 62,5 МГц. Частота сигнала и ее связь со скоростью передачи данных, а также передаваемой мощностью описываются далее в этой главе в разделе "Беспроводные сети".

К другим физическим характеристикам кабелей разных типов относится предельно допустимая длина отрезка кабеля, обеспечивающая передачу сигнала. (Для разных частот длина такого отрезка будет разная. С ростом частоты эта величина будет уменьшаться - Прим. ред.). Длина такого отрезка зависит от *затухания*. Затухание - это степень ослабления сигнала на участке кабеля фиксированной длины (обычно - 100 м на заданной частоте - Прим. ред.). Чем более подвержен кабель воздействию помех, тем сильнее заухает в нем сигнал. Следует различать затухание в кабеле, вызванное собственными потерями (обусловленное, например, потерями сигнала в диэлектрическом заполнении низкого качества), и затухание, обусловленное излучением сигнала из кабеля (вызванное недостаточным экранированием сигнальных проводников). В первом случае предельно допустимая длина отрезка кабеля будет небольшой, но внешние помехи не окажут воздействия на сигнал. Во втором - внешние сигналы могут наложиться на передаваемый (полезный сигнал и исказить его. - Прим. ред.). Для уменьшения затухания сигнала в сети используют различные устройства, например, повторители (репетиры), которые усиливают сигнал на длинных участках кабелей.

Помехи и затухание

Хотя помехи и затухание одинаково влияют на передачу данных, это совершенно разные явления. Помехи - случайный электрический сигнал, искажающий передаваемый полезный сигнал. При этом возможно искажение передаваемых данных и образование фактически нового сигнала: либо за счет добавления "горбов" (humps) к синусоидальной волне (колебанию) (полезный сигнал алгебраически складывается с сигналом помехи; такую помеху называют аддитивной. - Прим, ред.), либо за счет взаимодействия с сигналом (полезный сигнал алгебраически перемножается с сигналом помехи, что, в свою очередь, может происходить только в активных элементах; такую помеху называют мультипликативной. - Прим. ред.). Затухание же - это ослабление сигнала по мере его прохождения по линии связи. Затуханию подвержены любые сигналы. Так, по мере удаления от источника затухают звуковые сигналы, и на некотором расстоянии их уже невозможно разобрать. Точно так же, электрический сигнал, пройдя слишком большое расстояние, затухает настолько, что передаваемые данные искажаются.

Распространение сигналов и помех по сети напоминает распространение звуковых сигналов. С помехами вы сталкиваетесь, когда разговаривают множество людей, и вам трудно разобрать, кто именно и что сказал, и даже идентифицировать какой-либо голос, если его перекрывает другой. С затуханием вы сталкиваетесь, когда кто-нибудь находится слишком далеко от вас, и вы не можете понять, что именно вам сказали. Проблема помех решается экранированием посторонних "разговоров", а затухания - усилением сигнала.

Кабели типа "витая пара"

Если вы обернете один хороший проводник вокруг другого, то получите систему проводников, в определенной степени защищенную от внешних помех (RF-шумов). Именно так изготовлен кабель с витой парой. На практике используют два типа таких кабелей: неэкранированная витая пара (UTP) и экранированная витая пара (STP).

Кабели UTP и STP имеют два отличия. Первое: в UTP используются четыре пары проводников, а в STP - две. Второе, и основное, отличие заложено в самом названии кабелей. В STP предусмотрен дополнительный проводящий слой, окружающий витые провода, который обеспечивает дополнительную защиту от помех. Это отнюдь не означает, что кабель STP всегда лучше защищен от RF-шумов по сравнению с UTP. Просто в кабелях использован разный подход к проблеме защиты. Теоретически, в кабелях UTP два провода, скрученные друг с другом, каждый в отдельности является приемником шума, но эти шумы противофазные.

В кабелях же STP проводники защищены, в основном, дополнительным проводящим слоем, а не скручиванием друг с другом. В то же время, дополнительный защитный слой затрудняет работу с кабелем, поскольку придает ему жесткость. Кроме того, такая защита эффективна только при правильном заземлении и целостности экранирующего слоя. Различия между кабелями UTP и STP показаны на рис. 1.3.

Ассоциация электронной промышленности (EIA), Ассоциация телекоммуникационной промышленности (TIA) и Национальная ассоциация производителей электрооборудования (NEMA) установили стандарт кабелей UTP, подразделяющий их на пять категорий. Затем они уполномочили организацию Underwriter's Laboratories сертифицировать и сортировать и соответствии с этим стандартом кабели, продаваемые на территории Соединенных Штатов. Чем выше номер категории кабеля, тем больше в нем должно быть скруток на погонный фут и чаще меняться форма этих витков для исключения радиочастотных помех (RFI). Таким образом, хотя и не существует кабелей, которые совершенно нечувст-

вительны к помехам, чем выше категория кабеля UTP, тем менее он подвержен помехам RFI и EMI и, соответственно, обеспечивает более быструю и точную передачу данных Другими словами, кабели категории 3 обеспечивают передачу данных со скоростью до 10 Мбит/с и содержат не менее трех скруток на погонный фут. Они иногда встречаются в существующих локальных сетях. Однако практически во всех новых локальных сетях используют кабели UTP категории 5, которые допускают скорость передачи до 100 Мбит/с и позволяют расположить компьютеры на расстоянии до 90 м.

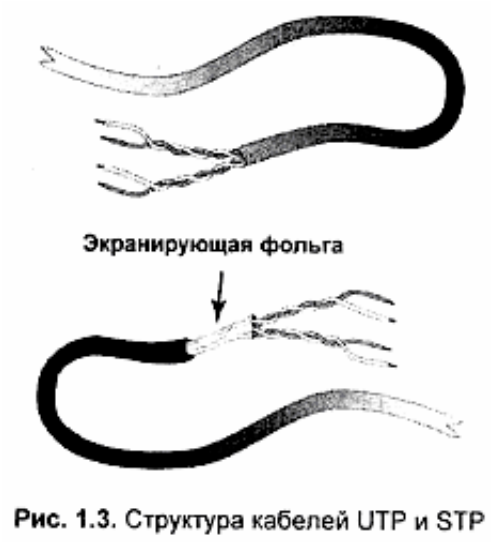


Рис. 1.3. Структура кабелей UTP и STP

Примечание

Кабель STP обычно используют в сетях Token Ring, UTP - в сетях Ethernet (10BaseT и 100BaseT), и изредка в сетях Token Ring.

Другие категории кабелей

Следует отметить, что кабель категории 5 относится к высшему сертифицированному стандарту кабелей с витыми парами. Помимо него, существуют ещё не прошедшие сертификацию стандарты: улучшенная категория 5 и категория 6.

Кабель улучшенной категории 5 подобен кабелю категории 5 (высокоскоростной UTP), однако несколько усовершенствован. По сравнению с обычным кабелем категории 5 форма витков кабеля намного разнообразнее, оме того, в нем использованы провода повышенного качества. Как правило, эти кабели позволяют пропускать сигналы с частотой до 200 МГц. Пока не известно, каким образом кабель улучшенной категории 5 будет описан в стандарте. Возможно, в нем будет указана предельная частота либо стандарт потребует поддержки частоты не менее 300 МГц.

Кабель категории 6 относится, скорее, к типу STP, поскольку в нем предусмотрена обязательная изоляция витой пары проводящей фольгой. Пока не ясно, какие частоты он будет пропускать, а также требования стандарта. Во всяком случае, его предельное значение частоты должно составлять 350-600 МГц. В стандарте категории 6 остается немало нерешенных вопросов, например, тип используемого разъема, точное определение его типа, а также поддерживаемая скорость передачи. Все это пока мешает более широкому применению кабели категории 6.

Кабель категории 5 соответствует требованиям сети Fast Ethernet, которая поддерживает скорость передачи данных до 100 Мбит/с. Зачем же нужны более "быстрые" кабели? В основном, они необходимы в сетях ATM и Gigabit Ethernet, работающих на частотах до

нескольких сотен МГц (350 МГц в ATM). По сравнению с этими скоростными сетями Fast Ethernet напоминает устаревший автомобиль (например, Pontiac Oldsmobil) вашего отца. При частоте, не превышающей 100 МГц кабель категории 5 не в состоянии обеспечить такие скорости передачи, поэтому следует либо улучшать характеристики кабеля UTP, либо перейти на оптоволоконные кабели.

Кроме того, в изделиях фирмы IBM предусмотрено использование кабелей различных типов с витой парой и двух типов оптоволоконных кабелей. Кабели подразделяются по функциональным признакам, а не по степени устойчивости к RFI. Ниже перечислены типы кабелей с витой парой.

Тип 1. Одножильный кабель STP, используемый для передачи данных. Каждый кабель состоит из двух пар проводов.

Тип 2. Сочетание четырех неэкранированных и двух экранированных одножильных проводов в единой оболочке. Неэкранированные провода (UTP) предназначены для передачи речевых сообщений (voice transmission), а экранированные (STP) - данных.

Тип 3. Состоит из четырех пар одножильных проводов, используемых для передачи речевых сообщений и данных.

Тип 6. Состоит из двух пар многожильных кабелей. Во многом подобен типу 1, однако вместо одножильного используется многожильный провод.

Тип 8. Специальный плоский кабель STP, что позволяет прокладывать его под коврами.

Тип 9. Состоит из двух экранированных пар STP, покрытых специальной оболочкой (plenum), а не поливинилхлоридом (PVC), поэтому его можно прокладывать в перекрытиях между этажами здания. При горении PVC выделяет токсичные газы, поэтому, чтобы кабель соответствовал правилам пожарной безопасности, используют иную оболочку.

Как правило, в сетях, проложенных кабелями с витыми парами, каждая сетевая плата соединяется с центральным коммутатором (centrally located switching area). Это может быть либо концентратор, либо подключенный к нему врезной соединитель, который служит точкой подключения множества кабелей. Концентраторы подробно рассматриваются в гл. 5 "Дополнительное сетевое оборудование".

Коаксиальные кабели

Коаксиальные кабели часто называют кабелями BNC, сеть на их основе называют "тонкой" сетью (Thinnet). Они состоят из центрального медного проводника, заключенного в изоляционную оболочку, покрытого слоем алюминиевой или медной оплетки, которая защищает проводник от RF-помех. Коаксиальный кабель состоит из четырех частей (рис. 1.4):

- центрального проводника, называемого внутренним проводником;
- изоляционного слоя, называемого диэлектриком, который окружает внутренний проводник;
- слоя фольги или металлической оплетки, называемого экраном (shield), покрывающего диэлектрик;

- слоя внешней изоляции (наружная часть кабеля), называемого защитным покрытием (jacket).

Рис. 1.4. Коаксиальный кабель

Скорость передачи данных по коаксиальным кабелям не превышает 10 Мбит/с. По современным стандартам это немного, однако в некоторых случаях кабели этого типа предпочтительнее UTP. Во-первых, предельная длина участка кабеля UTP составляет 100 м, а коаксиального кабеля - более 800 м. Однако после 185 м необходимо усилить сигнал с помощью устройства, называемого повторителем, которое рассматривается в гл. 5 "Дополнительное сетевое оборудование".

Во-вторых, вы можете использовать коаксиальные кабели для прямого соединения компьютеров друг с другом (вместо соединения с центральным концентратором) в последовательную цепь. Это очень удобно, если необходимо соединить всего лишь пару компьютеров в одной комнате, поскольку отпадает надобность в приобретении концентратора.

Примечание

На практике используется второй тип коаксиального кабеля, называемый "толстой сетью" (Thicknet). Он применяется в устаревших сетях и в настоящее время встречается редко. У этого кабеля большая протяженность рабочих участков, чем у Thinnet, однако с ним намного сложнее работать. Он настолько жесткий, что один знакомый подрядчик, называет его "замерзшим желтым садовым шлангом". На практике толстые сети используют не для соединения самих компьютеров, а для создания сетевой магистрали (backbone), к которой прочие компьютеры подключены короткими отводами тонкого коаксиального кабеля.

Оптоволоконные кабели

Один из путей решения проблемы защиты от RF-помех, заключается в том, чтобы полностью разрубить этот гордиев узел. Чтобы сделать кабель совершенно нечувствительным к EMI, можно совершенно отказаться от передачи электрических сигналов. Для этого можно использовать *оптоволоконные кабели.*

Оптоволоконные кабели нечувствительны к RF-шуму потому, что для передачи данных в них применяют свет, а не электрические импульсы. Свет проходит по тончайшей стеклянной или пластиковой нити, покрытой тонким изоляционным слоем, называемым *оболочкой* (cladding). Оболочка окружена покрытием, которое защищает непрочную нить. На рис. 1.5 показана структура оптоволоконного кабеля.

Рис. 1.5. Оптоволоконный кабель

Как вы понимаете, оптоволокно - критический элемент среды передачи данных. На каждом конце волокна находится устройство, которое называется *кодек* или *ко*дер/*дека*дер. Кодек отвечает за преобразование данных в световые импульсы и обратное их преобразование в электрические импульсы, с которыми работает компьютер. Чтобы передать данные, светодиод (LED) или лазер, находящийся на одном конце оптоволокна, посылает по кабелю световые сигналы. Когда эти сигналы достигают другого конца кабеля, они преобразуются в исходную (электрическую) форму.

Может показаться, что трафик оптоволоконного кабеля ограничен единственным трактом данных (path of data), но это не так. Во-первых, оптоволоконные кабели могут состоять из нескольких волокон, что позволяет передавать данные по множеству трактов. Чем больше волокон в кабеле, тем больше данных может проходить по нему одновременно (точно так же, как дорога с четырьмя полосами может пропустить намного больше машин, чем однополосная).

Во-вторых, существуют оптоволоконные кабели двух типов: одномодовые и многомодовые.

Примечание

Модой (mode) называют луч света, входящий в оптоволоконный кабель под определенным углом.

Одномодовый кабель передает данные по единственному тракту (path). Луч света в таком кабеле имеет высокую интенсивность, поэтому одномодовые кабели передают данные на большие расстояния. Поэтому они пригодны либо для систем, требующих интенсивного трафика, либо для передачи на большие расстояния.

Многомодовое оптоволокно одновременно пропускает по кабелю множество мод. На практике используют два типа многомодовых оптических волокон: оптоволокно со ступенчатым изменением показателя преломления и градиентное оптоволокно. В *оптоволокне со ступенчатым изменением показателя преломления* световые лучи двигаются внутри кабеля по зигзагообразным траекториям. В *градиентном оптоволокне* световые лучи следуют по более закругленным траекториям, напоминающим синусоидальную волну (рис. 1.6).

Система со ступенчатым изменением показателя преломления: свет следует по кабелю по зигзагообразной траектории

Система с градиентным оптоволокном: свет следует по более плавной траектории

Рис. 1.6. Многомодовые кабели одновременно передают несколько лучей света

Из-за того, что передается множество световых лучей, проходящих по многомодовым кабелям обоих типов, световые импульсы подвержены *модальной дисперсии,* т.е. рассеянию исходного импульса. (Процесс распространения прямоугольного импульса подобен забегу команды спортсменов: на старте они стоят на одной прямой линии (вершина импульса плоская). После старта более быстрые вырываются вперед и приходят к финишу первыми. При этом никакой прямой линии нет. Нет и плоской вершины импульса. — Прим. ред.).

Рассеяние замедляет прохождение сигнала, поэтому одномодовые кабели передают быстрее одномодовых. Чтобы понять, почему так происходит, представьте себе, что вы бросили мяч вниз по трубе. Если вы бросили только один мяч, и он летит, не касаясь стенок трубы, то он будет двигаться быстрее и точнее, чем если бы отскакивал от стенок. Точно так же, как отскакивание мяча от стенок трубы, замедляет его движение, скорость светового луча замедляется отражением от границы оптоволоконного кабеля.

Примечание

Одномодовые кабели дороже многомодовых и могут передавать сигнал на большие расстояния, не требуя усиления. Поэтому многомодовые кабели чаще прокладывают внутри зданий, а одномодовые - между зданиями.

Оптические волокна получили большое распространение в качестве Магистральных линий LAN с отводами на каждую рабочую станцию с помощью кабелей UTP в сетях с напряженным трафиком. Оптоволоконные Кабели редко прокладывают к рабочим столам по двум причинам. Первая: они дороже UTP (и расчете на погонный фут) и требуют для установки некоторых специальных знаний, что также удорожает применение кабелей. Вторая — связана с появлением сети Fast Ethernet, которая поддерживает скорость передачи до 100 Мбит/с по кабелю UTP. Она не достигла скорости работы оптоволоконных линий в сетях FDDI (гл. 2), однако соперничает с ней. Но поскольку для некоторых приложений требуется высокая скорость передачи, а стоимость оптоволоконных кабелей падает, вероятно, вскоре вы встретите их и на рабочих станциях.

Если оптоволоконные кабели слишком дороги для прокладки на рабочие станции и не всегда обеспечивают большую скорость, чем UTP, почему же их используют вообще? Во-первых, это *действительно* скоростные кабели и, кроме того, широкополосные кабели превосходно подходят для передачи трафика с критическими требованиями, например, видеоданных. Во-вторых, поскольку по кабелю передаются световые, а не электрические, сигналы, оптоволоконные кабели абсолютно невосприимчивы к EMI и FRI. Поэтому сигналы иногда могут проходить несколько миль без малейшего искажения. Некоторые типы оптических волокон допускают передачу на расстояние до трех миль в среде LAN, а в среде WAN, с помощью мощных лазерных устройств — через всю страну. Кроме того, оптоволоконные кабели полезны в опасных средах, поскольку не искрят в местах подключения (что потенциально возможно при использовании электрических кабелей). Более того, в них не используется металл, поэтому кабели устойчивы к коррозии. Наконец, к оптоволоконному кабелю труднее подключить несанкционированный отвод, чем к медному, поэтому он лучше защищен и, следовательно, предпочтительнее для создания засекреченных линий связи.

Сравнительно новый вид оптоволоконных сетей — *оптоволоконные каналы* — стирает различие между отдельными устройствами и сетью, причем даже в большей степени, чем это уже достигнуто в локальных сетях. Скорость работы оптоволоконных каналов может даже превысить скорость работы FDDI.

Беспроводные сети

Беспроводные сети не столь таинственны, как может показаться. По существу, в них обеспечивается соединение двух устройств без прокладки кабеля между ними. Такие сети в наибольшей степени полезны в следующих случаях.

- Проводная связь невозможна либо непомерно дорога по соображениям материально-технического (logistical) обеспечения.
- Клиенты (например, пользователи портативных компьютеров) часто соединяются и отключаются от сети, либо не имеют доступа к персональному компьютеру, подключенному к сети.
- Клиенты сети часто перемещаются с места на место.

Однако, если на то нет особой причины, создавать сеть (или часть сети), используя беспроводные соединения, не рекомендуется. Беспроводные сети работают медленнее, чем их проводные аналоги и в большей мере подвержены помехам. В то же время в некоторых случаях они незаменимы. Например, составление инвентарных списков намного облегчается с помощью портативного компьютера, соединенного с сетью беспроводной связью, что проще, чем с проводным терминалом, который необходимо постоянно держать включенным для ввода чисел.

Принцип работы беспроводных сетей точно такой же, как и у проводных Интенсивность работы и скорость передачи сигнала данных зависят от его частоты и от частоты несущей (carrier frequency). Частота несущей зависит от частоты сигнала данных. В этом отношении беспроводные сети можно разделить на два класса: использующие радиочастотные сигналы и инфракрасные. *Радиочастотные сигналы* занимают широкую полосу частот и способны огибать препятствия. Однако скорость обмена радиосигналами относительно невысока. Частота *инфракрасных сигналов* и скорость их передачи очень высока, однако этот сигнал распространяется только в пределах прямой видимости.

Соединение кабелей с сетевыми платами

Приобретение кабелей и сетевых плат — немаловажный этап работы по созданию локальной сети. Вам еще предстоит заставить их "разговаривать" друг с другом. С этой целью применяют разъемы, называемые соединителями (коннекторами).

Разъемы для коаксиальных кабелей

Для соединения коаксиальных кабелей используют разъемы (переходники) трёх типов.

- Тройник (Т-разъем);
- BNC-разъемы;
- Терминатор.

Тройник своим штыревым разъемом подключается к гнездовому разъему сетевой платы, расположенному на металлической планке. К тройнику можно подключить два разъема BNC (рис. 1.7).

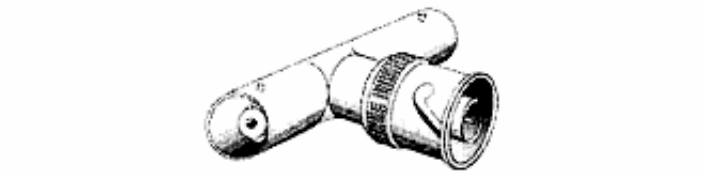


Рис. 1.7. К Т-разъему можно подсоединить разъем BNC

Разъем BNC (рис. 1.8) вставляется в Т-разъем, присоединенный к сетевой плате. Такое подключение платы к кабелю имеет характерную форму (рис. 1.9) и может также использоваться для соединения отрезков коаксиального кабеля.

Рис. 1.8. BNC-разъем позволяет соединять коаксиальные кабели друг с другом

Разъем BNC (рис. 1.8) вставляется в Т-разъем, присоединенный к сетевой плате. Такое подключение платы к кабелю имеет характерную форму (рис. 1.9) и может также использоваться для соединения отрезков коаксиального кабеля.

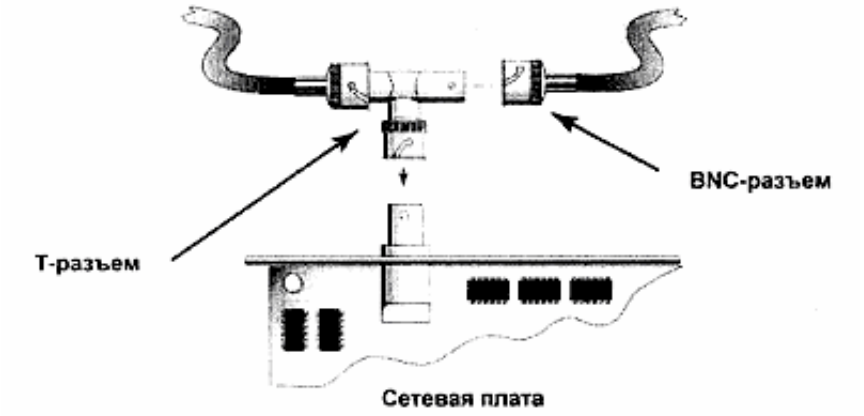


Рис. 1.9. Разъем BNC используется для подключения коаксиального кабеля к Т-разъему

Терминаторы (нагрузочные резисторы) устанавливают на концах сетевых сегментов (рис. 1.10) и используют для согласования концов кабеля. (Активное (омическое) сопротивление терминатора должно равняться волновому сопротивлению коаксиального кабеля. — Прим. ред.). Если на каждом конце коаксиального сегмента не установить терминаторы, сигнал будет отражаться от конца кабеля, что приведет к появлению *теневых пакетов.* Последние замедляют работу сети, поскольку повышают сетевой трафик, и могут исказить данные, если они неотличимы от подлинных пакетов. Согласование гарантирует отсутствие таких пакетов, когда сигнал достигает конца сегмента.

Рис. 1.10. Чтобы избежать появления теневых пакетов, к концам коаксиальных сегментов необходимо подключить терминаторы

Примечание

Терминаторы могут иметь различные сопротивления (для кабелей с волновым сопротивлением 50 и 75 Ом). Как правило, для построения компьютерных сетей используют кабель с волновым сопротивлением 50 Ом. Покупая терминатор, будьте внимательны, поскольку совместная работа терминаторов разных номиналов невозможна. В большинстве случаев в продаже есть именно 50-омные терминаторы.

Разъемы для кабелей "витая пара"

Для подключения кабелей UTP используют разъемы RJ-45, которые несколько напоминают разъемы для подключения телефонных аппаратов, однако выглядят более массивно (рис. 1.11). Они устанавливаются на обоих концах кабеля. Один конец в плату компьютера, а второй - в концентратор или врезной соединитель монтажного шкафа (wiring closet). По существу, кабель напоминает телефонный, однако несколько толще.

Рис. 1.11. На каждом конце сетевого кабеля UTP находится разъем RJ-45

Не все кабели UTP предназначены только для соединения концентратора с сетевой платой. В некоторых сетях можно использовать кросс-кабель (crossover cable) для последовательного соединения компьютеров. *Кросс-кабели* изготовлены так, что могут исполнять функции концентратора.

Разъемы для кабелей STP отличаются от разъемов для UTP. Для соединения кабеля STP с сетевой платой можно использовать разъем D (рис. 1.12). Для подключения кабеля к устройству многостанционного доступа (MAU) или концентратору, используют разъем IBM Data Connector (рис. 1.13).

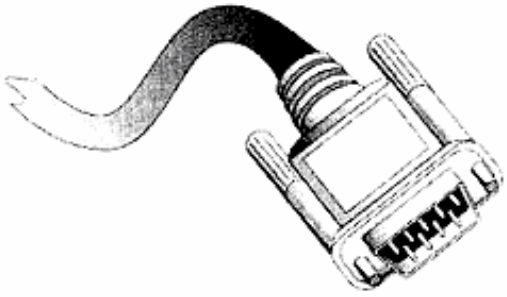


Рис. 1.12. Разъем D обеспечивает подключение кабеля к сетевой плате компьютера

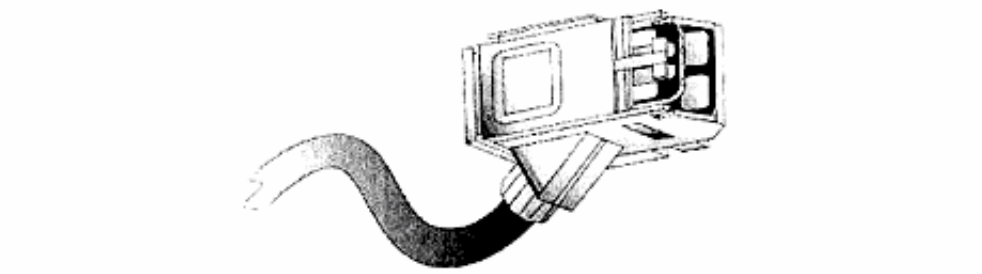


Рис. 1.13. Разъем IBM Data Connector обеспечивает подключение кабеля к MAU

Предупреждение

Нетрудно заметить, что разъем D, используемый для подключения сетевой платы Token Ring, точно такой же, как для подключения к видеоплате. Проявите осторожность: не подключите сетевой кабель к монитору.

Разъемы для оптоволоконных кабелей

В отличие от медных кабелей, в которых основной причиной ослабления сигнала является сама передающая среда (медный проводник и диэлектрик вокруг него), в оптоволоконных кабелях сигнал рассеивается главным образом, в разъемах. В оптоволоконных кабелях используют разъемы двух типов: *SMA* (соединитель с резьбовой оправкой) и *ST* (подпружиненная втулка). Для крепления на кабеле разъемов ST используют подпружиненную втулку, а разъем SMA накручивают на конец кабеля. Разъемы ST (рис. 1.14) используются чаще, чем SMA.

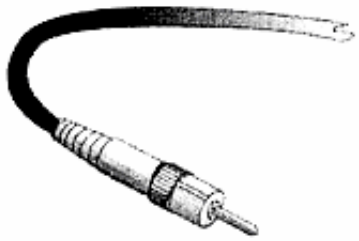


Рис. 1.14. Разъем ST и его футляр

Общие вопросы использования кабелей и разъемов различных типов

У вас возникли проблемы с усвоением информации обо всех этих кабелях и разъемах? Для упрощения, в табл. 1.1 перечислены все рассмотренные выше типы кабелей, приведены скорости их работы, максимальная длина рабочих участков и средства обеспечения подавления электрических помех.

Таблица 1.1. Типы кабелей и разъемов

Тип кабеля	Предельная скорость передачи данных	Максимально допустимая длина рабочего участка	Средства подавления помех	Разъём
Коаксиальный	10 Мбит/с	750 м	Наружный проводник	BNC
Неэкранированная витая пара (UTP)	100 Мбит/с	90 м	Скручивание пар проводников	RJ-45
Экранированная витая пара (STP)	100 Мбит/с	90 м	Скручивание пар в сочетании с металлическим экраном	D
Оптоволокно	155 Мбит/с и более	10 000 м	Специальные средства не используются	ST или SMA

Модель OSI

До сих пор мы говорили о физических элементах сети. Другой важный аспект заключается в методах передачи данных по этим элементам. Методы подробно рассматриваются в последующих главах, где обсуждаются типы сетей и протоколы передачи данных. Все станет намного проще при условии существования некоторой модели, включающей в себя эти методы, и позволяющей понять, как взаимодействуют элементы сети на различных уровнях ее организации.

Что такое модель OSI

На заре появления сетей системы связи между компьютерами разрабатывались на пустом месте. Причем задача взаимодействия стеков протоколов от различных поставщиков отнюдь не относилась к приоритетным.

Способствуя развитию стеков сетевых протоколов, которые *могли* бы общаться друг с другом, Международная организация по стандартизации (ISO) предложила модель для разработки *открытых систем* — т.е. таких сетевых систем, которые могут сообщаться с другими сетевыми системами, поскольку используют одинаковую модель связи. Полностью реализовать этот замысел не удалось, однако модель взаимодействия открытых систем **(OSI),** появившаяся в окончательном виде в 1984 г., предоставляет удобную основу для понимания того, каким образом различные компоненты сети "разговаривают" друг с другом.

Примечание

Модели OSI полностью соответствуют всего несколько (а может, и ни одного) существующих протоколов. В большинстве случаев в книге приводятся примеры различных сетевых протоколов, а иногда и аппаратных средств, выполняющих стандартные для каждого уровня функции. Эти протоколы описаны далее в этом разделе книги.

Основное преимущество использования систем, соответствующих модели SI для разработки сетевых стандартов, заключается в их гибкости. Это значит, что если вы измените физическую среду передачи данных, то вам не потребуется изменять всю структуру сети.

Модель OSI – возврат к милитаризму?

В феодальной Японии не было единого правительства. Она была поделена на связанные между собой, но более или менее независимые провинции, управляемые собственными военачальниками. Путешествуя по разным провинциям, им не могли рассчитывать, что законы одной провинции действуют в другой. Так было до тех пор, пока Юси Токугава (Ieyasu Tokugava) не объединил насильственно всю страну под властью центрального правительства.

Хотя модель OSI никто не вводил насильственно, она подобна режиму Токугавы в том смысле, что представляет собой попытку объединить "разделенный мир" и заставить взаимодействовать различные его части.

В августе 1998 г. в прессу просочилась внутренняя докладная записка (и Microsoft подтверждает ее подлинность), в которой один из служащих Microsoft предлагает отказаться от поддержки (returning to) этой модели. По каким причинам? Чтобы растоптать конкурирующие "открытые" операционные системы (open-source operating systems), такие как Linux опирающиеся на открытую организацию сети (open networking). Копию докладной записки (аннотированную Эриком Раймондом (Eric Raymond), адвокатом открытого программного обеспечения, упомянутым в записке), можно прочитать по адресу http://www.opensource.org/halloween.html.

Случится ли это? Со времени публикации записки прокатилась волна общественного протеста, так что в политическом аспекте создание фирмой Microsoft собственного протокольного стека затруднительно. Это особенно верно еще и потому, что Microsoft уже находится под следствием Министерства юстиции, расследующего нарушения антимонопольного законодательства. Но, даже если открытые системы останутся открытыми, это должно служить предупреждением: открытые системы опираются на общественную кооперацию, а не конкуренцию.

Уровни модели OSI

Как показано на рис. 1.15, модель OSI предусматривает разделение сетевых функции на семь уровней, причем каждый из них соответствует отдельной физической или логической части сети. Как правило, уровни этой модели изображают в форме стека, но отношения между ними станут понятнее, если представлять уровни концентрическими кругами, как и показано на рис. 1.15. Вообще говоря, каждый уровень поддерживает работу вышележащих уровней (т. е. уровней расположенных ближе к центру). Например, кабель UTP относится к средствам физического уровня, которое обеспечивает физическое соединение двух точек локальной сети (LAN). Сеть Ethernet (гл. 2), является носителем канального уровня, создающим виртуальный канал внутри физического канала путем задания физических адресов источника и получателя передаваемых данных. Протокол сетевого уровня IP (гл. 3), перемещается по виртуальному каналу, создаваемому протоколом канального уровня.

Поддержка отношений между уровнями модели OSI наиболее явно выражена на физическом, канальном и сетевом уровнях, но даже во внутренних кругах они поддерживаются

всеми уровнями, что их окружают. Например, протоколы прикладного уровня (application protocols) не могут работать вне сеансов клиент/сервер, которые устанавливаются протоколами передачи данных сеансового уровня (session data protocols).

Физический уровень

Физический уровень описывает физическую среду, составляющую сеть: медные провода, оптоволокно, космические спутники и все остальное. Если сеть состоит из нескольких носителей, определенных на физическом уровне, то необходимо установить оборудование, которое позволяет им "разговаривать" друг с другом.

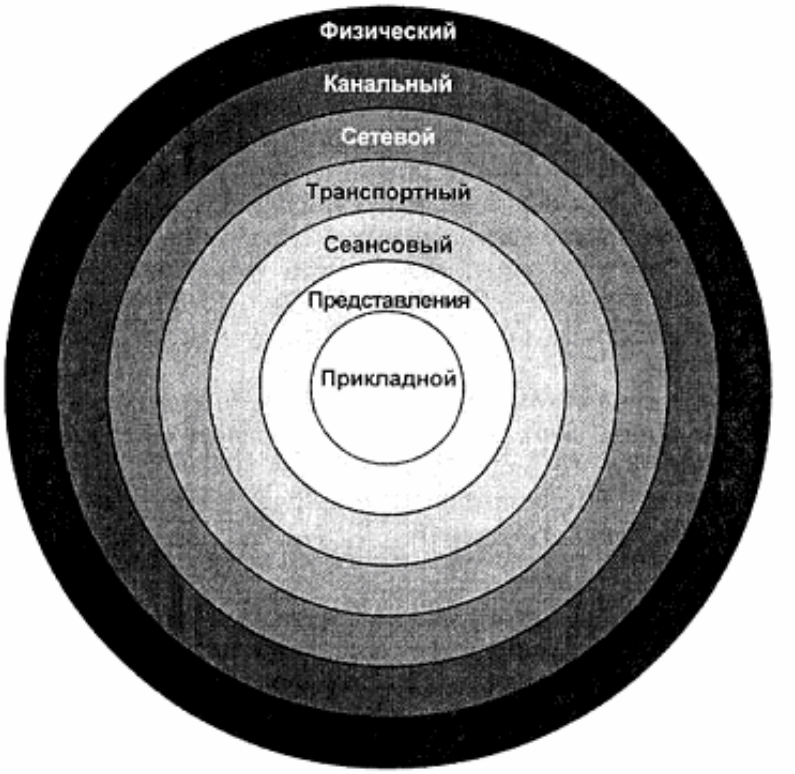


Рис. 1.15. Модель OSI

На физический уровень данные поступают как последовательность битов, всякой информации о формировании кадра (framing information) и чего-нибудь еще, кроме потока данных. В зависимости от типа соединения, поток может быть последовательным или параллельным, а связь — *дуплексной* (одновременная передача и прием данных) либо *полудуплексной* (поочередные прием или передача данных). Если сигнал ослабевает, то на этом уровне он усиливается устройством, называемым *повторителем.*

На физическом уровне не предусмотрено никакой формальной адресации, за исключением виртуальной цепи между отправителем и получателем пакета. Для организации адресации пользователям сети в доступной форме и предназначены высшие уровни.

Канальный уровень

Протоколы, работающие на *канальном уровне,* должны обеспечивать (по возможности) безошибочную передачу по месту назначения наборов данных (протоколов), передаваемых по физическому носителю. Поскольку носителей, совершенно исключающих ошибки, не существует, в протоколах канального уровня предусмотрен механизм контроля ошибок и повторной передачи искаженных пакетов. Например, в сетях Ethernet (гл. 2), предусмотрен выход из ситуации одновременной отправки двух пакетов (предполагается, что ни один из них не попадет к адресату) и механизм разрешения этого конфликта.

На канальном уровне необработанный битовый поток, проходящий по физическому носителю, перехватывается (trapped) и собирается в кадр (framed) для отправки. *Формирование кадра* (framing) означает упаковку данных в небольшие сегменты, называемые *пакетами* или *кадрами (фреймами).* Помимо данных, в каждом пакете содержится адресная информация и, иногда, запись о количестве данных в пакете. Таким образом, сеть может узнать об утрате части данных. Содержимое и структура фреймов зависит от типа сети. Поэтому, если в сети используется два протокола канального уровня (например, Ethernet и Token Ring), то для того, чтобы они могли взаимодействовать между собой, следует использовать устройство, называемое *мостом.*

Поскольку на канальном уровне сети биты передаются в порядке их поступления в канал, этот же уровень отвечает за их поступление в надлежащем порядке по месту назначения. По существу, протоколы канального уровня и предоставляют (организуют) надежные каналы связи между процессами сетевого уровня.

Сетевой уровень

Протоколы сетевого уровня отвечают за определение наилучшего пути маршрутизации данных между компьютерами. На этом уровне определяются логические сетевые адреса, такие как IP-адреса (имеется в виду часть протокола TCP/IP, относящаяся к сетевому уровню), использующиеся протоколами высших уровней. Поскольку маршрутизация выполняется на сетевом уровне, оптимальный путь доставки информации из одного сегмента сети в другой определяют устройства, называемые *маршрутизаторами,* обеспечивающие работу сети на данном уровне. Протоколы сетевого уровня не отвечают за доставку данных по конечному адресу, а только находят наилучший путь.

На транспортном уровне (который рассматривается ниже) не имеет значения тип физического носителя сети и число протоколов канального уровня, определяющих размер и содержимое пакетов. К нему относится только маршрутизация пакетов между логически заданными адресами. Кстати сказать, на сетевом уровне можно пакетировать данные в собственных устройствах (units). Это облегчает маршрутизацию, поскольку используются адреса низших уровней, неизвестные протоколам. На транспортном уровне эти адреса используются для гарантии доставки данных по логическому адресу, заданному в пакетах сетевого уровня.

Транспортный уровень

Протоколы *транспортного уровня,* такие как SPX или TCP, отвечают за доставку данных по логическим адресам, определяемым протоколами сетевого уровня. Эти протоколы анализируют и разделяют (subdivide) пакеты данных, отсылаемые им, упаковывают в пакеты меньшего размера и вновь собирают по достижении места назначения.

Протоколы транспортного уровня работают несколько медленнее протоколов сетевого уровня, поскольку в них содержится больший объем информации, необходимый для коррекции ошибок. Эта информация включается в состав пакетов на тот случай, если что-либо пойдет не так, как надо. Это — последний уровень модели OSI, который поддерживается большинством сетей.

Сеансовый уровень

Основное назначение *сеансового уровня* — поддержка двух следующих уровней: представления данных и прикладного. На данном уровне, путем передачи сообщений, определяется метод установления связи между двумя удаленными системами, называемый *удаленным вызовом процедур* (RPC — remote procedure call). Для выполнения этой задачи на сеансовом уровне имеются две функции: управление диалогом (dialogue control) и разделение данных (data separation). Функция *управления диалогом* предоставляет регламентированные средства начала переговоров, передачи сообщения между удаленными системами, а затем по завершении сеанса прерывания соединения. Процесс *разделения данных* предусматривает вставку в сообщение указателей, которые позволяют каждой рабочей станции сообщать о начале и конце сообщения. Обе функции для сеанса одинаково важны, поскольку гарантируют получение сообщения обеими машинами, причем в полном объеме, а также отсутствие в нем посторонней информации. Точное содержание сообщения на этом уровне не контролируется. Службы сеансового уровня предоставляет NetBIOS.

Уровень представления данных

Протоколы *уровня представления данных* выполняют функцию представления информации в виде понятном получателю. На этом уровне выполняется сжатие / восстановление, а также шифрование / дешифрование данных. Слово "представление" относится не к внешнему виду интерфейса данного уровня, а к методу представления данных.

Прикладной уровень

Наконец, прикладной уровень отвечает за передачу информации от интерфейса приложения к любому сетевому ресурсу, которому она необходима Протоколы, работающие на этом уровне, значительно различаются по размеру и сложности. Некоторые передают огромное количество данных между сервером и клиентом, другие — выполняют небольшое число задач. В хорошо спроектированном стеке протоколов прикладной уровень может охватывать до 90 % данных, передаваемых по сети. Поэтому производительность сети в большей или меньшей степени определяется параметрами этого уровня.

Выводы

В этой главе были приведены начальные сведения о работе сетей. Теперь вы знаете, каким образом сеть может улучшить работу вашего офиса. Кроме того, мы рассмотрели различные виды медных и оптоволоконных кабелей, а также разъемы для соединения ка-

белей с сетевыми платами разного типа. Итак, в этой главе рассмотрены следующие вопросы.

1. Локальными называют сети, которые ограничены пределами одного здания. Они облегчают совместное использование файлов и периферийных устройств, а также создают костяк вашего офиса, позволяя широко использовать различные средства связи, такие как электронная почта и офисные базы данных.
2. Сетевые платы можно классифицировать в соответствии: с типами поддерживаемой сети, типом шины, скорости работы и прочими параметрами, однако в любом случае сетевые платы относятся к периферийным устройствам, позволяющим компьютеру работать в сети. Конструкции сетевых плат предусматривают использование различных типов кабелей.

На передачу данных по сети неблагоприятное воздействие оказывают помехи. Эту проблему можно решить двумя способами. В электрических кабелях от помех можно защититься экранирующим слоем (либо скручиванием кабелей, либо экранированием), который защищает кабель от внешних воздействий, либо прокладкой оптоволоконных кабелей. Оптоволоконные кабели нечувствительны к электрическим помехам, поскольку для передачи данных используется световые, а не электрические сигналы. Единственный недостаток оптоволоконных кабелей — намного большая стоимость, по сравнению с электрическими.

Сетевые кабели подключаются к сетевым платам специальными разъемами (соединители, коннекторы). Для кабеля каждого типа используется особый разъем, соответствующий порту на сетевой плате. Наличие разъема и порта позволяет создать интерфейс между компьютером и сетью. В сетях некоторых типов необходимо использовать не только разъемы, но и терминаторы — устройства, позволяющие согласовать сегменты сети.

Сеть можно описать семиуровневой моделью OSI, определяющей различные протоколы, используемые при организации сети. И хотя многие, широко применяемые, протоколы работают на нескольких различных уровнях модели OSI, эта модель весьма удобна для понимания взаимодействия различных частей сети.

Для начала этого довольно. В гл. 2 "Планирование сетевой архитектуры", мы применим полученные знания о компонентах локальных сетей, начав с рассмотрения топологии сетей.

Упражнение 1

Заполните приведенную ниже таблицу недостающей информацией.

Тип кабеля	**Предельная скорость передачи данных**	**Максимально допустимая длина рабочего участка**	**Средства подавления помех**	**Разъём**
Коаксиальный		750 м		BNC
	100 Мбит/с	90 м	Скручивание пар проводников	
Экранированная витая пара (STP)	100 Мбит/с		Скручивание пар в сочетании с металлическим экраном	
	155 Мбит/с и более		Специальные средства не используются	ST или SMA

Глава 2

Планирование сетевой архитектуры

В гл. 1 "Концепция организации сетей и сетевые компоненты" были рассмотрены основные вопросы, относящиеся к сетям в целом. Вы уже познакомились с элегантными концепциями, относящимися к определению характеристик сетевых адаптеров, кабелей и разъемов. Однако остаются нерешенными несколько вопросов: как следует организовывать эти каналы, и какой тип сети следует использовать, чтобы можно было "переговариваться" друг с другом. В этой главе рассмотрим главные моменты планирования сетевой архитектуры, а также смысл понятий "физическая организация" и "логические связи" или, говоря более живым языком, физическую и логическую топологии сети.

Может быть, вы не знакомы с термином "топология". В математике — это раздел посвященный изучению таких свойств геометрических структур, которые не подвергаются изменениям при их растяжениях и изгибах. Применительно к сети этот термин имеет два значения. *Физическая топология* относится к физической структуре сети или же к тем ее характерным чертам, которые вы увидите, если начертите ее структурную схему (своего рода "вид сверху"). *Логическая топология* сети характеризует способ прохождения пакетов данных по сети, а также метод организации связи в сети, обеспечивающий одновременную работу "на передачу" только одной сетевой станции (поскольку все сетевые станции используют одну и ту же линию связи), и принципы организации контроля низкоуровневых ошибок, гарантирующие, что данные попадут туда, куда их направили.

Примечание

Хотя названия "физическая" и "логическая" топологии "перекрываются", эти понятия не имеют ничего общего. Например, имеются физическая и логическая топологии шины, однако сеть, организованная как логическая шина, не обязательно должна быть организована как физическая шина.

Физические топологии

Выбор физической топологии сети зависит от нескольких факторов:

- структуры офиса;
- способов диагностики неисправностей;
- стоимости инсталляции;
- типа используемого кабеля.

Первый фактор — устройство вашего офиса. При установке нескольких компьютеров в одну комнату появляется больше возможных вариантов организации сети, чем в случае, когда множество компьютеров распределяется по различным комнатам здания.

Второй фактор — наличие методов и средств диагностирования неисправностей — зависит в какой-то мере от используемой физической топологии. Например, некоторые топологические схемы характеризуются встроенной в них физической избыточностью, обеспечивающей бесперебойную связь даже при возникновении повреждений в кабеле. В

других топологических схемах каждый кабельный сегмент сети может быть отключен (перекоммутирован), поэтому одно повреждение не сможет привести к отказу всей сети.

Третий фактор — не все физические топологии эквивалентны друг другу по стоимости. Некоторая доля в стоимости, несомненно, определяется планом вашего офиса. Ясно, что разводка сети, расположенной в обширной области, более трудоемка, и в стоимости будут отражаться эти дополнительные усилия. Однако часть стоимости определяется сложностью выбранной вами топологии, и, что еще более важно, тем, насколько сложно эту топологию привести в соответствие с пространством офиса. Шинная топология, например, очень просто реализуется в пределах небольшой области, но может стать источником головной боли при прокладке кабеля по офису, занимающему несколько комнат.

Последний фактор — выбор физической топологии в значительной степени определяется типом кабеля и наоборот. Вспомните из Гл. 1 "Концепция организации сетей и сетевые компоненты", что при подключении каждого сетевого компьютера к концентратору кабелем UTP используется разъем RJ-45. Такая конфигурация называется *топологией звезды,* поскольку кабели, идущие от компьютеров к концентратору, напоминают лучи, радиально расходящиеся из некоего центра. Для сети с физической топологией звезды нельзя использовать коаксиальный кабель, поскольку он не пригоден для этого метода.

Теперь рассмотрим некоторые, наиболее распространенные, физические топологии, с которыми вы, вероятно, встретитесь в процессе работы.

Физическая шинная топология

Для простых сетей, расположенных в пределах небольшой территории, физическая шинная топология (известная в мире компьютеров Mac как "цепочка") может оказаться наилучшим решением. В топологии шины кабель идет от компьютера к компьютеру, связывая их в цепочке. Все компьютеры в сети связаны одним общим кабелем, как правило, коаксиальным.

Примечание

В сети с кабелем типа "витая пара" может использоваться физическая шинная топология. При этом можно подключать дополнительные компьютеры соедини тельным кабелем, но на самом деле это способ непрактичен при соединении в одну сеть трех и более компьютеров.

Вы можете подключаться к сети с шинной топологией двумя способами в зависимости от используемого кабеля. Если в сети используется толстый коаксиальный кабель (см. гл. 1), то такая сеть с шинной топологией имеет центральную магистраль, реализованную с помощью толстого коаксиального кабеля. К каждому компьютеру сети от магистрали подходят маленькие, более тонкие (и более гибкие) кабели, называемые *отводами.* Для физического подключения тонких кабелей к толстому магистральному кабелю используют небольшие устройства — *трансиверы*. Пример такой топологии показан на рис. 2.1.

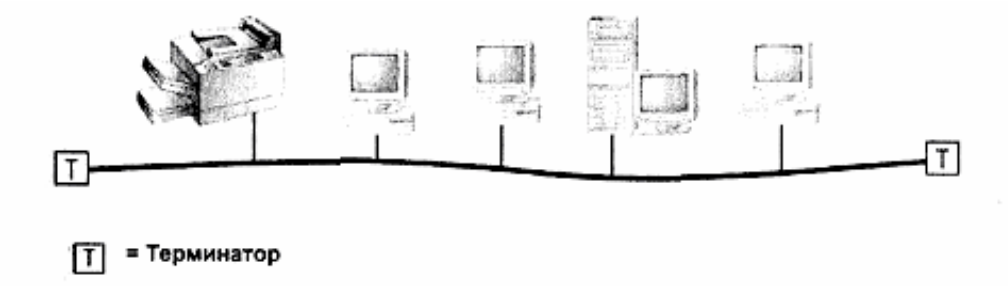


Рис. 2.1. Физическая шинная топология, реализованная с использованием толстого коаксиального кабеля

Конфигурация "толстой" сети Ethernet обычно используется при объединении мэйнфреймов и миникомпьютеров (рис. 2.1), но популярность таких сетей падает по мере того, как персональные компьютеры становятся более мощными и соответственно сети, базирующиеся на мэйнфреймах, — менее распространенными. Для новых сетей, использующих физическую шинную топологию, удобнее применять тонкий коаксиальный кабель.

В противоположность "толстой" Ethernet, в *"тонкой" сети (Thinnet)*избегают использования магистрали, а подключение всех сетевых устройств выполняется напрямую. Вместо толстого кабеля, для тонкой сети используют более гибкий коаксиальный, описанный в гл. 1 (рис. 2.2). Такая разновидность физической шинной топологии сегодня более популярна, чем её "толстый" двойник, в котором применяют отводы и трансиверы. Суть дела в упрощении работы - с толстым кабелем в "толстой" Ethernet тяжело работать, поскольку он очень жесткий.

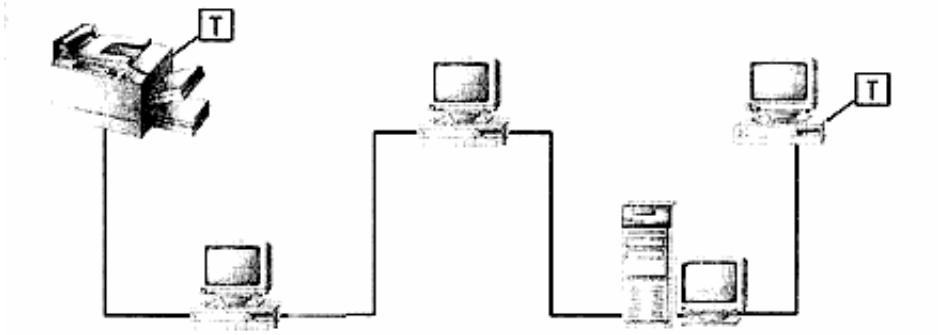


Рис. 2.2. При физической шинной топологии в "тонкой" сети персональные компьютеры могут подключаться к магистрали и напрямую

Наибольшая проблема, которая может возникнуть при работе с сетью шинной топологии, заключается в неправильном согласовании (вспомните, что было сказано о сопротивлении терминаторов в гл. 1). В этом случае сеть не может корректно выполнять передачу данных. Используя физическую шинную топологию, следует любым способом избегать нарушения целостности кабеля на всем его протяжении. Такие нарушения могут возникнуть из-за неправильной работы узлов и разрывов кабеля.

Сеть не сможет корректно передавать данные, даже если всего один узел работает неправильно, поскольку системе в целом необходимо, чтобы каждый узел был в рабочем состоянии, обеспечивая прохождение данных. Это вовсе не означает, что для корректной работы сети все компьютеры в сети должны быть включены и зарегистрированы. Имеется существенное отличие между неправильно работающим (например, по причине неполной стыковки разъемов кабельного соединения) и выключенным узлом. Если узел выключен, данные к следующему активному узлу проходят через Т-разъем, подключенный к сетевой плате. В этом случае сеть не будет "знать", что в ней имеется неактивный узел. Однако

если узел активный, но работает неправильно, то, безусловно, возникнет проблема. Активный узел, как и ранее, пытается обработать пакет, но делает это с ошибками, что замедляет работу всей сети или приводит к ее внезапной остановке.

Разрывы кабеля также вызывают появление проблем в сети с шинной топологией, поскольку корректная работа сети зависит от правильного функционирования кабеля на всем протяжении между его согласованными концами. Если в какой-либо точке кабель разрушен, сеть не сможет работать, и потребуется немало времени для определения места разрыва и замены поврежденного сегмента кабеля. При этом может потребоваться проверка каждого разъема, для того чтобы удостовериться, что он надежно установлен, что никто не пытался перезагрузиться или выйти из системы во время прохождения сигнала, и во многом другом.

Шинная топология имеет одно преимущество — это высокая эффективность кабельной системы, помогающая сэкономить деньги при создании наиболее дорогой части сети. Однако она может оказаться сложной для реализации, если сетевые компьютеры не расположены в строгом линейном порядке. Например, сеть, узлы которой распределены по всему зданию – неудачный кандидат на реализацию шинной топологии — и, вероятно, eel будет легче обслуживать, если реализовать сеть на основе топологии звезды.

Звездообразная физическая топология

В сети, построенной по *звездообразной топологии,* каждый сервер и рабочая станция подключаются к центральному концентратору, который обеспечивает связь между ними, поэтому сеть, в которой используется звездообразная топология, будет выглядеть примерно так, как показано на рис. 2.3.

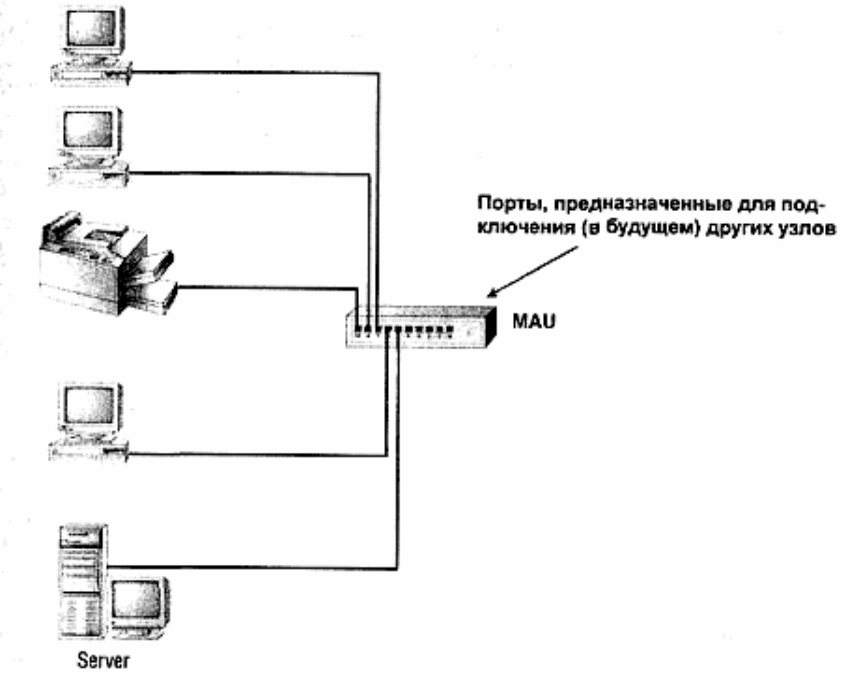


Рис. 2.3. В сети, построенной по звездообразной топологии, все ресурсы подключаются к центральному устройству

В первых сетях для передачи данных использовалась звездообразная топология для подключения неинтеллектуальных терминалов к мэйнфреймам. Почему же эта топология

повсеместно используется и до сих пор? Вероятно, потому, что при ее использовании существенно легче работать в сети. Каждая рабочая станция и сервер имеют отдельное соединение с центральной коммутационной станцией. Это значит, что каждое соединение работает независимо. Обрыв кабеля, идущего к рабочей станции А, не окажет воздействия на рабочую станцию В. Это также означает, что для такой сети относительно легко создать кабельную систему, поскольку можно не тревожиться о том, как расположены относительно друг друга компьютеры в сети. Пока длина отрезка кабеля от каждой рабочей станции или сервера до центральной коммутационной станции не превышает максимально допустимого значения, никаких проблем не возникает.

Центральной частью сети, построенной по звездообразной топологии, является концентратор. Концентраторы могут быть разными, но их суть проста: это устройства, реализующие центральный узел для всех сетевых кабелей, обеспечивая тем самым связь между портами, что позволяет компьютерам подключаться к нему для обмена сообщениями. (В гл. 5 "Дополнительное сетевое оборудование" конструкция концентраторов будет рассмотрена более подробно.)

Еще одним важным преимуществом такой сети является то, что в ней легко диагностировать неисправности. Как было ранее описано в разделе "Физическая шинная топология", при возникновении сбоя в сети с шинной топологией может оказаться очень непросто точно определить, в чем заключается проблема, если, конечно, не просматривать все узлы подряд В сети, построенной по звездообразной топологии, найти ее источник очень легко. Если некий узел не работает, то проблему, очевидно, следует искать где-то между портом концентратора и физически подключенным к нему узлом. Следует проверить, что является источником нарушения работоспособности:

- терминал;
- кабель между концентратором и терминалом;
- порт концентратора, обслуживающий терминал, вызывающий беспокойство.

Если ни один из узлов сети не обеспечивает качественное соединение
сервера и концентратора (неплохо держать один концентратор про запас, если это возможно), то проблема, вероятно, заключается в сервере. Если это так, то самое время уповать на то, что вы запланировали сделать для отказоустойчивой работы системы и на то, что вы сделали резервные копии файлов.
Звездообразная топология также хорошо подходит и для физически распределенных сетей. Представьте себе сеть с четырьмя компьютерами - три рабочих станции и один сервер. Если одна станция находится на этаже сверху, а две — на этаже снизу, да еще и в отдельных комнатах, то значительно проще проложить отдельный сетевой кабель к каждому компьютеру, не беспокоясь о связях всех узлов друг с другом, а затем подключить все кабели к концентратору.

Конечно, звездообразная топология имеет один серьезный недостаток: в ней используется много кабеля. К каждому элементу сети требуется проложить свой собственный кабель. Наличие центрального концентратора и в самом деле не является наиболее эффективным методом организации кабельной системы, поэтому если вы заинтересованы в снижении стоимости сети, а узлы расположены рядом друг с другом, вы, вероятно, предпочтёте шинную топологию.

Распределенная физическая звездообразная топология

Для больших сетей одного концентратора может оказаться недостаточно. Возможно, у него будет маловато портов для поддержки всех компьютеров сети или компьютеры слишком далеко отстоят от концентратора, или одновременно и то, и другое. Для подключения всех устройств к сети может потребоваться несколько концентраторов, но идея создания в одном здании трех или четырех отдельных сетей может показаться не очень привлекательной. Как же решить проблему?

Это случай, для которого может пригодиться одна из разновидностей физической звездообразной топологии: *связанная звезда (connected star)* или *распределенная звезда (distributed star)*. Здесь концентраторы сети последовательно подключены друг к другу, так что все они могут обмениваться информацией (рис. 2.4). Такая организация сети имеет некоторые недостатки, свойственные сети, построенной по шинной топологии: разрыв кабеля между двумя концентраторами изолирует части сети по обеим сторонам разрыва. Однако этот недостаток компенсируется тем, что при отсутствии шины концентраторы были бы изолированы друг от друга в любом случае.

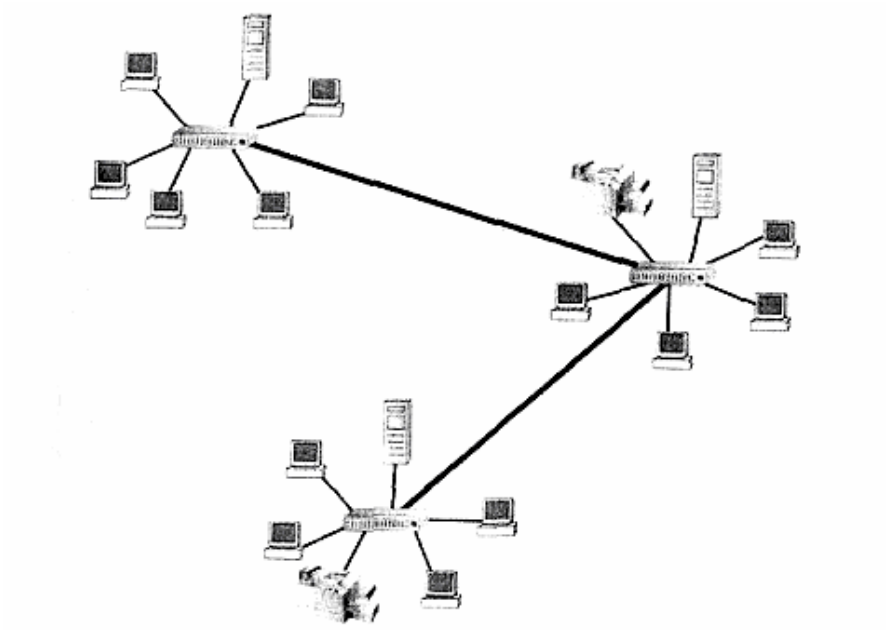


Рис. 2.4. Использование распределенной звездообразной топологии для подсоединения нескольких сетей, также построенных по звездообразной топологии

Физическая кольцевая топология

Наконец, рассмотрим физическую топологию, с которой вам вряд ли придётся столкнуться на практике, но, тем не менее, заслуживающую упоминания. Это сеть, построенная по физической кольцевой топологии (рис. 2.5), в которой все персональные компьютеры сети для обеспечения целостности сети соединены в кольцо, выполненное в виде пары кабелей, проложенных между каждым узлом. Такая система вполне работоспособна, но её стоимость и трудоёмкость прокладки кабельной системы весьма велики, поскольку и такой сети затраты на кабель удваиваются.

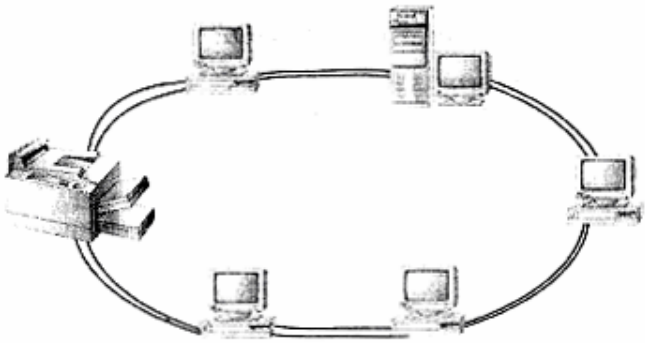


Рис. 2.5. В сети, построенной по физической кольцевой топологии, кабель соединяет все сетевые компьютеры в кольцо

Такую сеть иногда применяют для глобальных оптоволоконных сетей, поскольку это неплохой способ предоставить множеству узлов в региональной области доступ к оптоволоконной сети. Однако автору известна только одна локальная сеть, использующая физическую топологию кольца — старая система автоматизированного офиса фирмы IBM, называемая 8100. Вам, вероятно, не придется сталкиваться ни с одной подобной системой, поэтому просто учтите, что такая топология существует, и забудьте о ней. Исключением из этого правила является технология оптоволоконных каналов (см. раздел "Скоростные сети Fast Ethernet и Gigabit Ethernet" далее в этой главе), в которой может использоваться физическая кольцевая структура для создания средств физического уровня, реализующих высокоскоростную линию связи между узлами сети и другой аппаратурой. Из-за высокой стоимости оптоволоконных линий связи, вы вряд ли встретитесь с ними на практике, но реально они существуют.

Быть может, кто-то из читателей уже чешет затылок, говоря: "Я знаю кое-кого, кто пользуется сетью с кольцевой топологией!". Вероятно, они вспомнили сеть Token Ring. (Token Ring - система разводки сетевых связей, предложенная IBM, в которой используется логическая кольцевая топология и предусматривается передача маркера (token). Далее мы ее рассмотрим).

Логическая топология

Логическая, или *электрическая,* топология описывают способ, в соответствии с которым устройства сети передают информацию от одного узла к следующему, но нельзя путать его с теми линиями, которые нарисованы на структурной схеме сети. Однако это не просто понятия из области чистой теории, поскольку способ, в соответствии с которым сеть должна передавать информацию, может напрямую воздействовать на ваши решения при покупке кабеля или сетевых интерфейсных плат.

Поскольку мы переходим к рассмотрению логической топологии, помните, что физическая топология не имеет прямого отношения к логической. Сеть может иметь физическую звездообразную топологию и логическую кольцевую или физическую звездообразную и логическую шинную и т. д.

Логическая шинная топология

Ethernet — наиболее известный пример сети с логической шинной топологией — является самым популярным типом локальной сети. Как вы вскоре увидите, топология Ethernet — не то же самое, что физическая шинная топология (эта концепция не всегда легко воспринимается и приходится ее повторять для лучшего усвоения).

Как работает сеть с логической шинной топологией? Говоря простым языком, каждый раз, когда у какого-либо узла сети оказываются данные для другого узла, то первый узел производит "оповещение" всей сети. Все остальные узлы "слушают" сеть и проверяют, предназначены эти данные для них или нет. Если предназначены, то они "оставляют их себе", если нет — игнорируют. Каждая плата Ethernet имеет специфический (выделенный специально для нее) 48-битовый адрес, и каждая "порция" данных, путешествующая по сети, направляется по адресу платы в тот узел, который должен принять данные.

Примечание

А что произойдет, если пакет предназначен сразу для нескольких рабочих станций? Сетевое программное обеспечение может дать указание плате Ethernet "прослушивать" определенные групповые адреса. Если пакет для всей сети, то его целевой адрес должен быть равен 1s, и его должна принять каждая плата.

Кто бы и что бы ни передал в сеть, его услышат все. Это несколько напоминает старые телефонные линии коллективного использования, в которых несколько соседей совместно пользовались одним телефонным номером. Каждому из них назначался отличный от прочих сигнальный звонок, определяющий, кто должен принять телефонный вызов. Если, скажем, у вас три коротких звонка, вы принимали вызов, поскольку знали, что звонят вам. С другой стороны, если вы слышали два длинных и один короткий звонок, то знали, что звонят вашему соседу Барту и могли не обращать на звонок никакого внимания. Во всяком случае, звонок слышали все, а отвечать могла только одна персона — та, которой этот телефонный вызов предназначался. Сети с шинной топологией работают подобным образом, однако они эффективнее по сравнению со старыми "коллективными" линиями связи, поскольку соседние компьютеры в сети могут не обрабатывать не относящиеся к ним данные.

Итак, мы знаем, как данные находят в сети пункт назначения. Но как же сетевые компьютеры их посылают? В сети с шинной топологией каждая рабочая станция может посылать информацию в модуле сигналов, называемом *пакетом.* Данные, передаваемые по сети *любого* типа, должны удовлетворять жестко заданному формату - формату *кадра канального уровня (Data Link Layer Frame),* который используют для упорядочивания данных. Этот формат определен на канальном уровне модели OSI (см. гл. 1).

Примечание

Пакеты в Ethernet могут иметь различную длину, но длина не должна превышать 1518 байт, потому что тогда никакая рабочая станция не будет работать на передачу слишком долго, загружая сеть. (Об этом в разделе "Стандарт Ethernet (802.3n)" этой главы).

Перед тем как рабочая станция начнет широковещательную передачу в сеть, она прослушивает "эфир" и определяет, не пользуется ли сейчас сетью кто-либо еще. Если сеть свободна, рабочая станция начинает широковещательную передачу.

А что будет, если сеть занята? Наибольшая проблема в методе широковещательной сетевой передачи - расстояние. Если расстояние между двумя компьютерами в одной и той же сети (назовем их Узел А и Узел Б) слишком велико, они могут не услышать сигналов друг друга в линии связи. Если они не могут "слышать" друг друга, то Узел А не может сказать, передает информацию Узел Б или нет. Думая, что все тихо, Узел А может на-

чать свою передачу, когда Узел Б еще передает данные. Если это случится, и два узла будут передавать информацию одновременно, произойдет конфликт пакетов, приводящий к "пульсации" частоты сигнала в кабеле. Первый же узел, который заметит возросшую пульсацию частоты сигнала, пошлет высокочастотный сигнал, отменяющий все другие, и сообщит всем узлам, что случился конфликт, и что все узлы сети должны остановить передачу пакетов. Далее каждый узел "молчит" в течение некоторого промежутка времени, продолжительность которого задается случайным образом, после чего повторно делает попытку широковещательной передачи. Прежде чем отказаться от новых попыток они делают это до 16 раз. Познакомьтесь со вставкой "Восстановление работы узлов после конфликтов", описывающей этот процесс для сетей Ethernet. Рис. 2.6. иллюстрирует этот процесс в сетях Ethernet.

Рис. 2.6. Пересылка пакетов по сети, использующей логическую шинную топологию

Восстановление работы узлов после конфликтов

Метод, который используется узлами для выбора времени передачи данных, называется *усеченный двоичный порядок выдержки времени* (в отличие от почти всех терминов в мире LAN для этого названия нет общепринятого акронима или аббревиатуры). Говоря проще, этот метод работает так: каждый из двух узлов войдя в противоречие, генерирует случайное целое число в диапазоне между 1 и 2, умножает это число на одну вторую и затем делает паузу на это количество миллисекунд перед повторной передачей. Конечно, при первой попытке есть вероятность того (она равна 0,5), что узлы А и Б выберут одинаковое число, и поэтому им придется повторить попытку. В следующий раз узлы А и Б будут случайным образом выбирать число из диапазона 1—4 и снова повторять попытку. Если они снова выберут одинаковые числа, то далее уже будут выбирать число из диапазона 1—8. Все это продолжается вместе с удвоением верхней границы числового диапазона И каждом шаге, до тех пор, пока или узлы А и Б выберут разные числа, или не будет сделано 16 попыток. После этого дальнейшие попытки выбора прекратятся. Вероятность установления связи между узлами А и Б весьма высока, но при выполнении шестнадцатой попытки задержка перед соединением достигнет половины секунды. Представьте, что это значит для сети со скоростью передачи данных 100 миллионов бит в секунду. Однако необходимость выполнения такого количества попыток возникает очень редко.

Насколько вероятно возникновение конфликтов? Использование кабелей, длина которых не превышает допустимой величины, снижает шанс возникновения конфликта, поскольку узлы смогут услышать широковещательную передачу других узлов. (Например, применительно к сети Ethernet это значит, что участок кабеля не должен быть длиннее 185 метров, после чего сигнал следует усилить.) Фактически, метод работы сети с логической шинной топологией *увеличивает* вероятность возникновения конфликтов пакетов. Если узел не может выполнить широковещательную передачу, пока сеть занята, то что же случится, когда линия связи освободится, а несколько узлов уже будут иметь данные для передачи? Они внезапно начнут одновременно передавать свою информацию, в результате чего снова могут возникнуть конфликты.

Учтите, что описанная выше процедура имеет место в сетевых платах Ethernet. Поэтому, если вы намереваетесь использовать топологию Ethernet, во всех узлах сети должны быть установлены платы Ethernet. Сеть Ethernet может быть построена на базе физической шинной, звездообразной или кольцевой топологии.

Примечание

Сеть Ethernet не является единственным примером использования логической шинной топологии, однако это наиболее известный ее пример. Другие сети, в которых используется логическая шинная топология, включая LANtastic фирмы ArtiSoft и LocalTalk/AppleTalk, построены на базе компьютеров Macintosh. Сеть LocalTalk способна передавать только четверть миллионов бит в секунду, но в ней используются многие базовые принципы построения сети Ethernet.

Логическая кольцевая топология

Логическая шинная топология является системой широковещательной передачи: то, что "скажет" одна станция, "слышат" все остальные. А вот сеть построенная по кольцевой топологии функционирует иначе. В таких сетях, как Token Ring и FDDI (Fiber Distributed Data Interface - распределенный интерфейс передачи данных по оптоволоконным каналам), каждая станция должна повторять то, что она услышит от предыдущей, работая при переносе данных подобно "пожарной цепочке". Когда порция данных возвращается их отправителю, передача прекращается. Весь файл не может быть передан целиком в виде одного пакета, поэтому он будет передаваться порциями (рис. 2. 7).

Организационной основой логической кольцевой топологии является специальный формат пакета данных, называемый *эстафетой (token pocket).* (Кадр можно рассматривать как своеобразный контейнер, для упаковки данных с целью дальнейшей пересылки. Он выполняет те же функции, что и металлический контейнер для морских и железнодорожных перевозок: защищает содержимое от повреждений, имеет отличительные знаки на поверхности в определенных, регламентированных местах и, самое главное, на контейнере указан адрес получателя. Это и есть маркер, который можно рассматривать как пустой контейнер, снабженный флажком, на котором написано сообщение для всех железнодорожных станций и морских портов, встречающихся по маршруту его следования. — Прим. ред.). Использование маркера позволяет устранить конфликты пакетов, гарантируя то, что в данный момент времени только одна станция сможет посылать информацию через сеть. Такой метод называют эстафетой. Он действует подобно волшебной палочке, наводящей порядок в сети при появлении шумов. Суть метода состоит в том, что только один узел, который контролирует эстафету, может передавать информацию через сеть.

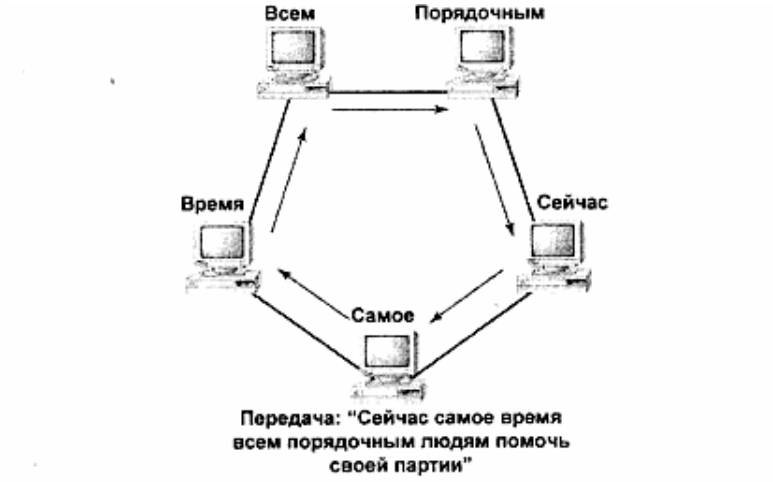


Рис. 2.7. Пересылка данных в сети с кольцевой логической топологией

Каким же образом эстафета проходит по сети? Когда рабочая станция завершает работу с эстафетой, она освобождает ее для какой либо ближайшей на линии станции. Если эстафету никто не захватит, то рабочая станция передает ее второй раз. Если никто не ответит и во второй раз, рабочая станция посылает общий запрос, называемый *кадром запроса преемника (solicit successor frame)*. Этот кадр проходит по всей сети, спрашивая: "Кто следующий должен принять маркер?". Если какая-либо рабочая станция ответит, то посылающая рабочая станция адресует маркер этой же ночей станции и передает его. Поскольку ни один узел не может осуществлять передачу данных до тех пор, пока порция (кадр) данных не сделает полный круг по всей сети, то ни один персональный компьютер не будет ждать дольше, чем требуется для одного оборота информации, перед тем как он получит шанс на передачу данных.

В сетевой кольцевой топологии не выполняется широковещательная передача данных по сети. Они передаются от узла к узлу, поэтому большое значение имеет синхронизация процессов, гарантирующая, что пересылаемые по сети кадры принимаются должным образом. Важно также, чтобы и маркер обеспечивал такую синхронизацию. Из-за важности маркеров для поддержания порядка в сети, построенной по логической кольцевой топологии, один компьютер специально выделяется для управления маркером. Этот компьютер, называемый *задатчиком маркера* или *активным монитором,* определяет потерю маркеров, отслеживает передачу кадров и создает новый маркер, если это необходимо. Активный монитор также генерирует импульсы сигналов времени в сети, синхронизирующие все остальные узлы сети.

Стандарты IEEE

Отдельные типы сетей в настоящее время стандартизованы Институтом Инженеров по Электротехнике и Радиоэлектронике (IEEE — Institute of Electrical and Electronics Engineers). Соответствующие стандарты определяют структуру сетей на физическом и канальном уровне модели OSI, описанной в гл. 1. Эти уровни в определенном смысле перекрываются друг с другом, поэтому стандарты описывают как физическую среду передачи данных, так и методы передачи пакетов. Другими словами, вы сможете узнать, как будет вести себя сеть, удовлетворяющая этим стандартам, и как эта сеть должна быть сконструирована для выполнения требуемых задач. Далее приводится обзор некоторых стандар-

тов IEEE, ссылки на которые вы, вероятно, встретите, когда будете иметь дело с организацией сетей.

Примечание

Все эти стандарты начинаются с цифры 802, поскольку за поддержку стандартов в области локальной сети отвечает 802-й комитет IEEE.

Стандарт 802.2

Стандарт 802.2 определяет правила передачи данных на канальном уровне для сетевых топологий, определенных в стандартах 802.3 - 802.5. Они применимы как к сетям Token Ring, так и к Ethernet, и описывают взаимодействие между сетевыми протоколами, например, TCP/IP, и сетями различных типов. Стандарт 802. 2 предусматривает функционирование сетей в режиме без соединения (для протоколов, которые не требуют установления явного соединения) или в режиме, ориентированном на соединение, (т. е. предназначенном для протоколов, требующих явного установления соединения).

В стандарте IEEE канальный уровень разделяется на два подуровня: подуровень *связи логических каналов (LLC — Logical Link Connection),* называемый также уровнем *соединения канала передачи данных (DLC — Data Link Connection),* и на подуровень *управления доступом к среде передачи (MAC - Media Access Control).* На LLC-уровне обеспечивается управление интерфейсом между всеми сетевыми топологиями и их протоколами передачи данных (сетевого уровня). Для выполнения этой задачи средства LLC-уровня опираются на средства уровня MAC, предоставляющего определенные сведения об адресации информации. Используемый же метод адресации информации определяется типом сети.

Стандарт Ethernet (802.3n)

Сеть Ethernet впервые была сконструирована в 70-х гг. доктором Робертом Меткалфом (Robert Metcalfe) как часть проекта "офиса будущего". В то время это была сеть со скоростью работы 3 Мбит/с. В 1980 г. сеть Ethernet была стандартизована консорциумом фирм DEC-Intel-Xerox (DIX) как сеть со скоростью 10 Мбит/с, а в 1985 г. Она была стандартизована 802-м комитетом IEEE. С тех пор новая технология Ethernet наследует признаки базовой структуры исходной схемы Ethernet, предусматривающей логическую шинную топологию и метод множественного доступа с контролем несущей и обнаружением конфликтов (CSMA/CD - Carrier Sensing Multiple Access with Collision Detection). В различных типах Ethernet используются различные физические топологии (например, звездообразная или шинная) и различные типы кабелей (например, UTP, коаксиальный, оптоволоконный).

Примечание

Все сети Ethernet типа 10Base2, 10Base5, 10BaseT или 10BaseF являются "вариациями на тему" стандарта 802.3.

Основы Ethernet

Информация, "путешествует" по сети Ethernet в виде пакетов, каждый из которых состоит из шести частей.

Преамбула. Содержит восемь байтов информации, используемой для позиционирования остальной части информации в пакете.

Адрес назначения. Содержит аппаратный адрес ("зашитый" в плату Ethernet) рабочей станции или станций, которые принимают эту информацию.

Адрес источника. Позволяет принимающей рабочей станции распознать Рабочую станцию, пославшую информацию.

Тип. Определяет тип информации, хранящейся внутри части пакета с Данными — является ли она графической информацией, текстом ASCII или чем-либо другим.

Фактические данные. Это может быть любая информация объемом от 46 до 1500 байтов.

Контрольная последовательность кадра. Позволяет определить ошибки передачи пакета; используется для проверки того, достигла ли остальная часть пакета места назначения без повреждения.

На рис. 2. 8 показаны части кадра Ethernet в соответствии со стандартом 802.3

Рис 2.8. Структура кадра сети Ethernet в соответствии со стандартом 802.3

Имеется несколько различных типов Ethernet, каждый со своим собственным номером и именем, под которым они наиболее известны. Эти типы описаны в табл. 2.1.

Таблица 2. 1. Некоторые типы сетей Ethernet и их описание

Номер стандарта IEEE	Общеупотребительное название	Физическая топология и среда передачи данных	Пропускная способность
802.3	10Base2	Шинная, тонкий коаксиальный кабель	10 Мбит/с
802.3	10BaseS	Шинная, толстый коаксиальный кабель для магистрали, тонкий – для отводов	10 Мбит/с
802.3u	100BaseT или Fast Ethernet	Звёздообразная, неэкранированная витая пара	100 Мбит/с (версия на 10 Мбит/с задана в 802.3)
803.3z	Gigabit Ethernet	Звездообразная, оптоволоконный кабель для магистрали, коаксиальный кабель для отводов к концентраторам	1000 Мбит/с

Интерпретация названий сетей Ethernet

Сети Ethernet различных типов имеют общепринятые названия, под которыми они известны более широко, чем по соответствующим номерам, присвоенным комитетом IEEE. Эти названия оформлены как комбинация букв и чисел и, возможно, выглядят не более содержательно, чем номера их стандартов, присвоенные ШЕЕ. Они не очень информативны, и основной принцип их составления состоит в том, что первое число описывает максимально возможную скорость передачи данных в сети (в мегабитах за секунду). Далее идет слово "base", означающее, что передача данных выполняется без модуляции несущей, т. е. данные передаются последовательно в отличие от широкополосных сетей типа тех, что иногда используются для соединений WAN и в которых данные могут передаваться параллельно. (Речь идет о передаче данных одновременно на нескольких разных несущих. — Прим. ред.) Наконец, последняя буква определяет предельно допустимую длину сегмента сети (в метрах).

Последняя часть обозначения, не очень полезна, поскольку не всегда содержит точные сведения. Например, в сети 10Base2 длина сегмента фактически не может превышать 185 метров. Но на этом месте не всегда может стоять число, иногда здесь указывается тип кабеля, например, 100BaseT (витая пара) или 100BaseF (оптоволоконный кабель). Тем не менее, если вы когда-либо задавались вопросом, почему сеть 10Base2 названа именно так, то теперь вы получили ответ.

Примечание

Независимо от типа физической топологии, в сети Ethernet всегда используют логическую шинную топологию, означающую, что все кабели LAN - часть одного и того же тракта передачи данных и доступны всем сетевым PC.

Независимо от типа сети, наиболее примечательной особенностью стандарта 802. 3n является *метод множественного доступа с контролем несущей частоты и обнаружением конфликтов (CSMA/CD — Carrier Sensing Multiple Access with Collision Detection).* Метод множественного доступа с контролем несущей частоты и обнаружением конфликтов — совершенно невозможно выговорить, не правда ли? Название отражает самую суть наибольшей проблемы сетей Ethernet, коротко описанную ранее: как можно одновременно посылать через сеть огромное количество информации без всяких конфликтов?

Краткий ответ таков: невозможно. Однако этот ответ не такая уж большая неприятность: Ethernet *рассчитана* на возникновение конфликтов время от времени. Чтобы разобраться в CSMA/CD давайте разобьем это название на части. Слово "Carrier" (несущая) означает: все узлы перед попыткой передачи данных "слушают" сеть чтобы определить ее состояние (свободна или занята). Слова "Multiple access" (множественный доступ) означают: все узлы сети имеют доступ к одному и тому же кабелю, т. е. выполняется широковещательная передача сигнала по всей LAN. Наконец, слова "Collision detection" означают: любой узел может определить, что другой узел начал передачу в то время, когда первый узел еще передает данные. Короче, CSMA/CD предоставляет средства, позволяющие уменьшить вероятность конфликтов между пакетами путем использования каждым PC широковещательной предварительной передачи сигнала, называемого *сигналом контроля несущей (carrier-sensing signal)* перед передачей данных с целью определения, не ведет ли широковещательную передачу какая-либо другая рабочая станция. Если такой передачи нет, то по результатам приема сигнала контроля несущей принимается решение "все свободно", и рабочая станция начинает передачу пакета. Однако если в результате приема сигнала контроля несущей обнаруживается передача данных другой рабочей станцией, то

первая станция ожидает некоторое время, прежде чем начать широковещательную передачу.

Описанный метод позволяет избегать конфликтов до тех пор, пока сетевой трафик не слишком интенсивен и длина кабелей LAN не превышает предельного значения. Если же выполняется какое-либо из этих условий, то конфликт, скорее всего, произойдет, несмотря на использование метода CSMA/CD. Он не гарантирует передачу данных только одной рабочей станцией. Он обеспечивает лишь "молчание" всех станций перед тем, как одна из них начнет передачу. Если две рабочие станции случайно начнут передачу одновременно, то средства CSMA/CD не смогут устранить конфликт.

Если же два пакета "перекрываются", то CSMA/CD позволит избежать повторения конфликта. Как было указано ранее в этой главе, сразу после возникновения конфликта каждая рабочая станция выбирает случайное число между 1 и 2 перед повторением попытки передачи. Если две рабочие станции выберут одно и то же число, произойдет повторный конфликт при их попытке выполнить одновременную широковещательную передачу. Тогда они выберут число между 1 и 4 и сделают вторую попытку. Процесс идет до тех пор, пока рабочие станции успешно не завершат передачу своих данных или пока не выполнят 16 безуспешных попыток. Если они не смогут устранить конфликт за шестнадцать попыток, обе рабочие станции сделают паузу и предоставят шанс другим станциям выполнить передачу данных.

Совет

Если 16 попыток не приводят к успешному выполнению передачи данных, то это означает наличие в сети некоторой неисправности. Проверьте целостность кабелей или выполните холодную перезагрузку оборудования сети.

В приведенном ниже списке перечислены диапазоны чисел, используемых при каждой повторной попытке устранения конфликта передачи.

Номер попытки	Диапазон чисел
1	1-2
2	1-4
3	1-8
4	1-16
5	1-32
6	1-64
7	1-128
8	1-256
9	1-512
10-16	1-1024

В сети Gigabit Ethernet обеспечивается как полудуплексная передача данных для разделяемых областей сети (тех областей, в которых узлы "борются" за использование полосы пропускания сети), так и дуплексная, применяемая для неразделяемых областей, построенных по принципу "коммутатор к коммутатору". Разделяемые области, в которых для устранения конфликтов пакетов используется метод CSMA/CD, взаимодействуют несколько иначе, чем разделяемые области, содержащие более медленные сети Ethernet. Это обусловлено повышенными скоростями линии связи. Поскольку скорость сети высока, в применяемые способы синхронизации должны быть внесены изменения, иначе узлы не смогут "услышать" друг друга перед началом своей передачи. Поэтому в сетях Gigabit Ethernet для устройств, работающих в полудуплексном режиме (узлы сети), минимальный квант времени, предоставляемый каждому пакету, увеличивается от 64 до 512 байтов, т. е.

каждому узлу предоставляется окно, достаточное для передачи 512 байтов вместо 64. В пакетах с размерами менее 512 байтов свободные места будут заполнены незначащей информацией, чтобы их размеры соответствовали увеличившимся квантам времени. Поскольку укрупнение квантов времени замедляет передачу пакетов из-за более редких импульсов временных сигналов, в сети Gigabit Ethernet поддерживается групповая передача пакетов, при которой в течение одного временного кванта посылается целая группа маленьких пакетов. Однако такое изменение метода синхронизации не способствует совместимости с медленными сетями Ethernet, в частности, потому, что в дуплексных областях сети Gigabit Ethernet используется такой же 64-битовый квант времени, что и в медленных разновидностях сетей, определенных стандартом 802.3n.

Описанное выше изменение способа синхронизации сети приводит к появлению и другого усовершенствования, применимого, главным образом, для сетей Gigabit Ethernet, используемых на магистральных участках — использовании устройства, называемого *буферизованным распределителем (buffered distributor).* Буферизованный распределитель аналогичен концентратору, соединяющему два и более сегмента сети Gigabit Ethernet, подобно повторителю (описываемому в гл. 5). Главное отличие между буферизованным распределителем и повторителем состоит в том, что повторитель адресует пакеты во внешние сегменты сразу после их получения, в то время как распределитель может помещать полученные кадры в буфер, что позволяет эффективнее использовать имеющуюся полосу пропускания.

Вряд ли вы в ближайшем будущем увидите сеть Gigabit Ethernet, подключенную к вашим настольным рабочим системам — она слишком дорогая. Скорее всего, эта технология будет вначале использоваться для создания высокоскоростных соединений между маршрутизаторами или коммутаторами (описанными в гл. 5) в сети Ethernet. Развертывание ее для настольных рабочих систем произойдет только после снижения стоимости, как это произошло в свое время с сетью Fast Ethernet.

Использование оптоволоконных линий связи для высокоскоростных сетей

Технология Gigabit Ethernet создавалась не на пустом месте. Применяемые в ней методы обеспечения высокой скорости передачи данных по каналам линий связи сети базируются на методах, первоначально разработанных для сетей с оптоволоконными линиями связи.

Оптоволоконный канал изначально задуман как метод, стирающий различия в скорости между сетевыми аппаратными средствами и самой сетью, однако с помощью средств, отличных от обычно применяемых с этой целью. Вместо попытки сделать все части сети доступными из единого пункта (чего, фактически, пытаются достичь во всех других методах организации сети), оптоволоконные каналы физически делают все части сети единым устройством путем замещения сетевых кабелей и высокоскоростных каналов передачи данных (например, сетевых устройств с интерфейсом SCSI описанным в гл. 8) на высокоскоростные оптоволоконные каналы, сразу работающие с гигабитными скоростями. Тем самым сервер может быть подключен к жесткому диску кабелями, идущими из него через всю комнату, но при этом жесткий диск остается устройством, локально подключенным к сетевым аппаратным средствам.

В оптоволоконных каналах предполагается, что соединения могут быть трёх типов. Первый: двухточечные, связывающие два устройства. Второй: организованы как физическое кольцо, в котором все устройства соединены вместе кольцевой связью. Третий: организованы в виде так называемой *фабрики (fabric),* в которой устройства одновременно

являются частью физической и логической сети.

Поскольку оптоволоконные каналы — высокоуровневая и дорогостоящая технология, вам не придется часто встречаться с ними. Однако сейчас стоит обратить внимание на них как на средства, родственные методам Gigabit Ethernet и конкурирующие со SCSI-интерфейсом, поскольку они позволяют физически распределить все части сети способом, наиболее удобным для пользователей, без каких бы то ни было жестких ограничений, налагаемых параметрами каналов данных.

Стандарт Token Bus (802.4)

Пытаясь разработать стандарт сети, менее склонной к конфликтам, чем не предусмотрено стандартом 802. 3, подкомитет IEEE 802. 4 разработал такое сочетание шинной и кольцевой топологий, которое обеспечивает передачу информации через кольцо, но использует для этого физическую шинную топологию. Стандарт 802. 4 разработан как результат учета того,
что компьютеры склонны к тем же недостаткам, что и люди — стоит дать им хоть малейшую возможность, как они начинают перебивать друг друга при разговоре. Рассматривая эту проблему, комитет 802. 4 представил описание эстафеты, которое сеть может использовать для решения вопроса о том, какому компьютеру следует "говорить" в данный момент. Все это содержится в стандарте 802. 4.

Только та рабочая станция, которая владеет эстафетным маркером, может посылать определенную информацию, и после того, как эта рабочая станция получит уведомление о получении этой же информации, она должна передать маркер следующей на линии рабочей станции. Как же сеть определяет, кто находится следующим на линии? Согласно стандарту 802. 4 сеть специальным образом отслеживает, кто следующий должен получить маркер. Подобно тому, как управляющий фирмы имеет большее право голоса, чем лицо, ответственное за убранство офиса, некоторые рабочие станции, могут иметь более высокий приоритет при получении маркера.

Метод разрешения конфликтов не является единственным. Чем стандарт 802. 4 отличается от стандарта 802. 3? Во-первых, несколько отличается среда передачи данных: в сети Token Bus используется либо коаксиальный кабель с волновым сопротивлением 70 Ом (в отличие от кабеля с волновым сопротивлением 50 Ом в сетях 10Base2), либо оптоволоконный кабель. Во-вторых, как вы можете заметить на рис. 2. 10, кадр сети Ethernet стандарта 802. 4 отличается от кадра стандарта 802. 3. Он содержит преамбулу, начальный разделитель кадра, управление кадром, адрес назначения, исходный адрес, данные, контрольную последовательность кадра, конечный разделитель кадра.

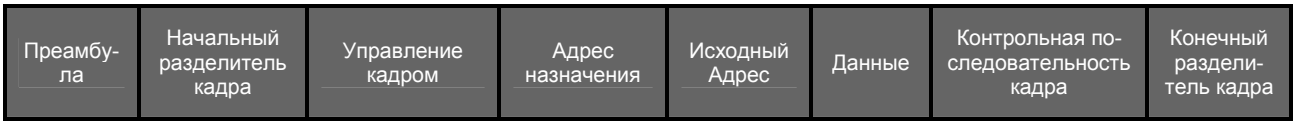


Рис 2.10. Структура кадра сети Ethernet в соответствии со стандартом 802.4

Хотя комбинация средств маркер/шина позволяет устранить конфликты, стандарт 802. 4 имеет ряд недостатков, сдерживающих его широкое распространение. Наиболее

значительные потери производительности сети с шинно-кольцевой структурой обусловлены сбоями аппаратных средств, приводящими к потере или "затенению" эстафетного маркера. В последнем случае ситуация будет выглядеть так, будто в сети существует несколько маркеров. Вообразите себе заседание правления компании, в котором одновременно говорят несколько докладчиков!

Стандарт Token Ring (802.5)

Стандарт 802. 5 разработал комитет IEEE 802. 4 в союзе с фирмой IBM. Этот стандарт специально предназначен для сетей Token Ring, использующих маркерные методы пересылки информации от одной рабочей станции к другой.

Как и в случае со стандартом 802. 4, рабочие станции в сети Token Ring, построенные в соответствии со стандартом, используют маркер для определения того, какая рабочая станция должна передавать информацию и данный момент времени. Если она ничего не должна передавать, то передаёт следующей рабочей станции свободный маркер, и этот процесс продолжается до тех пор, пока маркер не достигнет рабочей станции, которой требуется передать данные.

Данные путешествуют, начиная от исходной рабочей станции последовательно от узла к узлу сети. Каждая станция проверяет адрес, приведенный пакете данных. Если данные предназначены этой рабочей станции, она сохраняет копию данных и посылает оригинал далее. Если данные не предназначены этой станции, она просто пересылает их следующей станции в сети. Когда посылающая рабочая станция получает обратно копию исходного пакета данных, она определяет, пора ли остановить передачу и послать свободный маркер (передать эстафету) следующей рабочей станции. Этот процесс проиллюстрирован на рис. 2. 11, 2. 12 и 2. 13.

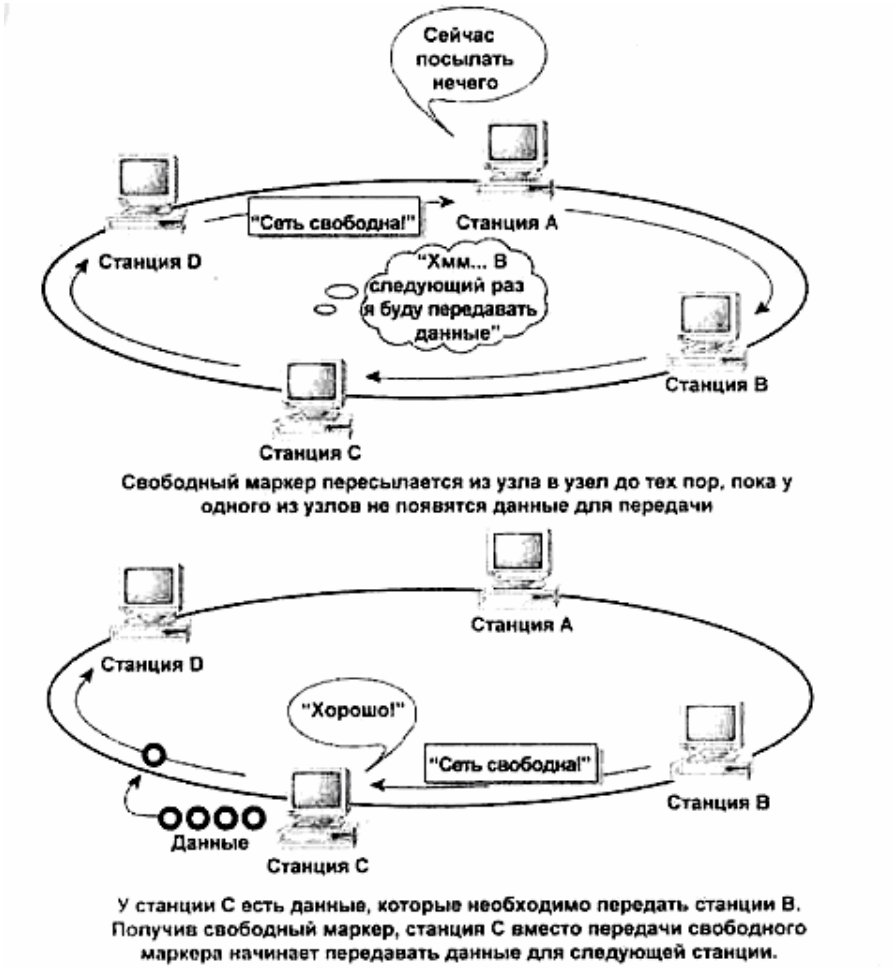
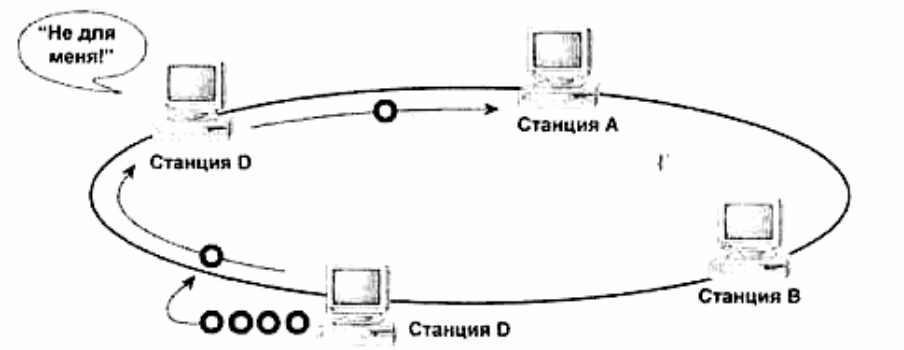
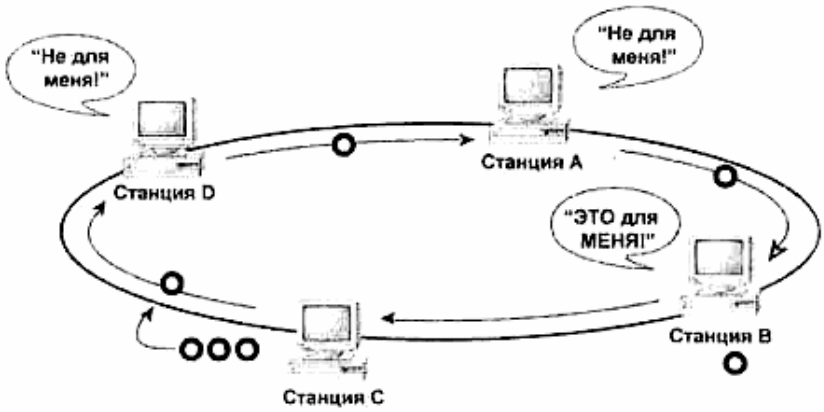


Рис. 2.11. Как осуществляется передача маркера (шаг 1)

Стандарт 802. 5 содержит несколько рекомендаций. С помощью интеллектуальных концентраторов система Token Ring может восстанавливать соединение сети при неисправностях, вызванных аппаратными сбоями — это прекрасная возможность, отсутствующая в стандарте Token Bus. Если рабочая станция неисправна и вследствие этого либо не генерирует свободный маркер после окончания "оборота" очередного маркера, либо передает неправильный маркер по сети, интеллектуальный концентратор может распознать наличие неисправности и исключить эту рабочую станцию из сети, позволяя остальной ее части нормально функционировать.



Станция D получает данные и определяет, что они предназначены не ей, поэтому она пересылает данные далее и забывает о них



Станция A, как и другие, принимает данные, замечает, что предназначены не для нее, и передает их далее. Однако станция B распознает, что адрес места назначения совпадает с ее адресом и оставляет себе копию данных. Далее вместо остановки передачи данных она продолжает пересылку данных по кольцу.

Рис. 2.12. Как осуществляется передача маркера (шаг 2)

Сеть, определенная в соответствии со стандартом 802. 5, может обеспечивать связь на большее расстояние, чем сети, построенные в соответствии со стандартами 802. 3 и 802. 4, поскольку в ней пакет путешествует от одной станции до другой и при этом ретранслируется (т. е. помимо всего прочего при этом обеспечиваются определенные амплитудные параметры передаваемого сигнала. — Прим. ред.) и, следовательно, расстояние между отдельными узлами сети может равняться предельно возможному (для данного типа кабеля).

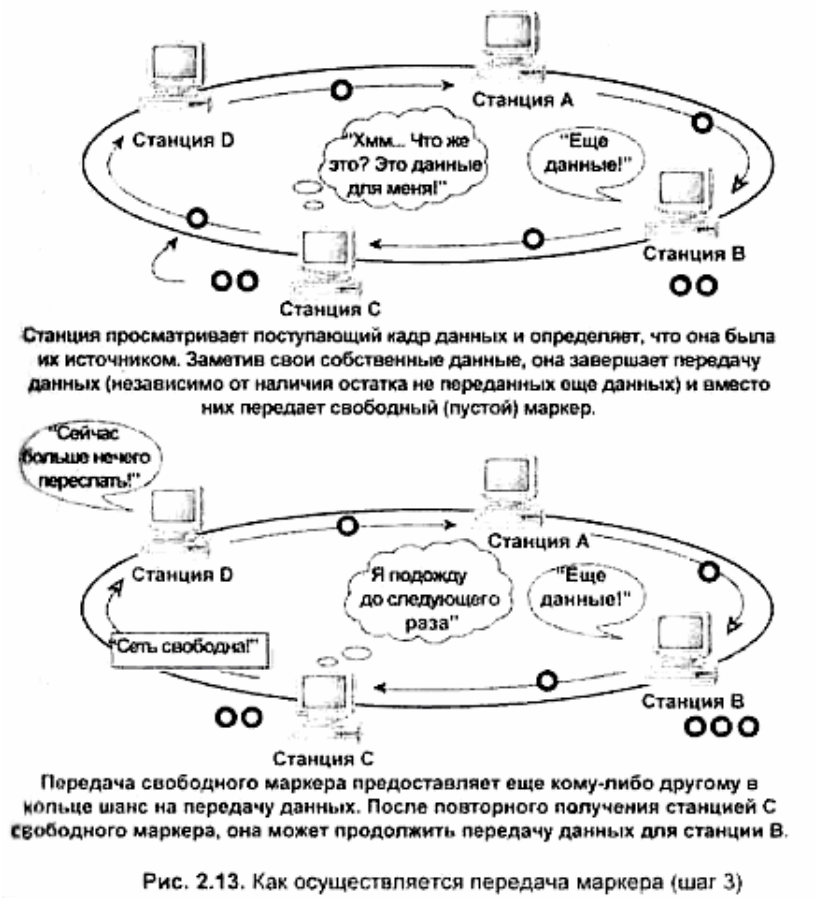


Рис. 2.13. Как осуществляется передача маркера (шаг 3)

Платы Token Ring присоединяются к устройствам MAU (Multistation Access Unit — устройство многостанционного доступа) с помощью D-разъема, установленного внутри устройства. К устройству MAU можно подсоединить восемь PC. Кроме того, одни MAU могут быть соединены с другими MAU. В сети Token Ring отсутствуют терминаторы, так как один конец кабеля подключается к плате, а другой — к устройству MAU.

Как и с помощью концентраторов, применяемых в сетях l0BaseT, используя MAU в рассматриваемых сетях вы можете легко организовать свою сеть так, что кабели будут проходить от центрального монтажного шкафа на каждый этаж, а затем и к каждому компьютеру на этаже. Кабели между устройством MAU и сетевым устройством могут быть до 45 м длиной, что достаточно для подключения кабелей к монтажным шкафам в большинстве зданий.

Хотя сеть Token Ring имеет логическую кольцевую топологию, в ней используется физическая звездообразная топология. Вместо концентраторов в Token Ring применяются устройства MAU (Multistation Access Unit — устройство многостанционного доступа). Не спутайте эти устройства MAU с *блоками доступа к среде передачи данных* (также сокращенно называемых MAU - Medium Attachment Unit), которые являются приемо-передающими соединениями с AUI-портом адаптеров Ethernet.

Выводы

Приведем краткий обзор всех типов сетей. Чаще всего вы будете использовать одну из двух логических топологий. Шинная топология, применяемая в различных реализациях сетей Ethernet, предусматривает широковещательную передачу данных по всей сети с последующим их перехватом теми сетевыми узлами, которым эти данные адресованы. В каждый момент времени передачу данных может выполнять только один узел, поэтому перед их передачей каждая станция должна "прослушать" сеть, чтобы определить, свободна она или нет. Если сеть занята, узел ждет некоторое время и снова повторяет попытку передачи. Если сеть свободна, узел передает данные и в случае, если другая станция также станет передавать свои данные в это же время, обе станции остановятся и будут ждать, пока сеть не освободится. Применение логической кольцевой топологии позволяет избежать одновременного использования канала связи двумя станциями несколько другим способом. В такой сети по кольцу пересылается пакет, называемый *эстафетой (эстафетным маркером),* причем передача данных разрешена только одной станции и только в то время, когда она контролирует маркер.

Несколько усложняет понимание функционирования сетей наличие физической шинной и кольцевой топологий. В физической шинной топологии все компьютеры подключаются к одной и той же магистрали как с помощью отводов, так и напрямую и соединяются в одну линию связи Редко используемая в сетях физическая кольцевая топология работает аналогичным образом, за исключением того, что применяется физическое кольцевое соединение, и в сети может использоваться двойной кабель для устранения сбоев при разрывах основного кабеля. В небольших офисах обычно требуется достаточно гибкий набор сетевых средств, но нет необходимости организовывать магистраль. Поэтому чаще всего физическая топология таких сетей — звездообразная, когда каждый PC подключается к центральному концентратору.

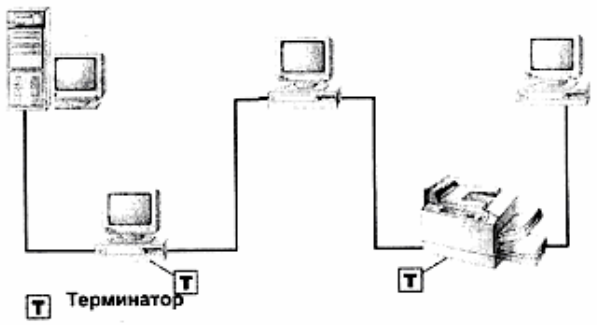
Из всех физических и логических топологий сетей, которые здесь описаны, наиболее популярна 100BaseT. Это сеть Ethernet, построенная по логической шинной топологии с применением кабеля категории 5, проложенного согласно физической звездообразной топологии, что позволяет достигнуть скоростей передачи вплоть до 100 Мбит/с. Весьма вероятно о использование в новых LAN. Популярность сетей такого типа объясняется их скоростью и гибкостью. Как уже было сказано, сети Token Ring чаще всего встречаются в локальных системах IBM, требующих подключения к мэйнфреймам, а сеть 10Base2 наиболее подходит для малых организаций. Компьютерами, установленными компактно в одном месте. Учитывайте параметры своей физической "среды обитания" при выборе топологии сети и выбирайте ту из них, которая наиболее вам подходит.

Выбор физической топологии может оказаться самой легкой частью задачи. В гл. 3 обсуждается низкоуровневое программное обеспечение, в том числе перехватчики, драйверы сетевых плат и сетевые транспортные протоколы. Если вы уже забыли, как работает модель OSI, самое время вернуться к гл. 1, поскольку далее мы углубимся в изучение связанных с этой моделью средств.

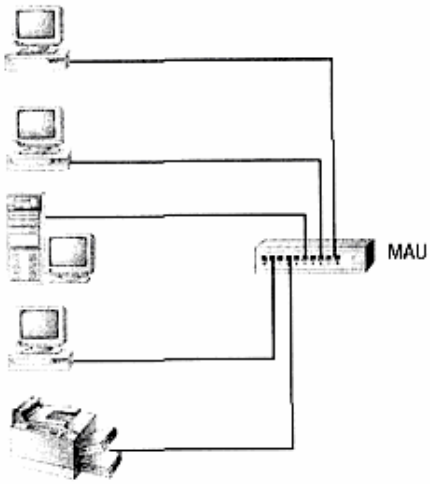
Упражнение 2

1. В случае сбоя сети, в какой из указанных ниже физических топологии будет легче диагностировать неисправность и почему? Как называется каждая из представленных здесь топологий?

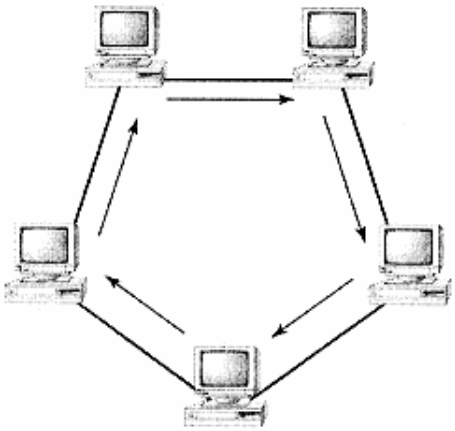
Топология 1



Топология 2



Топология 3



2. Опишите сети двух типов, упомянутых в этой главе, в которых объединены одна из физических и одна из логических топологий.
3. Какое устройство требуется для транслирования совместимых с 10Base2 кадров Ethernet в кадры, совместимые с Gigabit Ethernet?
4. В каком стандарте IEEE описана архитектура сети с топологией Token Bus?
5. Какая технология Ethernet поддерживает групповую передачу пакетов?

Глава 3

Сетевые протоколы и интерфейсы прикладных программ

Чтобы передать по локальной сети (LAN) данные из пункта А в пункт к, необходимо не только оборудование (гл. 1), организованное в одну из конфигураций (гл. 2), но и сетевое программное обеспечение, которое должно собрать передаваемые данные в пакет. Сетевое программное обеспечение состоит из трех частей:

- редиректор (redirector), отсылающий запросы в сеть, а не на локальный жесткий диск;
- драйверы сетевых плат, обеспечивающие связь между операционной системой и сетевой платой;
- сетевые протоколы для отсылки и приема данных.

Такой способ организации передачи информации показан на рис. 3. 1.

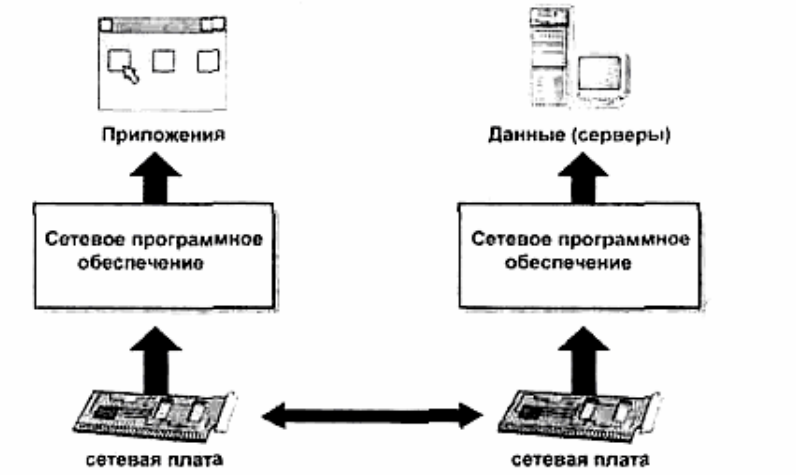


Рис. 3.1. Использование сети предоставляет пользователям возможность централизованного хранения данных

Так, например, в случае, когда Фрэд пытается сохранить файл WordCruncher со своего компьютера на общем жестком диске сетевого файлового сервера, происходит следующее.

1. Фрэд щелкает на кнопке **Save (Сохранить)** и выбирает опции сохранения документа на диске G:, который фактически является сетевым общим диском D: файлового сервера.
2. Редиректор проверяет этот запрос на сохранение, фиксирует локальную недоступность диска и направляет запрос в раздел операционной системы, называемый *драйвером сетевой файловой системы.*
3. Драйвер сетевой файловой системы передает запрос драйверу сетевой платы.
4. Драйвер сетевой платы передает запрос (вместе с данными) сетевой плате.

5. Сетевая плата создает пакет данных для передачи и отсылает его по сети.
6. Сетевая плата файлового сервера отмечает факт прибытия пакета и принимает его.

Далее процессы идут в обратном направлении: драйвер сетевой платы сервера передает запрос драйверу файловой системы операционной системы и записывает файл на локальный диск.

Если вы организуете сеть, то весьма вероятно, что рано или поздно вам понадобится соединить ее с другой сетью. Именно так и зародилась Internet: локальные сети получили средства соединения друг с другом в единое целое. Большинство сетей растут постепенно, а не создаются сразу в окончательном виде. Часто сети состоят из оборудования, сетевых операционных систем и линий связи смешанных типов. Это, в свою очередь, означает, что в сетях необходимо использовать редиректоры разных типов и устанавливать несколько сетевых протоколов. Кроме того, сетевые платы могут использовать разные драйверы. Короче говоря, даже при самом тщательном планировании, рост и слияние сетей представляют собой достаточно сложный процесс. В этой главе рассматриваются различные сетевые компоненты. Ознакомившись с ними, вы сможете управлять сетевым программным обеспечением, когда это потребуется.

Прежде всего, мы обсудим роль редиректора — он должен обеспечить связи между приложениями и операционной системой, необходимые для получения приложением данных через сеть. Затем рассмотрим назначение драйвера сетевой платы. И, наконец, изучим три транспортных протокола, которые чаще всего используются в сетях персональных компьютеров.

Назначение и работа редиректора

Как показано на рис. 3.2, с точки зрения компьютера, инициализирующего запрос по сети, редиректор играет главную роль в создании сетевого соединения. Его задача – «обманным» путём заставить приложение на локальной машине полагать, что оно получает данные с локального, а не сетевого диска. Суть применения редиректора: место хранения запрошенного файла не должно иметь значения, так как метод доступа должен быть единым.

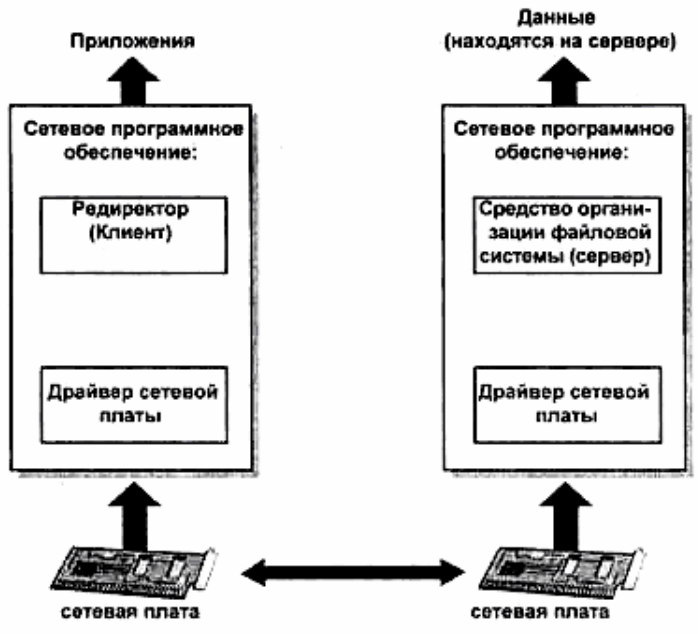


Рис. 3.2. Место редиректора в сети

Например, что случится, если вы запустите программу WordCruncher и откроете файл, хранящийся на сетевом диске? С точки зрения WordCruncher ни *не существует.* Она знает только о существовании нескольких доступных дисков с именами, состоящими из букв с двоеточиями, например, F:, B:, C: и т. д. Как и любое другое приложение, WordCruncher способна использовать только локальные устройства хранения. Таким образом, необходимо задействовать тот уровень программного обеспечения (расположенный непосредственно под уровнем WordCruncher), задача которого заключается в предоставлении WordCruncher обычного интерфейса, основанного на буквенных обозначениях дисков (common drive-letter interface). Но делать это необходимо и в случае, когда приложению требуются данные, хранящиеся в сетевом устройстве. WordCruncher полагает, что она обращается к локальным дискам, однако ее запросы информации с сетевых дисков должны *перехватываться* и направляться по сети. Итак, если вы скомандуете WordCruncher получить данные из каталога DOCS, находящегося на сервере с именем BGDOG, программа редиректора передаст запрос так, как описано в самом начале главы.

Примечание

Редиректоры нередко называют *клиентами* (например, клиент Windows 98 для сетей NetWare), поскольку они обязательно входят в состав программного обеспечения клиентного компьютера.

Следовательно, прежде чем вы сможете подключиться к сети, вы должны установить редиректор, соответствующий типу сети. Отнюдь не *во* всех сетевых операционных системах используют одинаковые редиректоры. Поэтому вы должны установить редиректор, соответствующий операционной системе той сети, к которой подсоединяетесь. Различие между редиректорами может быть обнаружено на уровне представления данных модели OSI, (гл. 1). Так, в сетях Microsoft для передачи данных используют блоки сообщений сервера (Server Message Blocks — SMBs). Поэтому для них необходим редиректор, способный выразить запросы в терминах SMBs. В сетях Novell с этой же целью применяют программу NetWare Control Protocols (NCPs). Таким образом, чтобы запросить сервер NetWare, вы должны использовать редиректор, который может выразить запрос в терминах NCPs. Обратите внимание: недостаточно применить общий транспортный протокол, такой как TCP/IP — вы должны использовать редиректор, работающий с той операционной системой, к которой вы подсоединяетесь. К счастью, если на уровне представления данных задействован протокол, одинаковый для нескольких операционных систем, поддержка редиректора обеспечивается автоматически. Так, если вы работаете в Windows 98, то можете использовать Client for Microsoft Networks (Клиент сетей Microsoft), поддерживающий SMB, чтобы подключиться к любой операционной системе, поддерживающей SMBs.

Редиректоры и средства API

Как указано во введении в эту главу, большинство пользовательских приложений "не подозревают" о наличии используемой сети (сетей). Однако некоторые приложения, например, электронная почта или групповое программное обеспечение *должны* быть "осведомлены" о наличии сети, поскольку они вообще нужны *только для* работы в сети, должны быть способны "подключаться" к ней и устанавливать связь с другими программами, которые исполняются сетевыми машинами.

Программисты разрабатывают приложения, способные определять наличие сети таким образом, чтобы они воспринимали набор команд, предоставляемый сетью

приложениям. Эти наборы команд называют средствами API или *интерфейсами прикладных программ.* API можно представить чем-то вроде комбинации органов управления и приборов автомобиля. Комбинация приборов вашего автомобиля — видимая часть интерфейса, предназначенного для управления автомобилем. Фактически, вы не представляете, что творится под капотом — просто нажимаете педаль газа, и автомобиль разгоняется.

Таким образом, вам нет необходимости детально знать устройство автомобиля, чтобы ездить на нем. Более того, если вы умеете управлять одним автомобилем, вы справитесь и с другим, поскольку его элементы управления — т. е. API — везде одинаковы.(Однажды вечером, во время поездки на "Фольксвагене" моего друга, я узнала, что в разных автомобилях этой марки используются разные "API" для заднего хода. Это часто бывает в автомобилях с ручным переключением передач, но в целом наша аналогия верна.)Комбинация органов управления автомобилем позволяет передать только несколько простейших команд: торможение, ускорение, переключение скоростей и т. д. Например, нельзя дать команду "выехать задним ходом на дорогу". Вы должны отдать множество простейших команд, чтобы выполнить *фактическое* действие: выехать задним ходом на дорогу. В известном смысле необходимо создать программу с помощью стандартной комбинации органов управления, расположенных в некотором порядке.

Функции API вашего компьютера во многом работают точно так же. Сетевые программные средства, подобные редиректору, должны находиться на верхнем уровне различных транспортных протоколов. Если бы не было API, программистам сетевого программного обеспечения пришлось бы разработать одну программу-редиректор для подключения Windows NT (сетевая операционная система) к IPX/SPX, а другую программу-редиректор — для подключения Windows NT к TCP/IP. Структурно редиректор будет один и тот же. Просто он будет в состоянии "разговаривать" I разными транспортными протоколами. Чтобы избежать этого, следует видать общую комбинацию органов управления и приборов для всех сетевых служб. Таким образом, программа-редиректор встроена не в протокол, а в API (в нашем примере - в NetBIOS). NetBIOS может "сидеть" на верхнем уровне протоколов IPX/SPX, NetBEUI и TCP/IP. Это означает, что транспортный протокол может изменяться, однако вам нет нужды переписывать сетевые утилиты, поскольку они написаны для API (NetBIOS).Широко известным примером API служат *гнезда* (sockets) — временные каналы связи, установленные для передачи информации между клиентной серверной программами. Данные программы могут работать как на одной машине, так и на разных машинах через сеть. Существуют три API, с которыми вы, вероятно, уже сталкивались.

- Гнезда Novell.
- NetBIOS.
- Гнезда TCP/IP.

API перехватывают ваши сетевые запросы и выполняют поставленную задачу с помощью соответствующего транспортного протокола.

Драйверы файловых систем

Редиректор расположен на том конце соединения, которое создает (генерирует) запрос. Другая часть, расположенная на том конце соединения, на котором *выполняется* за-

прос, — драйвер файловой системы. Драйверы файловых систем используют для генерирования не только сетевых, но и любых других запросов на доступ к устройству хранения данных. Например, в Windows NT функции драйвера сетевой файловой системы может выполнять одна из поддерживаемых файловых систем: FAT, NTFS, CDFS и сеть.

Примечание

FAT - это таблица размещения файлов, первоначально предназначавшаяся для работы с гибкими дисками (дискетами) и допускавшая работу с жесткими дисками объемом не более 4 Гбайт. NTFS (NT File System) - файловая система, использующаяся в Windows NT. В ней предусмотрена поддержка дисков больших объемов и средства защиты, отсутствующие в FAT. В приводах CD-ROM персональных компьютеров применяют файловую систему CDFS (Compact Disc File System).

В целом же роль *любого* драйвера файловой системы заключается и упорядочивании данных в устройстве хранения, которое он обслуживает. Так, в популярной дисковой файловой системе FAT, нумеруется каждый кластер и указывается, какой файл в нем сохраняется. Если для хранения данных, содержащихся в файле, необходимо несколько кластеров, в каждый кластер включают указатель на следующий кластер диска, хранящий данные из этого же файла. В последний кластер включается метка End of File (конец файла), которая позволяет файловой системе FAT "узнать" что файл закончился. А как файловая система "узнает", где находится кластер? Когда вы форматируете диск, то разбиваете его на кластеры с помощью специальной программы.

Когда вы предписываете программе найти файл, файловая система FAT предоставляет ей все необходимые данные и гарантирует их полное извлечение (поскольку весьма вероятно, что данные разбросаны по разным кластерам). Точно так же, когда вы пытаетесь сохранить файл на диске, файловая система FAT позволяет найти на нем первый свободный кластер и начать записывать данные, составляющие этот файл, в свободных кластерах, помечая каждый кластер так, чтобы он указывал на следующий занятый данным файлом кластер.

Примечание

В зависимости от структуры доступного дискового пространства свободные кластеры могут и не составлять непрерывный блок. Файловая система не ищет первую группу свободных кластеров, общий размер которой достаточен для хранения всего файла в целом, а находит только первый свободный кластер. Если файл мм помещается в него полностью, то остальные данные будут последовательно записываться в следующие свободные кластеры, в каком бы месте диска они не находились.

Геометрия диска

Вы уже сбиты с толку этими разговорами о кластерах и сохранении и них данных? Суть файловой системы проста: в файловых системах Microsoft кластером называют наименьшую возможную логическую единит предназначенную для хранения данных. Поверхность диска разделена на концентрические круги, называемые *дорожками* (tracks), а они, в свою очередь, разделены на клиновидные участки (напоминающие нарезанный пирог), называемые *секторами.* Сектор — наименьшая единица хранения вместимостью 512 байт.

Кластерами называют логические группы секторов. Точное число секторов в кластере зависит от используемой файловой системы и размера диска. Чём больше емкость диска, тем больше общее количество кластеров в файловой системе, хотя в современных файловых системах и наблюдается тенденция к снижению количества кластеров.

Использование более крупных кластеров позволяет снизить время доступа к диску, поскольку в крупном кластере можно сохранить больше данных, причем в одном месте на диске. С другой стороны, использование крупных кластеров при сохранении небольших файлов ведет к бесполезной трате дискового пространства, поскольку короткий файл все равно занимает весь кластер полностью. Так, если на диске хранится файл длиной 4 Кбайта, а размер кластера данного диска составляет 8 Кбайт, то оставшиеся незанятыми 4 Кбайта будут потеряны, поскольку они не могут использоваться для хранения других данных.

Сетевая файловая система представляет собой всего лишь еще один интерфейс для чтения дискового пространства. Единственное ее отличие от других файловых систем заключается в том, что она используется для сетевого, а не локального доступа. Таким образом, когда сервер получает от какого-нибудь клиента сети запрос на доступ к диску, он направляется в сетевую файловую систему, которая и выполняет то, что обязана — находит данные, сохраняет файл или что-либо еще. Достоинство ее состоит в том, что сетевая файловая система позволяет клиенту не беспокоиться о формате жёсткого диска сервера. Даже если файловая система, в которой был отформатирован сетевой диск, не поддерживается клиентным программным обеспечением, это никак не сказывается на работе локального приложения, поскольку для выполнения сетевых запросов локальная файловая система не используется. Пока клиент "разговаривает" с сервером, тот будет интерпретировать для клиента свою файловую систему.

Драйверы сетевых плат

Теперь вы знаете, каким образом запрос поступает от приложения в операционную систему и выполняется ею. Как же этот запрос поступает в сеть? Эту задачу выполняет часть программного обеспечения, называемая *драйвером сетевой платы.*

Вообще говоря, любой драйвер устройства представляет собой часть программного обеспечения, позволяющего операционной системе и физическому устройству взаимодействовать друг с другом. Некоторые драйверы устройств входят в состав файлов операционной системы. Другие же можно загрузить с диска или Internet, однако они в любом случае остаются интерфейсом между сетевой платой и операционной системой.

Почему же нельзя просто встроить функциональные средства, необходимые сетевой плате, непосредственно в операционную систему, особенно, если учесть, что современные операционные системы создаются с учетом возможности работы в сети? Главным образом потому, что это непрактично. Десятки и даже сотни производителей предлагают тысячи моделей сетевых плат, причем в каждой модели используют собственный драйвер. По этой причине просто невозможно встраивать в операционную систему функции поддержки всех сетевых плат. И даже если бы эта схема имела практический смысл, она была бы нежелательна. В этом случае операционная система занимала бы слишком много места, намного больше *реально* необходимого. Если вы установили единственную сетевую плату, остальные драйверы вам не нужны. И более того: обновление драйверов для улучшения поддержки оборудования потребовало бы замены операционной системы. Разве вам понравится переустанавливать операционную систему при каждом обновлении драйвера сетевой платы? Не думаю.

Кстати сказать, в некоторых операционных системах используют модульную конструкцию, позволяющую в нее включить определенные функции драйвера. Подразумевается, что производителям оборудования нужно будет только дописать оставшуюся часть программы (stub portion) драйвера. Идея такого подхода такова (рис. 3. 3): хотя каждая сетевая плата может управлять передачей данных между операционной системой и сетью методом несколько отличным от используемых в других платах, основная функция сетевой платы неизменна в любом случае. Таким образом, эту функцию действительно можно встроить в операционную систему. С этой точки зрения создателю драйвера сетевой платы достаточно написать инструкции специфичные для данной платы, которые позволят плате получать доступ к функциональным средствам, встроенным в операционную систему.

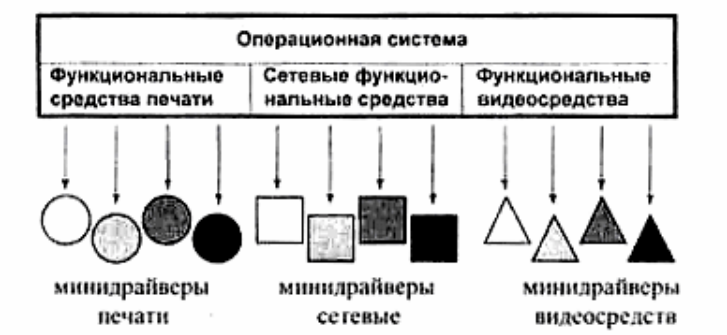


Рис. 3.3. Взаимодействие микродрайверов с операционной систем

На этом мы завершим обсуждение общих вопросов, связанных с драйверами операционной системы, и приступим к основному — работе этих драйверов.

Что делают драйверы сетевых плат

Драйверы сетевых плат (сетевые драйверы) отвечают за управление всеми внешними связями компьютера, в том числе и доступом в Internet для каждой используемой модели сетевой платы необходимо установить соответствующий сетевой драйвер. Так, если в состав персонального компьютера входит кабельный модем для подключения к Internet, а также сетевое оборудование, то ему необходимы дна драйвера. Если в компьютере установлено несколько сетевых плат разного типа (например, он используется в качестве маршрутизатора), то для каждой платы также следует установить собственный драйвер. Однако если в компьютере есть две одинаковые платы, достаточно поставить единственный драйвер. По существу, драйверы обеспечивают сетевое соединение компьютеров на канальном уровне, позволяя, например, получать доступ к сетям Ethernet.

Интерфейсы сетевых компоновок

В принципе, возможно создать сетевой драйвер, который сможет посылать Винные как на сетевую плату, так и в сеть. По сути, он будет объединять собственно драйвер и средства поддержки сетевого протокола. Драйверы такого типа называют *монолитными драйверами устройств.*

Обратите внимание: я сказала *"возможно"*. Этот подход не рекомендуется во многом по тем же причинам, что и встраивание драйверов устройств в операционную систему.

Гибкость обеспечивается только модульным подходом. Предположим, в драйвер вашей сетевой платы включены средства поддержки транспортного протокола. В этом случае, чтобы заменить или добавить еще один транспортный протокол, придется заменить драйвер. Такой подход неудобен, поскольку поддерживает только единственный транспортный протокол.

Поэтому вместо монолитных драйверов устройств в современных драйверах для "привязки" сетевых плат к транспортным протоколам используют мой инструмент — *интерфейс сетевых компоновок.* Как показано на рис. 3.4, — это интерфейс между драйвером сетевой платы и стеком транспортных протоколов (transport stack).

Примечание

Интерфейс сетевых компоновок - именно то средство, которое обеспечивает "увязку" протокола с сетевой платой. Это, в сущности, "свадьба" драйвера сетевой платы с сетевым транспортным протоколом.

Принцип его применения совершенно очевиден. Интерфейс сетевых компоновок связывает каждый установленный драйвер с каждым установленным транспортным протоколом. Названия этих связей (clump) зависят от типа сети. Так, в сетях NetWare их называют модулями. Обменом данных модулями управляет программа, которую называют LAS в сетях NetWare и PROTMAN. SYS в Microsoft. Вся информация, необходимая интерфейсу компоновок, сохраняется в текстовом файле, таком как PROTOCOL.INI в сетях Microsoft или NET.CFG в NetWare. Однако, если в драйверах используют стандартные значения параметров, то в этих файлах содержится совсем немного информации.

Рис. 3.4. Интерфейс сетевых компоновок позволяет нескольким протоколам связываться с единственным драйвером

Связующие нити

Как указано выше, основное преимущество использования интерфейс сетевых компоновок — возможность использования каждым сетевым драйвером нескольких транспортных протоколов. По умолчанию все сетевые транспортные протоколы "привязываются" ко всем установленным драйверам сетевых плат. Какой же протокол используется при отсылке данных по сети? Ответ зависит от порядка, в котором "привязывались" транспортные протоколы. Этот порядок можно изменять, поставив на первое место протокол, используемый чаще остальных. Это позволит уменьшить число повторных попыток его поиска, что необходимо для доступа к конкретному серверу.

Если же необходимо запретить доступ к серверу, использующему конкретный протокол, достаточно просто удалить его из списка протоколов, "привязанных" (bound) к сетевой плате. Запутались? Хорошо. Если вы запутались сейчас, но этот вопрос все же вас интересует, знайте, что я вернусь к нему в гл. 15 "Защита сетей".

Звание "законодателя мод" в мире стандартов интерфейса сетевых компоновок оспаривают два конкурента: открытый интерфейс передачи данных (ODI) фирмы Novell и спецификация интерфейсов сетевых драйверов (NDIS) фирмы Microsoft. Принцип работы обоих интерфейсов во многом сходен. Основное различие в том, что драйверы ODI работают в реальном (незащищенном) режиме. Значит они должны использовать первые 640 Кбайт памяти, установленной на машине, и не могут "договариваться" другими драйверами. Напротив, драйверы NDIS функционируют в защищенном режиме и поэтому могут работать в многозадачном режиме вместе с прочими драйверами. Кроме того, они *не используют* дефицитную обычную память.

Зачем же применяют драйверы ODI, если они не работают в защищенном режиме? Главным образом потому, что иногда они необходимы редиректору. Отнюдь не все редиректоры могут работать с драйверами NDIS. Чтобы рассеять сомнения, поднимите документацию на вашу операционную систему и ознакомьтесь с требованиями к редиректору. Вообще же говоря, как NDIS, так и ODI работают со всеми транспортными протоколами, а ограничения налагаются, в основном, со стороны драйвера.

Сетевые транспортные протоколы

На протяжении всей главы я постоянно упоминала транспортные протоколы, фактически не пояснив, что же это такое. Во-первых, *что такое* протокол вообще? Проще всего представить протокол как стандарт или правил.

С протоколами часто приходится иметь дело в повседневной жизни. Например, если в вашей квартире зазвонил телефон, вы снимаете трубку и говорите: "Алло?". Почему *вы* сначала сказали "Алло"? Почему вызывающая сторона, прежде всего не идентифицировала себя? Да просто таков обычай. По традиции, в Соединенных Штатах первым отвечает вызываемое лицо. Иными словами, таков американский *протокол* ответа по телефону. Если бы вы жили в материковом Китае, вы подняли бы трубку и ожидали, когда вызывающая сторона скажет "Вэй" (Wei), чтобы обозначить себя. Что вы делаете, встретив знакомого: обнимаете, целуете, пожимаете руку? Опять же, ответ зависит от протокола.

Какое отношение все это имеет к сетям? Сетевые транспортные протоколы определяют метод передачи данных по сети, а также метод их пакетирования и адресации. Чтобы два сетевых компьютера могли установить связь, они должны использовать одинаковые транспортные протоколы, поскольку протокол определяет метод пакетирования и обмена данными.

Примечание

С технической точки зрения к протоколам можно отнести *любое* соглашение, задающее метод передачи данных через сеть, независимо от того, функционирует ли это соглашение на канальном или прикладном уровнях. Однако нередко протоколами называют соглашения, которые задают метод пакетирования и передачи данных по сети. Именно это я буду иметь в виду в дальнейшем. Протоколы NetBEUI, IPX/SPX и TCP/IP работают на сетевом и транспортном уровнях модели OSI. Поскольку они работают на нескольких уровнях, их нередко называют *стеками протоколов, а* не просто протоколами.

Современные операционные системы могут одновременно поддерживать несколько протоколов, поэтому вы всегда можете использовать для установления связи протокол нужного типа. К сожалению, *не все* операционные системы поддерживают *все* транспортные протоколы. Фактически они "склонны" к специализации, и даже некоторые протоколы с одинаковыми именами невозможно использовать на всех платформах. Однако в настоящее время возможности операционных систем в достаточной мере перекрываются, что допускает связь и взаимодействие между ними.

Совет

Использование нескольких транспортных протоколов дополнительно загружает оперативную память (RAM). Поэтому, хотя современные операционные системы позволяют загружать несколько транспортных протоколов, рекомендуем выбрать только те, которые действительно необходимы.

Предупреждаю: последующие разделы следует рассматривать как введение в три основных протокола сетей персональных компьютеров. Протокол TCP/IP чрезвычайно сложен, в нем предусмотрены многочисленные параметры конфигурирования, достойные отдельной книги или даже нескольких. То, что приведено здесь, должно просто помочь вам получить общее представление о работе каждого протокола и всего, что с ним связано.

Протокол NetBEUI

Давным-давно, когда IBM только вышла на рынок сетей персональных компьютеров, ей понадобился базовый сетевой протокол. Фирма не собиралась создавать крупные сети, а предусматривала организовывать небольшие рабочие группы, не более нескольких дюжин компьютеров.

Исходя из такой задачи и была разработана базовая сетевая системе ввода-вывода — NetBIOS. Она представляет собой набор из 18 команд, которые позволяют создавать, поддерживать и использовать соединения между сетевыми компьютерами. Вскоре IBM дополнила NetBIOS, создав расширенный пользовательский интерфейс среды NetBIOS — NetBEUI. По существу NetBEUI — усовершенствованный вариант NetBIOS. Однако со временем имена NetBEUI и NetBIOS приобрели разный смысл. NetBEUI обозначает транспортный протокол, в то время как NetBIOS — набор программных команд, используемых системой для управления сетью (фактически это — API). Обращаясь к модели OSI, можно отметить, что NetBIOS работает на сеансовом уровне, в то время как NetBEUI — на сетевом транспортном.

NetBEUI относится к числу наиболее скоростных протоколов (с точки зрения скорости пакетирования данных для передачи и извлечения их получателем из пакета). Кроме

того, он прост в установке: вы устанавливаете протокол, "привязываете" его к сетевому драйверу и можете приступать к работе. Не требуется никакого конфигурирования, а в качестве адресов компьютеров используются присвоенные вами же имена компьютеров, которые нетрудно запомнить.

Примечание

Имена компьютеров в сетях, использующих протокол NetBEUI, фактически представляют собой имена NetBIOS. Длина имен не должна превышать 16 символов, а регистр не имеет значения.

Применение NetBEUI ограничивает серьезная проблема: этот протокол не поддерживает маршрутизацию. Иными словами, если ваша сеть состоит из нескольких сегментов, то вы не сможете использовать его для передачи данных за пределы локального сегмента. Кроме того, он поддерживается только операционными системами Microsoft и OS/2, и если вы планируете связываться с файловым сервером, работающим под управлением UNIX или сервером печати NetWare, то потерпите фиаско.

В настоящее время использование NetBEUI ограничено. Быстродействие протокола TCP/IP возросло, так что NetBEUI потерял былое преимущество в производительности. В связи с повсеместным распространением Internet, вам непременно следует использовать TCP/IP — основной протокол этой сети. И даже несмотря на то, что некоторые приложения NetBIOS требуют поддержки протокола NetBEUI, в настоящее время с тем же успехом можно использовать NetBIOS "поверх" (over) протокола IP.

В целом же протокол NetBEUI нельзя назвать совсем бесполезным, но применимость его ограничена небольшими сетями, состоящими из единственного о узла, которым не нужна связь с Internet и другими сетями.

Протокол IPX/SPX

Транспортный протокол IPX/SPX— интеллектуальная собственность фирмы Novell. Фактически он состоит из двух протоколов: IPX и SPX. IPX (Internet Package Exchange - межсетевой обмен пакетами) - протокол сетевого уровня, не ориентированный на установление соединения (connectionless). Он отвечает за поиск наилучшего пути передачи пакетов к месту назначения и за отбор их по прибытии, управляет адресацией и маршрутизацией пакетов. Таким образом, на уровне IPX назначают логические сетевые адреса (в отличие от адресов аппаратных средств, которые используют на канальном уровне и "зашиты" изготовителями в сетевые платы). IPX-адрес состоит из четырехбайтового (32-битового) сетевого номера и шестибайтового (48-битового) узлового номера.

Что означают эти номера? *Сетевой номер,* называемый также *внешним сетевым адресом,* идентифицирует физический сегмент, к которому *подключен* компьютер. Если в сегмент входят несколько серверов, они должны использовать единый внешний адрес.

Примечание

Внешние сетевые адреса присваивают только серверам NetWare. Клиентные машины сетей NetWare наследуют эти адреса от серверов, с которыми устанавливают связь.

Узловой номер, или *внутренний сетевой адрес* — это обычно адрес аппаратных средств сетевой платы компьютера, что очень удобно, поскольку избавляет от необходимости транслировать имена, назначенные программными средствами (software-assigned names) в имена аппаратных средств. При установке сервера Novell NetWare вам предлагают принять или заменить внутренний номер IPX. Затем этот номер становится иден-

тификационным номером (ID) данного сервера. Если на рабочей станции ввести команду `slist`, то вы увидите список ID для каждого перечисленного сервера.

На рис. 3. 5 показан формат полного IPS-адреса сети NetWare.

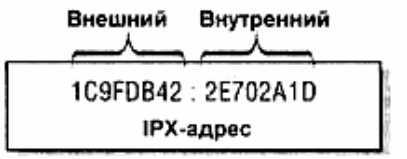


Рис. 3.5. Логический адрес NetWare

Совет

Если вам необходимо поддерживать NetBIOS, вы можете задействовать поддержку NetBIOS "поверх" IPX/SPX.

Обратите внимание: протокол IPX управляет *маршрутизацией.* Иными словами, протокол IPX/SPX, в отличие от NetBEUI, относится к маршрутизируемым протоколам. Поэтому с его помощью можно соединять сегменты сети, разделенные маршрутизаторами. Чтобы найти наилучший путь, каждые 60 с в сети с протоколом IPX (средствами протокола RIP (Routing Information Protocol — обмен информации о маршрутизации) или NLSP (NetWare Link Service Protocol — обслуживание каналов NetWare)) передается широковещательный запрос (broadcast), т. е. посылается в предполагаемое место по всем известным каналам. После этого возвращается своеобразное "эхо". По времени задержки эхо-сигнала определяется кратчайший путь, ведущий в заданное место. Подобный метод имеет единственный недостаток: протокол IPX/SPX слишком "шумный" — постоянно обновляя текущие маршруты данных, оборудование генерирует значительный сетевой трафик. Подробнее маршрутизация рассматривается в гл. 5 "Дополнительное сетевое оборудование".

Поскольку IPX не поддерживает обработку ошибок, в некоторых случаях он дополняется средствами протокола SPX (Sequenced Package Exchange - последовательный обмен пакетами). Этот протокол транспортного уровня ориентирован на установление соединений. Он гарантирует установление надёжного соединения перед отправлением данных по сети.

Поскольку протокол SPX обеспечивает корректность работы соединения, то отвечает за обработку искаженных пакетов и других ошибок. Его основные функции заключаются в вычислениях в среде пар клиент/сервер, которым необходима связь, исключающая ошибки.

Протоколы IPX и SPX являются собственностью фирмы Novel, но благодаря протоколам, совместимым с IPX/SPX, их применение не ограничено сетями NetWare. Аналогичные протоколы отличаются от исходного, но могут устанавливать с ним связь. Эти совместимые протоколы позволяют сетям Microsoft устанавливать связь с сетями NetWare, хотя в них и не используется общий транспортный протокола. Протоколы NetWare IP и TCP/IP фирмы Microsoft друг с другом не совместимы.

Протокол TCP/IP

TCP/IP разработан ARPANET (Сеть перспективных исследований и разработок) по заказу министерства обороны США. Предназначен для соединения сетей с разнородным оборудованием, скажем, систем Sun с мэйнфреймами, а мэйнфреймов — с персональными компьютерами. Каждая половина имени протокола "TCP/IP" означает его ориентированность на решение собственной задачи.

Примечание

Строго говоря, TCP/IP состоит не из двух частей - фактически это набор из нескольких протоколов. Однако аббревиатуры IP и TCP известны лучше всех, так что здесь мы и остановимся на них.

Протокол Internet (IP — Internet Protocol) работает на сетевом уровне, предоставляя различным сетям стандартный набор правил и спецификаций для межсетевой пакетной маршрутизации с помощью IP-адресов. Протокол IP позволяет устанавливать связь, как между локальными сетями, так и между отдельными компьютерами. С другой стороны, протокол управления передачей данных (TCP — Transmission Control Protocol) работает на транспортном уровне модели OSI. Он обеспечивает прием сетевой информации и трансляцию ее в форму, "понятную" сети, и таким образом организует взаимодействие процессов между двумя компьютерами или клиентами. IP можно представить себе как часть, задающую правила установления связи, а TCP – как часть, отвечающую за интерпретацию данных.

Вы можете сами оценить работу TCP/IP по тем задачам, которые он решает. Это - транспортный протокол Internet, системы, соединяющей тысячи отдельных компьютеров и сетей по всей планете. Хотя TCP/IP первоначально предназначался для использования университетами и армией, он стал самым популярным протоколом и офисных приложений, так как позволяет соединять локальные сети, UNIX-машины, миникомпьютеры DEC VAX, а также и множество компьютеров иных типов.

Что происходит, если удаленный компьютер Macintosh отсылает данные на персональный компьютер главного офиса? Во-первых, средства протокола TCP обеспечивают установление связи, гарантирующей дуплексный контроль ошибок (контроль ошибок данных в обоих направлениях) между обеими платформами. Во-вторых, IP задает правила установления связи и обеспечивает соединение портов компьютеров. К этому времени в соответствии с TCP подготавливаются данные. Соответствующая программа забирает их, разделяет на меньшие части, если их объем слишком велик, и вставляет в пакет новый заголовок ("адрес пересылки"), чтобы гарантировать правильную доставку пакета. Кроме того, в пакете указывается тип содержащихся данных и их объем. Затем пакет конвертируется в стандартный зашифрованный формат и передается на персональный компьютер главного офиса. Наконец, программа, установленная на персональном компьютере и главном офисе, транслирует шифрованный пакет в собственный формат и соответствии с TCP. Этот процесс показан на рис. 3.6.

Во многих сетях, разбросанных по всему миру, протокол TCP/IP используется как стандартный. Это — единственное средство коммуникации, позволяющее связываться рабочим станциям всех типов — PC, Macintosh, UNIX. Кроме того, он необходим для выхода в Internet. TCP/IP работает несколько медленнее NetBEUI, однако издержки производительности компенсируются широкой поддержкой протокола. И действительно, лучше работать несколько медленнее, но иметь возможность связаться со всем миром, чем быстрее, но в пределах небольшой рабочей группы.

Требования к конфигурированию TCP/IP

Один из недостатков протокола TCP/IP состоит в трудности его установки неопытными пользователями, поскольку необходимо задать множество адресов и серверов. Как указывалось ранее, установка адресов протоколов NetBEUI и IPX/SPX не встречает затруднений. При использовании NetBEUI вы назначаете имя компьютера, а при IPX/SPX — идентификатор сети (network identifier) и позволяете системе назначить собственный идентификатор узла (node identifier), основываясь на адресе аппаратных средств

сетевой платы компьютера. Однако протокол TCP/IP требует указания множества адресов, а именно:

- локальный IP-адрес;
- IP-адрес сервера DNS (Domain Name Service — служба имен домена), который транслирует легко запоминаемые человеком адреса, например, computer.company.com, в IP-адреса;
- в сетях Windows NT, использующих имена NetBIOS для идентификации компьютеров, следует указать IP-адрес сервера WINS (Windows Internet Name Service — система присвоения имен Internet для Windows), который транслирует имена NetBIOS в IP-адреса;

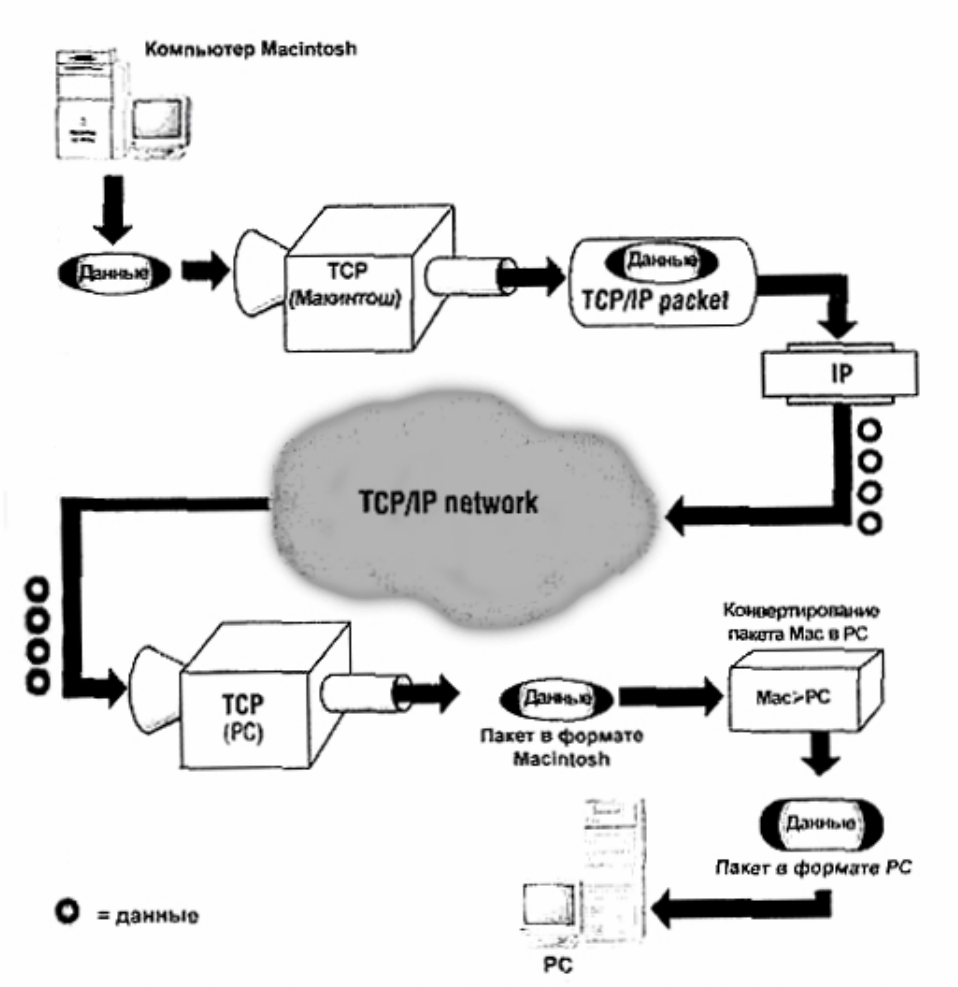


Рис. 3.6. Пересылка пакета с компьютера Macintosh на PC по протоколу TCP/IP

- шлюз (gateway) по умолчанию (т. е. портал (главный вход) в следующий сегмент сети), который необходим также и для доступа в Internet;
- число (называемое *маской подсети),* идентифицирующее сетевой сегмент, в котором расположен данный компьютер;
- если задействовано динамическое присвоение IP-адресов, следует указать IP-адрес сервера, назначающего IP-адреса.

Если вы уже хоть немного работали в Internet, вероятно, вам знакома концепция IP-адресов. Говоря упрощенно, они представляют собой 32-битовые (четырехбайтовые) числа, которые идентифицируют сетевой компьютер. По сути, это программный адрес ком-

пьютера, в отличие от аппаратного адреса, "зашитого" в сетевую плату. В двоичном формате IP-адрес выглядит примерно так:

```
11000000 01101010 01111110 11000001
```

В таком виде его нелегко понимать пользователям, за исключением разве что программистов (и компьютеров). Поэтому, исключительно для удобства, IP-адреса обычно записывают в формате октетов, разделенных точками. В этом формате каждый байт из 32 битов номера преобразуется и десятичное число.

```
192.106.126.193
```

Каждой сетевой плате, работающей в сети TCP/IP, присваивается уникальный IP-адрес, идентифицирующий ее *во всей сети,* а не только в локальном сегменте.

Откуда берутся эти IP-адреса? Где узнать, какие числа следует включать в них? Ответ зависит от "области охвата" вашей сети. Если вы создаете IP-адреса для локальной сети TCP/IP, которая *никогда* не будет подключена к Internet, то можете назначать их до некоторой степени произвольно (достаточно помнить, что двум сетевым платам *нельзя* назначать одинаковый адрес). Если же вы собираетесь подключиться к Internet, необходимо получить уникальные IP-адреса, обратившись в международную организацию InterNIC.

InterNIC - единственная организация, которая уполномочена выделять IP-адреса заинтересованным фирмам и организациям. В первом приближении можно считать, что она выделяет группы IP-адресов, основываясь на размерах организаций. С этой целью InterNIC предоставляет организации конкретные числа для первого байта (первых двух, или трех байтов), а для назначения остальных адресов позволяет организации использовать оставшиеся номера по собственному усмотрению. Так, например, если вы запросили у InterNIC набор адресов Internet, вам могут предоставить набор, скажем, 192. 106. X. X. Это означало бы, что все ваши IP-адреса должны начинаться с префикса 192. 106, но вы можете назначить номера (вплоть до 255) по собственному усмотрению остальным двум октетам. Часть, назначенную InterNIC, называют *полем сети* адреса, а ту, что назначена вами, - *полем узла* (host portion).

Совет

Если вас еще не испугала идея самостоятельно назначать IP-адреса каждому компьютеру вашей организации, ужаснитесь сейчас. Вам предстоит не только назначить номера, но также и создать файл, сопоставляющий имена компьютеров < IP-адресами. Этот файл должен поддерживаться и постоянно обновляться на каждом сетевом компьютере. Чтобы упростить задачу, вы можете запустить сервер DHCP (протокол динамического конфигурирования компьютера), чтобы взять IP-адреса из специального буфера, а затем использовать серверы WINS или DNS для преобразования имен в адреса. Серверы WINS работают с именами NetBIOS, а DNS - с доменными именами.

Краеугольный камень адресации Internet заключается в идентификации не собственно компьютера, а *подсети,* т. е. той части сети, в которую компьютер входит. Это достигается не с помощью внешнего сетевого адреса, как в адресах IPX/SPX, а с *масками подсети.* Маска подсети — число, которое можно "наложить" на IP-адрес. Если сетевая часть IP-адресов компьютеров совпадает с ней, значит, машины находятся в одной подсети. В противном случае, два IP-адреса относятся к разным подсетям.

Установить связь между двумя компьютерами одной подсети несложно. Оборудование передает данные (в соответствии с требованиями протокола TCP/IP) с помощью широковещательной передачи, а компьютер, адрес которого совпадает с указанным в пакете IP, принимает данные. Если компьютеру одной подсети необходимо связаться с компьютером в другой, —

запрос должен поступить на маршрутизатор, соединяющий подсети. Маршрутизатор просматривает сетевой адрес места назначения, определяет, находится ли он в данной подсети или нет, а затем направляет пакет в следующую подсеть. Затем этот маршрутизатор проверяет IP-адрес места назначения, определяет, находится ли он в *данной* подсети, и вслед за этим либо передает сообщение с помощью широковещательной передачи, либо снова направляет пакет в следующую подсеть. Эта процедура продолжается обнаружения нужной подсети. Задача маршрутизации весьма сложна (мы вернемся к ней в гл. 5 "Дополнительное сетевое оборудование").

Когда пакет поступает в место назначения, протокол определения адреса (ARP) преобразует IP-адрес в аппаратный адрес сетевой платы. Помимо того, протокол ARP отвечает за трансляцию адресов исходящих данных.

Куда мы двинемся дальше? Часть I - протокол IP версии 6

Internet воплотил предсказания авторов фантастических романов о создании мировой компьютерной сети. Поскольку же эта сеть работает по протоколу TCP/IP, его изменения соответственно отражают и потребности Ной глобальной сети.

Примечание

В настоящее время используется версия 4 протокола IP. Версии 5 не существует.

В конце 1998 г. протокол IP - часть набора протоколов TCP/IP, отвечающая за маршрутизацию пакетов по сети, - начали адаптировать к изменениям типов передаваемых данных и для улучшения управления возрастающего трафика Internet. Изменения в протоколе позволяют:

- улучшить адресацию, поддерживающую более длинные (до 128 бит) адреса, а также *кластерные адреса* (cluster address) или *групповые адреса* (anycast address), идентифицирующие группы узлов сети TCP/IP;
- упростить форматы заголовков, позволяющие компенсировать влияние на сеть укрупненных пакетов IP;
- улучшить поддержку расширений и параметров, включая пробел для пустых расширений с целью облегчения изменения формата пакета (если это понадобится в дальнейшем);
- ввести метки потоков, идентифицирующих потоки пакетов, поступающих с конкретного узла;
- ввести дополнительные расширения, повышающие возможность контроля ошибок и идентификации пользователей, а также (при необходимости) защиту данных.

Подробные сведения о версии 6 протокола IP (IPv6) описаны в RFC 1883. Здесь они приведены частично, в основном, для тех, кто ни за что в жизни не желает конструировать маршрутизаторы.

Повышенная гибкость маршрутизации. Логически IP-адреса совершенно несложны: их число не превышает того, что можно "выжать" из 32 бит, т. е. всего-навсего 4 294 967 296 (около 4 миллиардов - если это вам интересно), а каждое устройство в Internet "требует" собственного IP-адреса, Если принять во внимание, что не все> адреса доступны, то это число дополнительно ограничивается следующими причинами:

- Десятичное значение каждого октета 32-битового адреса не превышает 255.

- Многие адреса резервируются для целей, отличных от тех, для которых предназначены обычные IP-адреса. Например, адреса, начинающиеся с 10 в первом октете используются только локально.
- Фирмам и организациям выдают *группы* адресов, которыми они распоряжаются самостоятельно, независимо от того, нужны они им или нет. Например, все адреса, начинающиеся с 192. 233. x. x принадлежат фирме Novell. И даже если адрес 192. 233. 54. 5 в ней не используется, *никто,* кроме Novell, не сможет им воспользоваться.

Для уменьшения числа необходимых IP-адресов предпринималось несколько попыток (серверы DHCP для временного выделения адресов, CIDR и т. п.). Однако число пользователей Internet растет, и вскоре потребуются 128-битовые адреса. Я не прорицатель, и это нравится мне точно так же, как необходимость звонить по телефонному номеру из 10 цифр, но, тем не менее, 128-битовые IP-адреса необходимы точно так же, как телефонные номера из 10 цифр - более краткие идентификаторы уже непригодны.

Для облегчения адресации пакетов группам пользователей (не обязательно подсетям или сетям) предусматривается использование групповых адресов (anycast address). Вместо отсылки пакетов индивидуально каждому члену группы, вы должны будете отсылать их кластеру, который представляет собой логическую, а не физическую группу.

Примечание

Групповые адреса (anycast addresses) заменят широковещательные адреса (broadcast address), использование которых предусмотрено протоколом IPv4.

Метки потоков (Flow labelling). Удлинение адресов может причинить неудобства пользователям, которым придется их вводить, однако упростит идентификацию компьютеров Internet. Другая проблема Internet, вызывающая беспокойство, — трафик.

На заре своего появления Internet поддерживала небольшой трафик. Большую часть данных, передаваемых по сети, составляли файлы и сообщения электронной почты. Однако со временем характер трафика изменился. Теперь он состоит из поддержки групп новостей и досок объявлений, позволяющих посылать сообщения на всеобщее обозрение. Появились комнаты для переговоров (chat rooms) и Web. Кроме того, в настоящее время стали возможны и телефонные переговоры по Internet. Загрузка данными продолжает расти, и это вызвано ростом числа служб и пользователей — они сами по себе загружают трафик значительно больше, чем передача файлов.

Однако представьте себе на мгновение, что Internet — это множество сетей, соединенных маршрутизаторами. Маршрутизаторы рассматриваются в гл. 5 "Дополнительное сетевое оборудование". Каждый маршрутизатор отвечает за идентификацию наилучшего пути передачи данных по месту назначения. С этой целью он должен идентифицировать место назначения каждого принятого пакета, т. е. открыть и исследовать множество пакетов. Так вот, в пакете IPv6 есть поле, где можно указать конкретный поток, к которому относится пакет. Идея такова: если маршрутизатор установит, что пакет является частью потока пакетов, следующих в одно и то же место, ему фактически нет нужды определять, где находится это место, после того, как он исследует первый же пакет в проходящей группе (flow group).

Примечание

По умолчанию маршрутизатор должен "помнить" метку потока в течение шести секунд, однако это время можно увеличить вручную.

Приоритет пакета. Иногда трафик Internet может стать настолько тяжелым, что пакет может "погибнуть". Как правило, пакеты отбрасываются без учёта их важности. Однако пакетам IPv6 можно присваивать приоритеты в соответствии с назначением.

Значения приоритетов разделены на два диапазона: 0—7 и 8—15. При перегрузке сети пакеты с низшим приоритетом (номером) в пределах данного диапазона отбрасываются в первую очередь, причем каждый диапазон рассматривается отдельно. Иными словами, пакет с приоритетом 6 не обязательно отбрасывается ранее пакета с приоритетом 8, поскольку пакет с
приоритетом 6 в пределах своего диапазона имеет высший приоритет.

Значения приоритетов 0—7 используют для указания приоритета трафика, для которого источник обеспечивает контроль перегрузки (congestion control), т. е. трафик, использующий протокол высшего уровня (например, TCP) для отслеживания способности системы управлять потоком данных, при перегрузке системы прерывается. Ниже приведены значения приоритетов трафика с контролем перегрузки, предусмотренные спецификацией IPv6.

0 - трафик без приоритета.
1 - трафик - "заполнитель" ("Filler" traffic) (сетевые новости).
2 - необслуживаемая передача данных (электронная почта).
4 — обслуживаемая передача большого объема данных (FTP, NFS),
6 — интерактивный трафик (telnet, протокол дисплея).
7 — управляющий трафик Internet (маршрутизирующие протоколы, SNMP).

Примечание
Приоритеты 3 и 5 зарезервированы на будущие категории.

Значения 8—15 используют для указания приоритета трафика, который не прерывается в ответ на перегрузку. К нему относятся пакеты речевой и видеоинформации, отсылаемые с постоянной скоростью. Они не отмечены в спецификации, но, как правило, более важная информация (скажем, слабо различимый голос) должна иметь приоритет выше, чем информация, которая при передаче имела бы превосходное качество, но малосущественна (скажем, высококачественная видеоинформация).

Поддержка крупнейших пакетов. Среди прочих расширений (extensions), предназначенных для улучшения "отклика" IPv6 на условия работы в Internet, можно отметить те, которые позволяют увеличить размер пакетов IP, т. е. нести больший объем полезных данных по сравнению с IPv4. Это весьма полезная возможность, поскольку применение крупных пакетов позволяет передать данные с помощью меньшего числа пакетов, что, в свою очередь, уменьшает задержку при маршрутизации пакетов.

Куда мы двинемся дальше? Часть II - миграция к IPv6

Как вы заметили, текущая реализация протокола IP значительно отличается от той, что маячит на горизонте. Без использования новых параметров, таких как приоритеты и управление потоками, адресация пакетов была бы значительно сложней. Если же в пакете этих установок не существует, новые возможности игнорируются. Переход на новый протокол не происходит автоматически. Не думайте, что одним прекрасным утром вы обнаружите, что все узлы вашей сети обновились до IPv6.

Задача перехода от IPv4 к IPv6 отнюдь не проста. В настоящее время *открылись* курсы, на которых обучают решению этой проблемы и, кроме того, можно использовать некоторые сетевые ресурсы. Лучшие из них находятся по адресу http://www.emos.be/ ccexist/etg071/gintrod.htm - INICIO.

Не вдаваясь в детали, укажу четыре метода перехода сети на протокол IPv6.

- Поддержка обоих протоколов.
- Включение в один пакет адресов для обоих протоколов.
- Создание туннеля IPv6 посредством протокола IPv4.
- Трансляция заголовков с тем, чтобы узлы IPv6 могли связываться с узлами IPv4.

Примечание

Вы не понимаете, что все это значит? Туннелирование рассматривается в гл. 6 "Общие сведения о глобальных сетях", трансляция заголовков - при обсуждении мостов в гл. 5 "Дополнительное сетевое оборудование".

Если же вы решитесь пройти весь этот путь, вам придется обновить всю сеть в следующем порядке.

1. Обновить сервер DNS для поддержки новых адресов.
2. Обновить узлы для поддержки как IPv4, так и IPv6.
3. Развернуть обновленные узлы.
4. Обновить область (сегмент сети) для полного перехода на протокол IPv6, причем оба протокола должны поддерживать только граничные маршрутизаторы.
5. Обновить маршрутизаторы для полного перехода на протокол IPv6.
6. Развернуть новые маршрутизаторы.

Итак, вы обновляете систему определения имен, а затем, работая "изнутри", распространяете IPv6 по всей сети, причем по ходу процесса обеспечиваете совместимость протоколов.

Поддержка нескольких стеков транспортных протоколов

Теперь, по прочтении главы, вам должны быть очевидны два момента. Во-первых, идеального сетевого протокола не существует. Во-вторых, весьма вероятно, вам понадобится использовать все три протокола (NetBEUI, IPX/SPX и TCP/IP), причем каждый по особой причине — к счастью, это возможно. Поддержка множества транспортных протоколов является немалой ценностью современной сетевой модели (рис. 3. 7).

Можно заметить, что в клиентный компьютер загружено четыре транспортных протокола, в то время как на сервере загружен единственный. Это бывает в том случае, если клиентный компьютер одновременно связан с несколькими серверами. Стек протоколов IPX может обеспечивать связь с серверами Novell, стек TCP/IP — с сервером Internet, а протокол NetBEUI используют для локального доступа к компьютерам с операционными системами Microsoft. Каждый транспортный протокол привязан к драйверам и редиректору, установленным на каждом компьютере. Как указывалось ранее, в разделе "Интерфейсы сетевых компоновок", порядок компоновки различных протоколов можно изменять. Таким образом, при соединении с серверами NetWare в первую очередь будет использован протокол IPX/SPX (или совместимый с ним); а при соединении с Internet - протокол TCP/IP.

Выводы

Чтобы передать данные по компьютерной сети, вам необходимо не только оборудование, но и сетевое программное обеспечение.

- Редиректор, гарантирующий отправление запроса драйверу соответствующей файловой системы для получения с ее помощью доступа через сеть.
- Сетевая файловая система, предназначенная в данном случае для отображения дискового пространства.
- Сетевой драйвер, позволяющий операционной системе установить связь с сетевой платой.
- Сетевой транспортный протокол, обеспечивающий пакетирование и I отправление информации по адресу назначения через сеть.

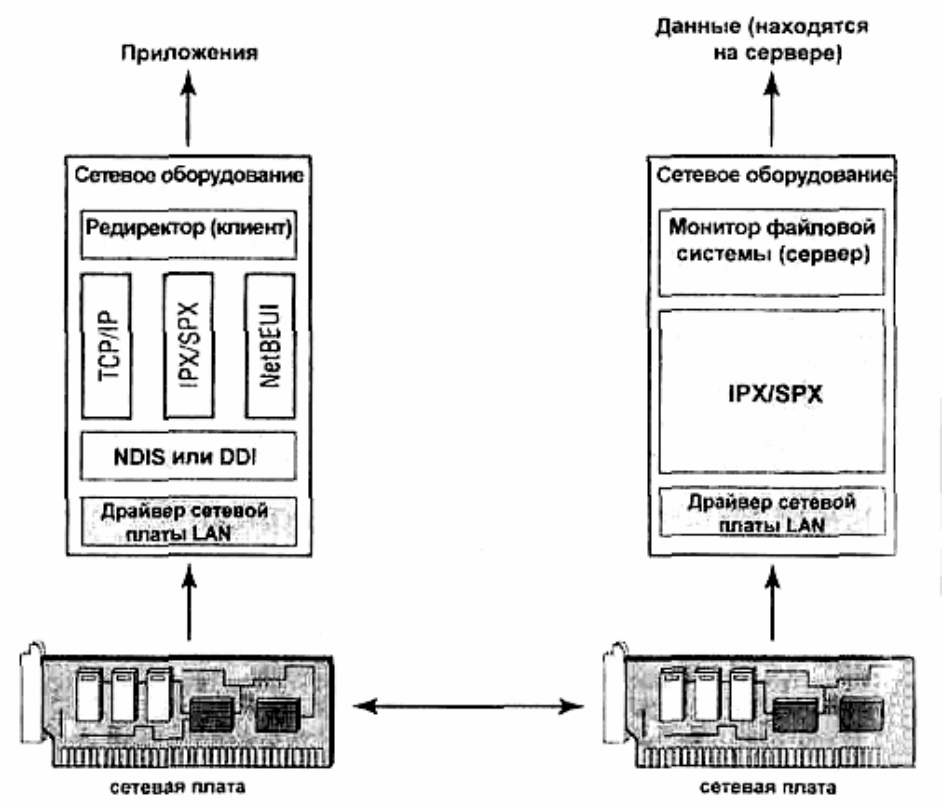
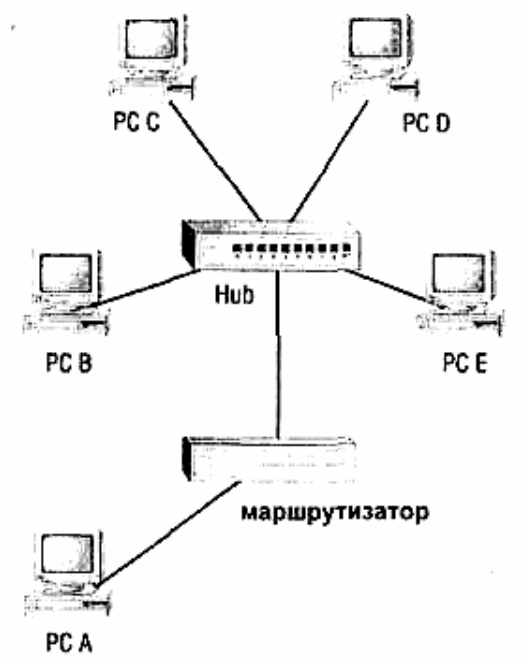


Рис. 3.7. Сеть, допускающая использование нескольких транспортных протоколов

Каждая часть сетевого программного обеспечения обособлена, что придает системе гибкость и упрощает при необходимости замену (обновление) отдельных компонент. Тем не менее, все части жизненно важны для установления надежной связи между компьютерами. В предыдущих главах большое внимание уделялось подробностям сетевых соединений. Вы получили начальные сведения о тех из них, которые понадобятся в дальнейшем. В следующей главе я расскажу, как собрать все это вместе, чтобы создать локальную сеть.

Упражнение 3

1. Посмотрите на рисунок, приведенный ниже. Какие транспортные протоколы, из числа обсуждавшихся в этой главе, можно использовать для отсылки данных от PC A к PC D? Если есть ограничения, то какие?
2. Допустим, один компьютер работает под управлением Windows 98, а второй — DOS. Следует ли использовать на *каждом* компьютере сетевые драйверы ODI или NDIS. Или это не имеет значения?
3. В каком транспортном протоколе, упомянутом в этой главе, используют шлюз по умолчанию (default gateway)?
4. Адреса IPv4 имеют длину ____ бит, а адреса IPv6 _____ бит.
5. Какая часть сетевого программного обеспечения управляет запросами данных с сетевых дисков с приложениями?
6. Средство API, используемое для установки связи между клиентной и серверной программами, называют _____.
7. Что такое монолитный драйвер устройства?



Глава 4

Установка Сетевых плат и кабелей

На протяжении трех глав обсуждались теоретические вопросы. Вам же, вероятно, не терпится запачкать себе руки. Наконец в этой главе рассматривается установка сетевых плат и кабелей сети, которая объединит ваши компьютеры.

Подготовка к прокладке кабелей

Большинство вопросов, которые я хочу обсудить, касаются подготовки к приему представителей фирмы-подрядчика и всего того, что вам необходимо знать о физической установке сети до начала прокладки кабелей. Это отнюдь не полное руководство по монтажу и прокладке кабелей. Во-первых, для этого здесь не хватит места. Во-вторых, трудно создать такие инструкции, если не известна среда, в которой будет прокладываться кабель. В-третьих, сложную кабельную разводку обычно выполняют специалисты. Поэтому я собираюсь обсудить только основные вопросы, чтобы вы могли самостоятельно выполнять простейшие работы по прокладке кабелей или квалифицированно присматривать за нанятыми специалистами. Изучив эту главу, вы сможете объяснить монтерам, чего вы от них хотите. Такие работы стоят недешево, во время их проведения будет "щелкать счетчик", поэтому подготовьтесь к ней как можно лучше.

Разработка перспективного плана

Вот самый очевидный совет (которым обычно пренебрегают): думайте не о сегодняшних нуждах, а о том, что вам понадобится через 5 или 10 лет. Прокладка кабеля в здании не такая уж простая работа, чтобы выполнять ее дважды. Поэтому разработайте перспективный план.

Во-первых, изучите обстановку. Поднимите синьки с планировкой здания и внимательно просмотрите их. Где проходят кабельные каналы? Где проложены электрические провода и как они экранированы? Какие сюрпризы вас ожидают? К какому классу с точки зрения пожарной безопасности относятся помещения? Где можно обойтись кабелем в поливинилхлоридной оболочке, а где следует воспользоваться специальным кабелем?

Используйте кабель с максимальной пропускной способностью в пределах ваших возможностей. Пусть даже сейчас он не нужен. Однако весьма вероятно, что рано или поздно такой кабель пригодится, например, тогда, когда ваша фирма начнет использовать настольные базы данных, видеоклипы и тому подобное. Купите, если можете, кабель категории 5 на 100 Мбит/с или даже оптоволоконный — впоследствии вы сэкономите немало средств, избежав повторной прокладки кабелей.

Предусмотрите резервы

Никогда не планируйте закупку кабеля "в обрез". Напротив, предусмотрите некоторый его запас. Во-первых, он понадобится просто потому, что вы не сможете громоздить компьютеры один на другой для подключения к сети. Если сеть имеет физическую шинную топологию, вам понадобится примерно через каждые 10 футов делать отводы для подключения компьютеров.

Совет

Коаксиальные кабели некоторых типов выпускают с отметками через каждые 10 футов. Это очень удобно, поскольку позволит вам точнее определить, на каком расстоянии следует делать подключения.

Кроме того, запас никогда не помешает. Если кабель закуплен точно в соответствии с вашими нуждами, рано или поздно какой-нибудь агрессивный пользователь захочет передвинуть компьютер на пять футов влево. Если не предусмотреть этого сразу, ваша сеть разрушится. Прокладывая кабель по потолку или полу, оставьте несколько петель (2—3 м для магистрального кабеля) в каждом углу помещения либо у двери, или в любом приметном месте здания, чтобы впоследствии их можно было найти. Закрепите петли изолентой (electrical tape), чтобы они имели аккуратный вид и не мешали работе. Когда вам понадобится удлинить кабель, вы сможете ими воспользоваться. В противном случае вам придется наращивать кабель самостоятельно либо приглашать для этого монтера. Как правило, подрядчики оценивают стоимость работы не по длине проложенного кабеля, а по числу отводов (terminations). Наращивание кабеля означает оплату двух бесполезных разъемов, которые нужны только для удлинения, что можно было бы запланировать с самого начала. Точно так же, прокладывая отводы от магистрали или концентратора, оставьте про запас 3—5 м, с тем, чтобы впоследствии при необходимости можно было переставить компьютер.

Предупреждение

Если вы просчитались при планировании и теперь вам необходимо удлинить кабель, его следует наращивать, а *не пытаться вытянуть.* Вытягивание может повредить кабель, особенно многожильный, а поврежденный кабель в значительно большей степени подвержен внешним помехам.

Чтобы сделать комнату более свободной, используйте также кабельные каналы (conduit). В крупных сетях с высоким уровнем защиты нередко создается центральная магистраль (central backbone), проходящая по широкому кабельному каналу, от которого ответвляются кабельные каналы меньшего размера. Такая конфигурация стоит очень дорого, а крупногабаритные отводы удорожают ее еще больше. Тем не менее, обязательно предусмотрите установку кабельных каналов большего размера, пусть даже сейчас это и не нужно. Например, если увеличение ширины канала на 1/2 дюйма позволяет сделать два отвода от центральной магистрали, увеличьте ширину на 3/4 дюйма, что позволит при необходимости дополнительно проложить 3—4 отвода. Даже если сейчас это кажется слишком дорогим, в будущем такая возможность наращивания сети сохранит вам немалые средства, избавив от прокладки новых кабельных каналов и "выброса на слом" уже оплаченной проводки.

Точность расчетов

Не забывайте ни на секунду, что после прокладки кабеля вам придется работать с ним. Поэтому по возможности облегчите к нему доступ. например, если кабель планиру-

ется прокладывать по потолку, вы можете попробовать проложить его прямо по полу, поскольку это менее трудоемко. Действительно, поначалу это так. Однако впоследствии вам вряд ли понравится спотыкаться о кабель, лежащий на полу. Чтобы избежать этого, Прикрепите кабель к чему-нибудь вроде креплений каркаса подвесного Потолка. Для этой цели выпускают специальные крепления, но можно использовать обычную изоленту. Кроме того, можно прикрепить кабели к Трубопроводам системы кондиционирования или отопления.

Если вы оставили все кабели на "полу" (т. е. наверху) подвесного потолка, то, по крайней мере, свяжите их в пучки, чтобы они находились вместе. Тогда, если понадобится убрать их, вам достаточно будет удалить единственный пучок, а не шесть различных кабелей, перепутанных друг с другом.

Примечание

Отнюдь не все подвесные потолки выдерживают вес кабельной разводки, так что, возможно, вам придется прикрепить их к каким-либо опорам или вентиляционным каналам.

Прокладка кабелей под полом тоже требует планирования. Опять-таки, прокладывайте кабели аккуратно, чтобы их можно было легко найти. Если вам позволяют средства, проложите кабели в специальных туннелях, чтобы они оставались в одном и том же месте. Кроме того, постарайтесь проложить кабели так, чтобы к ним можно было добраться *после* расстановки мебели в помещении. Может показаться, что удобнее всего проложить кабели вдоль стены. Однако весьма вероятно, что там будут расставлены шкафы или очень тяжелые столы. Лучше всего использовать середину комнаты — маловероятно, что в ней расставят мебель.

Если вы прокладываете кабели *поверх* пола, то требования несколько иные. В этом случае предпочтительно прокладывать именно вдоль стен и подальше от прохода. Тогда на них не будут слишком часто наступать проходящие мимо служащие, нанося вред себе и сети. Кроме того, менее вероятно и повреждение сети излишне старательной уборкой помещения. Прикрепите кабели как можно тщательнее — тогда они не перепутаются, и люди не будут спотыкаться.

И, наконец, снабдите *все* надписями. Во время аварии необходимо знать, куда идет каждый кабель. Иначе вы когда-нибудь увидите такую сцену: "Вася (или Джон), когда я крикну "Давай!", дерни кабель, чтобы я смог найти нужный конец!". Как правило, далее следует: "Не, это не тот... Когда крикну, дергай следующий... ".

Чтобы избежать подобных сцен, можно пометить концы кабелей разноцветной изолентой либо приклеить к ним небольшие бирки с номерами, либо (если у вас бездонный карман) использовать разноцветные кабели. Это поможет вам узнать, какой кабель вы держите в руках, а какой тянете, когда работаете, согнувшись в три погибели под потолком. Я не рекомендую использовать надписи от руки, поскольку иногда их трудно разобрать. Но если только вы прокладываете не слишком сложную кабельную систему, которая требует подробного описания, лучше всего используйте условные обозначения. Вы можете распознать их с первого взгляда, без расшифровки чьего-нибудь неразборчивого почерка либо вращения кабеля, чтобы прочесть всю надпись. Помните также и еще об одном: около 10 % мужчин не могут отличить красный цвет от зеленого. Поэтому рекомендуем избегать использования зеленого или красного кабелей.

Совет

Поместите описания кодов кабелей на видном месте, чтобы сотрудники могли разобраться в них, даже если вас нет в офисе.

Другие проблемы

Наконец, продумайте, что еще будет находиться в том месте, где проходит ваш сетевой кабель. Если вокруг расположено множество устройств, генерирующих помехи, применяйте кабель с дополнительным экранированием, такой как коаксиальный или STP, или, лучше всего, оптоволоконный, совершенно нечувствительный к RFI.

Совет

Флуоресцентные лампы генерируют значительные EMI, поэтому не прокладывайте кабели непосредственно над ними.

Если в помещении уже проведена электропроводка, не прокладывайте сетевые кабели параллельно ей, особенно вблизи крупных пучков проводов, ведущих к щитку электропитания. Если после установки сети начнется прокладка нового кабеля электропитания, вы можете избежать проблем с помехами, используя бронированный кабель (в металлической оболочке) вместо обычного в пластиковой оболочке. Опять-таки, поначалу это влетит в копеечку, но впоследствии такая предосторожность сбережет ваши деньги.

Что следует выяснить заранее

Я рассказала о некоторых специфических проблемах, о которых следует знать перед прокладкой кабелей. Ниже приведено несколько вопросов, которые вы должны выяснить вместе с вашим подрядчиком. Это нужно вделать с самого начала, и вы сбережете немало времени, денег и избавитесь от головной боли.

Есть ли у вас кабельные каналы? Во многих зданиях предусмотрены встроенные в стены и потолки ниши (каналы), в которых вы можете проложить кабель. Часто в этих кабельных каналах предусмотрена специальная защита. Это также означает, что вы сможете использовать дешевый кабель в поливинилхлоридной оболочке.

Как вы проверяете ваши кабели? Вам необходимо знать точный метод тестирования кабелей после их прокладки. В этом следует больше полагаться на здравый смысл. (Помните, однако, что здравый смысл иногда подводит.) Потребуйте письменное описание метода проверки и убедитесь, что полностью его понимаете.

Как вы документируете ваши действия? Убедитесь, что кабельная система документирована, а кабели помечены в соответствии со стандартом, принятым в вашей фирме. Если же ваша фирма не использует внутренние стандарты подобного рода, то вы должны их принять. А также должны Выть уверены, что понимаете систему маркировки кабелей. Поэтому я рекомендую, чтобы стандарт на маркировку устанавливала ваша фирма, а не подрядчик.

Каковы условия ремонта кабельной сети? Потребуйте от подрядчика прибытия по вызову на место ремонта не более чем через 24 часа. Многие подрядчики согласятся с этим, имея в виду ответ по телефону, но не реальное прибытие на место (которое в действительности может затянуться на неделю). Вам, однако, нужно не это: компьютерные проблемы с кабельной разводкой требуют *немедленного* решения.

Есть ли у подрядчика не менее трех рекомендаций местных фирм? Вы должны получить от подрядчика не менее трех рекомендаций от местных фирм, чтобы воочию

убедиться в качестве его работы и документирования. Большинство фирм не откажут в просьбе посмотреть на их кабельные системы, если они довольны проделанной работой. Не забудьте и вы в дальнейшем отплатить любезным согласием на просьбу потенциальных клиентов вашего подрядчика осмотреть вашу квалифицированно спроектированную и установленную кабельную разводку.

Соблюдаете ли вы строительные нормативы и требования пожарной охраны? Чтобы гарантировать безопасность служащих, соблюдайте местные строительные нормы и требования пожарной безопасности. Необходимо выбрать подрядчика, который может на практике показать, что хорошо знаком с местными правилами. Если у вас возникли сомнения, проконсультируйтесь сами с местными властями.

Должны ли вы извещать о своих планах других обитателей здания и окрестностей? Возможно, вам следует проконсультироваться с прочими обитателями вашего здания и убедиться, что установка кабельной системы не помешает их работе. Это не столько обязанность, сколько правила приличия. Нередко администрация здания сама извещает его обитателей.

Каков гарантийный срок работы кабельной системы? Узнайте у подрядчика гарантийный срок на выполненные работы и самих кабелей. Желательно заключить, по крайней мере, годичный контракт на обслуживание. Разумная сумма контракта на годичное обслуживание не должна превышать 12 процентов общей стоимости работ.

Беспроводные сети

Подготовка к развертыванию беспроводной сети (или, вероятнее, беспроводной части сети) мало отличается от подготовки прокладки проводной сети. Вы точно так же должны проанализировать окружающие факторы и методы передачи данных из пункта A в пункт B.

В локальных сетях используют два типа беспроводных сетей. Чаще всего используют радиочастотные (RF) беспроводные сети, которые позволяют соединять компьютеры и серверы на огромной территории. Однако скорость передачи данных по таким сетям невелика (около 1 Мбит/с). В специализированных устройствах, таких как беспроводные принтеры или клавиатуры используется инфракрасная (IR) связь, позволяющая создавать высокоскоростные соединения на небольших расстояниях.

Наиболее значительной проблемой беспроводных сетей, с которой вам, вероятно, придется столкнуться, будут помехи. В инфракрасной связи используются чрезвычайно высокие частоты, поэтому, чтобы использовать ее, отправитель и получатель должны находиться рядом — в зоне прямой видимости. Если вы не протянете прямую "нитку" между принимающим и передающим устройствами, они не смогут связаться. Поэтому, если вы приобрели IR-принтер, желательно поставить его в таком месте, где пользователи портативных компьютеров с IR-портом могли бы получать к нему беспрепятственный доступ, а это значит, что другие люди не должны ходить между этими устройствами.

Примечание

Как указано в гл. 1, рабочая частота определяет количество данных, которые можно передать в течение заданного промежутка времени. При этом высокочастотные системы связи более чувствительны к помехам, чем низкочастотные.

RF-устройства в меньшей степени чувствительны к помехам, поскольку используемые в них низкочастотные (по сравнению с инфракрасными системами) сигналы в большей или меньшей степени способны огибать препятствия и, следовательно, не блокируются ими. По этой причине радиус действия IR-устройств ограничен комнатой, в которой они установлены, в то время как RF-устройства можно устанавливать на расстоянии 300—500 футов (100—150 м) от источника в пределах помещения и 800—1000 футов (250—300 м) - вне помещения. Сигналы ослабляются толстыми стенами и металлическими барьерами, но в прочих отношениях они неуязвимы.

Установка и конфигурирование сетевых плат

Итак, кабели проложены. Теперь можно их к чему-нибудь присоединить. Если вы не знакомы с монтажом и конфигурированием кабельной сети, продолжайте читать далее и узнайте о том, как в компьютер устанавливается сетевая плата, как затем она конфигурируется для работы с другими сетевыми платами, если они там уже есть.

Установка сетевых плат

Если у вас есть хотя бы небольшой опыт установки в компьютер «пличных плат, техника установки сетевых плат для вас не будет неожиданной. Выключите компьютер, наденьте антистатический браслет, снимите крышку с корпуса компьютера и найдите на материнской плате свободный слот, соответствующий типу сетевой платы.

Совет

По возможности, выберите слот, рядом с которым нет другой платы - это улучшит вентиляцию корпуса компьютера.

Если для установки новой платы необходимо сначала вынуть старую плату, выполните следующие действия.

1. Убедитесь, что от извлекаемой платы отсоединены все внешние кабели.
2. Открутите небольшие винты, соединяющие металлическую планку платы с корпусом компьютера, и отложите их в сторону.

Совет

Для хранения винтиков я использую коробку для яиц. Она превосходно подходит для этой цели - дешевая, удобная, в ней множество небольших гнезд, куда можно складывать винты разного размера. Кроме того, ее можно закрыть, и если вы уроните коробку со стола, винтики не разлетятся по всей комнате. Единственный недостаток заключается в том, что кто-либо (из благих побуждений), не разобравшись, зачем тут кругом лежат эти коробки, может выбросить их в мусор.

3. Осторожно потяните плату обеими руками, слегка раскачивая вперед и назад, чтобы высвободить ее из слота. Это требует некоторых усилий, однако если плата не выходит легко, остановитесь и убедитесь, что действительно отсоединили металлическую планку платы от корпуса компьютера.
4. Отложите снятую плату. Если вы планируете использовать ее впоследствии, то поместите плату в собственную упаковочную коробку (если она сохранилась). Не ка-

сайтесь позолоченных контактов платы пальцами: потожировые выделения на вашей коже способствуют коррозии даже золотого покрытия и таким образом, ухудшают качество контактов платы.

Установка платы — почти такой же процесс, только выполняется в обратном порядке.

1. Отключите компьютер и снимите с корпуса крышку.
2. Извлеките плату из упаковки, стараясь не касаться руками позолоченных контактов.
3. Найдите на материнской плате свободный слот, соответствующий шине, для которой предназначена плата. Для плат ISA используют слот ISA, а для PCI - слот PCI.

Примечание

Вероятнее всего, вам придется работать с платами ISA и PCI. Платы MCA и EISA встречаются редко. Маловероятно, что вам встретятся сетевые платы, рассчитанные на шины подобного типа. Иногда встречаются EISA, но это бывает еще реже.

4. Отвинтите на задней панели компьютера заглушку, закрывающую щель свободного слота, и отложите заглушку и винты в сторону. Возможно, заглушка понадобится впоследствии, а винты мы вскоре используем.
5. Приставьте сетевую плату к слоту материнской платы и осторожно, но в то же время с усилием, нажмите на нее так, чтобы плата плотно вошла в слот. Возможно, для этого понадобится значительное усилие, величина которого, если у вас нет навыка установки плат, вызывает некоторые опасения. Если вы правильно выбрали слот и вставляете плату точно в него, то плата должна надежно в нем зафиксироваться.
6. Используя винты, отложенные ранее (п. 4), привинтите планку платы к небольшим отверстиям в корпусе, чтобы зафиксировать ее. Если плата вставлена правильно, это действие практически не изменит ее положения, однако предохранит плату от перекосов или расшатывания.
7. Наденьте крышку на корпус и, если кабели уже подведены, соедините их с платой.

Установка драйверов сетевых плат

Процесс установки драйверов плат зависит от операционной системы. Подобно всем дополнительным платам, сетевые платы поступают вместе с диском (дискетой или CD-ROM), содержащим нужные драйверы. Для правильной установки этих драйверов следуйте инструкциям, которые прилагаются к сетевой плате. Процесс установки, как правило, инициируется достаточно простыми операциями, наподобие запуска программы INSTALL с устройства A:. В такого рода установочных программах используется интерфейс, подобный приведенному на рис. 4. 1.

Совет

Драйверы плат могут входить и в состав операционной системы, однако если операционная система установлена более года назад, то с сетевой платой, вероятно, поступят более новые драйверы.

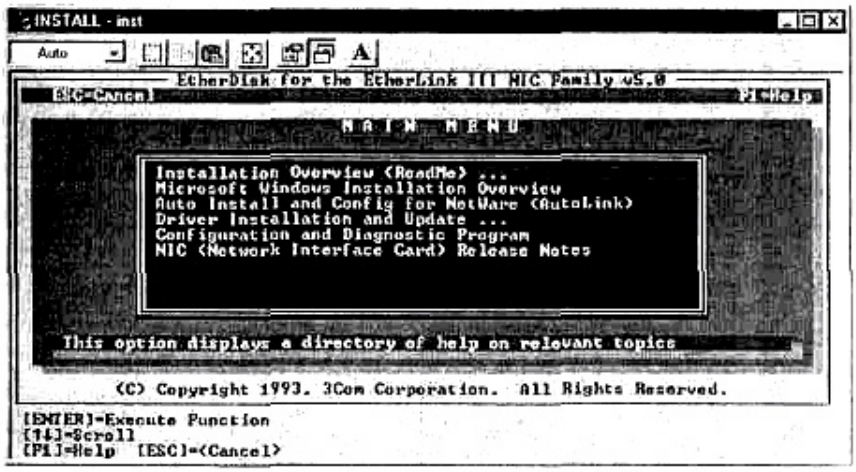


Рис. 4.1. Установка сетевых плат с гибкого диска

В состав новейших версий операционных систем могут входить драйверы плат. Их загружают, используя интерфейс самой операционной системы. Например, в Windows95/98 есть мастер установки нового оборудования (Add New Hardware Wizard), который используют для обнаружения платы и автоматической загрузки нужного драйвера. В то же время, вы по-прежнему можете загружать драйверы с гибкого диска, если там записана новая или оптимизированная для данной платы версия. Рассмотрим, например, сетевую плату 3Com EtherLink III NIC, описанную в предыдущем примере (рис. 4. 1). Если плата устанавливается для использования в среде операционной системы Windows NT, то использовать драйверы, входящие в состав операционной системы, нежелательно. Вместо этого следует вручную выбрать тип платы и установить драйвер с гибкого диска. Если же вы не знаете, как поступить, ознакомьтесь с документацией, прилагаемой к сетевой плате, либо поищите ее на Web-узле производителя.

Раз уж разговор пошел о Web-узлах, то учтите: имея доступ к Internet, вам нет нужды использовать драйверы, находящиеся на прилагаемом к плате гибком диске *или* входящие в состав операционной системы, — скорее всего, они уже устарели. Вместо этого войдите в Web-узел производителя сетевой платы и найдите раздел, относящийся к загрузке программного обеспечения. Выберите тип и модель вашей платы. Чаще всего откроется страница, подобная показанной на рис. 4. 2. С нее можно перейти к загрузочным страницам данной модели платы.

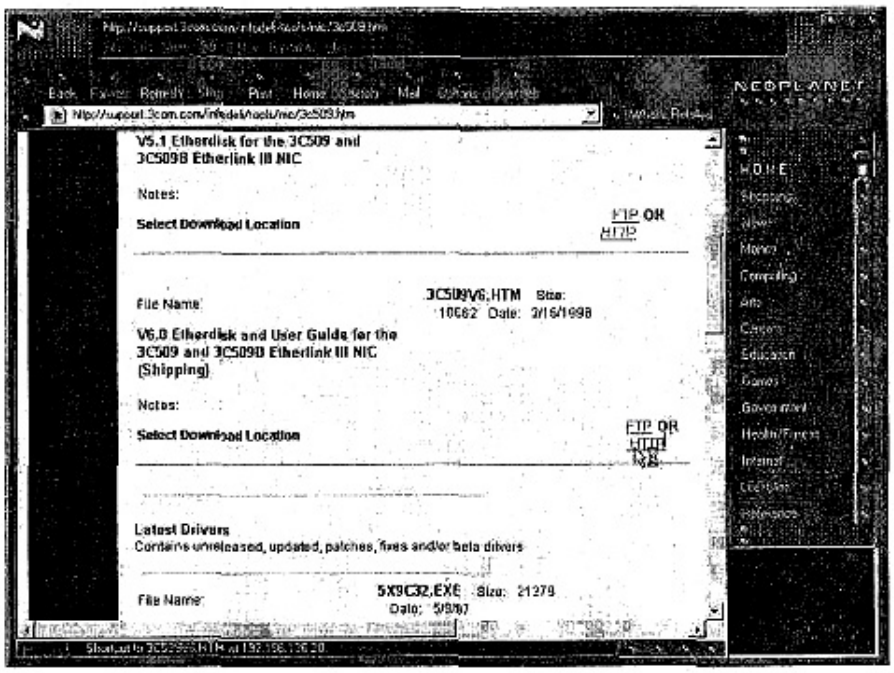


Рис. 4.2. Загрузка из Web обновленных драйверов (авторские права принадлежат NeoPlanet и Bigfoot)

Сейчас, когда вы читаете эту книгу, драйверы, выпущенные в феврале 1998 г., уже устарели. Тем не менее, сравнив их с драйверами, записанными на гибкий диск в 1993 г., вы сможете оценить преимущества обращения к Web- или FTP-узлам за новейшими версиями драйверов плат. (Учтите также, что плата была куплена в 1996 г, когда драйверы *уже* устарели.)

Совет

Наш совет по загрузке драйверов через Internet применим не только к сетевым платам, но и к любым устанавливаемым устройствам. Разумеется, не все драйверы часто обновляются, однако в целом это дело стоящее.

Конфигурирование ресурсов платы

Во многом физическая установка платы — простейшая задача: вы вставляете ее и система готова продолжать работу. Конфигурирование же сетевой платы — совершенно особое дело. В гл. 3 рассмотрены логические адреса, используемые платами. Кроме того, отмечено, почему эти адреса должны быть уникальными во всей сети. Все это, однако, несложно. Сложность заключается в обеспечении гарантированного доступа сетевой платы к процессору, а также места для хранения ее данных, ожидающих обработки процессором. Иными словами, сетевая плата должна иметь собственное прерывание, адрес буфера ввода/вывода и (изредка) каналы DMA.

Совет

В современных платах значения прерываний, буферов ввода/вывода и DMA задаются либо программным путем, либо программой SETUP, либо автоматически определяются операционной системой. В платах старых образцов некоторые установки следует выполнять с помощью перемычек или переключателей, расположенных на самой плате. Поэтому до установки платы в машину, определите метод конфигурирования платы: программный или аппаратный.

Если вам знакомы эти термины, то можете пропустить несколько следующих страниц. На них я собираюсь объяснить, что означают установки и зачем они нужны.

Совет

Если вы используете только платы PCI, а ваша операционная система поддерживает стандарт Plug-and-Play (подключи-и-работай), то можно не беспокоиться о проблемах конфигурирования, рассматриваемых далее в этой главе. Платы PCI поддерживают стандарт Plug-and-Play, т. е. конфигурируются автоматически. Они используют те же ресурсы, которые здесь описываются, - просто вам не придется конфигурировать их вручную.

Привлечение внимания процессора - запросы прерывания

Сетевая плата предназначена для передачи и приема информации. И в то же время, она ничего не может с ней *сделать*. Все "перемалывание" чисел, передача их в основную память или манипулирование данными должно осуществляться процессором.

Это, конечно, прекрасно, однако все остальные устройства внутри компьютера, а также подсоединенные к нему — клавиатура, жесткий диск, видеоплата, звуковая плата и т. п. — тоже конкурируют за доступ к процессору. Периферийные устройства могут получить доступ к CPU одним из двух методов. Первый: каждые несколько миллисекунд (тысячных долей секунды) процессор может обратиться к сетевой плате и спросить: "Прошу прощения, мистер NIC, нет ли у вас информации, которую необходимо обработать?". Этот метод периодического "обращения" к плате, установленной в системе, называется *опросом* (polling). Его работа показана на рис. 4.3.

Так все это работает, и, действительно, некоторые устаревшие сетевые платы требуют, чтобы процессор опросил их для определения их статуса. Недостаток метода заключается в том, что такой процесс крайне неэффективен. Если бы процессор работал подобным образом, ему приходилось бы постоянно прекращать обработку данных, только для того, чтобы запросить у сетевой платы информацию, которой у нее может и не быть. Это привело бы к значительной бесполезной трате времени работы процессора, особенно, если в компьютере установлено множество других устройств, которые также необходимо опросить. Если в компьютере используется только метод опроса, может случиться так, что процессор фактически будет затрачивать все свое время на переходы между устройствами и выполнение запросов: "У вас есть что-нибудь для меня?". Это не оставит, ему времени на обработку Данных, для чего, собственно говоря, и предназначен процессор.

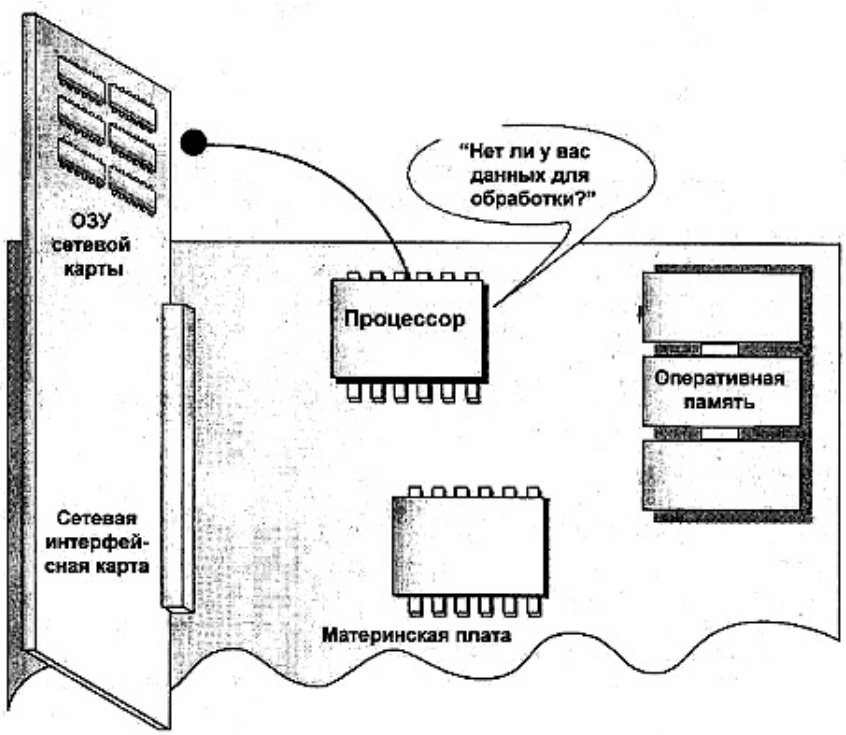


Рис. 4.3. Процессор запрашивает данные у сетевой платы

В современных системах чаще используют альтернативный метод: *прерывание (interrupt).* Если у сетевой платы есть пакеты, которые ожидают обработки (рис. 4. 4), то они сохраняются в памяти сетевой платы. Когда пакет прибывает в "зал ожидания", т. е. в память сетевой платы, она подходит к процессору, хлопает его по плечу и говорит: "Прошу прощения, мистер процессор, но в памяти мистера NIC есть некоторая информация. Когда вы улучите момент, прервите, пожалуйста, вашу работу и обработайте эту информацию или передайте ее в основную память". То, что делает сейчас сетевая плата, называют *запросом прерывания (interrupt request).*

Получив запрос, процессор продолжает работать. Однако, улучив момент, он обращается к плате и начинает обработку информации или перемещает её из буфера платы в основную память.

Вам трудно представить все это? Тогда вообразите, что процессор — это "главный администратор" вашего компьютера, а каждое периферийное устройство — начальник отдела. Дверь кабинета "CPU" закрыта, однако на его столе стоит множество разноцветных телефонов, так что он может отвечать по каждому отдельно. Телефон — линия горячей связи с соответствующим отделом. Скажем, если звонит розовый телефон, значит поступил запрос от жесткого диска поместить в основную память данные из кластера 492. Звонит зеленый, — клавиатура настаивает на регистрации нажатых клавиш и ее буфере прежде, чем они будут потеряны. А если звонит черный телефон... ну, в общем, вам понятна идея. Каждое устройство использует собственную горячую линию связи с процессором, с тем чтобы попросить его сделать что-нибудь для себя. Когда звонит какой-либо конкретный телефон, процессор может немедленно определить, кому необходима помощь, а если он уже работает с каким-то другим запросом, то может назначить ему приоритет. При этом процессор ориентируется на важность запросов, ассоциированных с данным телефоном.

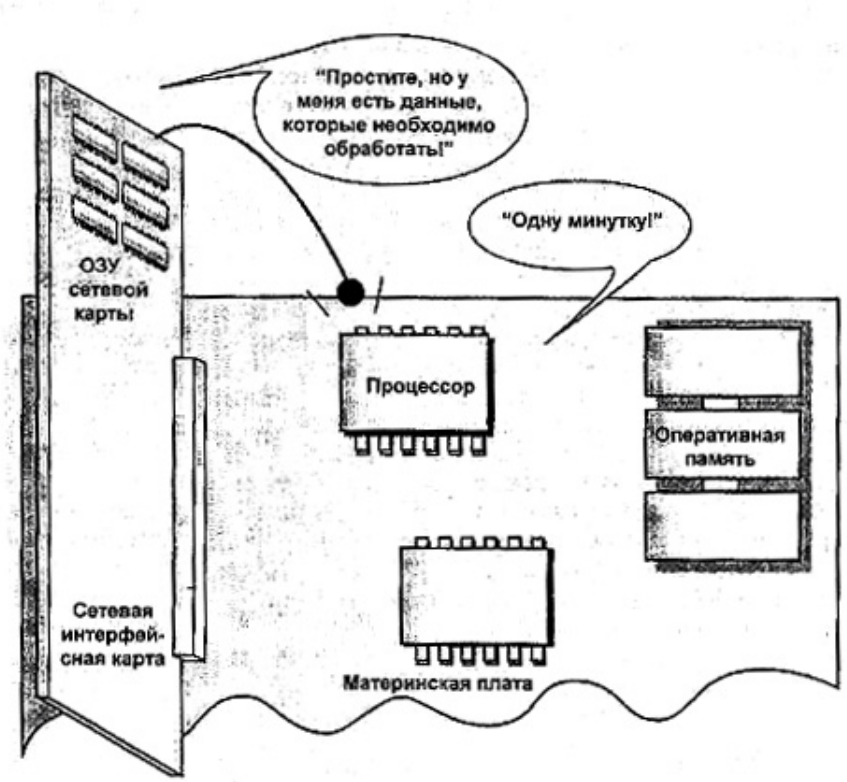


Рис. 4.4. Сетевая плата просит процессор переместить данные

Единственный недостаток метода — ограниченность числа телефонов. Действительно, в большинстве случаев каждому периферийному устройству нужна собственная телефонная линия — совместное их использование невозможно. Некоторые же устройства вообще могут использовать только один телефон из нескольких имеющихся. Так, ваша сетевая плата может работать только с голубым и оранжевым телефонами, а с пурпурным и черным — нет. Таким образом, вы должны назначить по одному телефону каждому устройству, которое необходимо использовать, причем эта линия должна быть одной из тех, с которыми может работать каждое конкретное устройство. Если вас когда-либо удивляло, почему многие сетевые администраторы преждевременно седеют или лысеют — это одна из причин.

Как все это работает? Аналогия с телефонами недалека от истины. В системной плате предусмотрены печатные проводники, которые работают как линии связи различных плат (установленных в слоты на шинах) с процессорами. Некоторые из этих линий называют *линиями запросов прерывания* (IRQ). Каждый слот системной платы содержит 16 линий IRQ, пронумерованных от 0 до 15.

Вообще говоря, каждому сетевому устройству, которому необходимы прерывания, следует назначить особую линию IRQ. Почему? Вернемся к аналогии с телефонами и предположим, что на столе у процессора стоят два красных телефона. Если они зазвонят одновременно, процессор не сможет установить, какому устройству следует уделить внимание. В таком случае одно из устройств, а возможно и оба, просто не будут работать. Когда звонит красный телефон, процессор не в состоянии установить, какое именно устройство обращается к нему. Поэтому он может игнорировать обе линии, а иногда отвечать

только по одной из них. Так, если назначить одинаковое IRQ сетевой плате и порту LPT2, иногда не будет работать плата, иногда — порт, а иногда и оба сразу.

Как определить, какие прерывания может использовать ваша сетевая плата, и какие из них свободны? Ответ на первый вопрос вы найдете в документации на сетевую плату. В ней обязательно должен быть список поддерживаемых прерываний. Большинство сетевых плат поддерживают два или три прерывания, одним их которых, вероятно, будет IRQ 5.

Совет

Если прерывания, поддерживаемые вашей платой, недоступны, а доступны другие прерывания, попробуйте найти в вашей системе устройство, которое можно переключить на свободное прерывание. Предположим, например, что сетевая плата поддерживает IRQ *5* и 10, однако свободно только IRQ 7. Если же звуковая плата использует IRQ *5,* но может поддерживать и IRQ 7, то переключите вашу звуковую плату на прерывание 7.

На второй вопрос можно ответить двояко. Один из методов заключается в тщательном документировании каждого прерывания, области буфера ввода/вывода (I/O buffer area), а также используемых каналов DMA. Запишите их на листе бумаги и храните этот лист в конверте, приклеенном к корпусу компьютера. Этот метод имеет два преимущества. Во-первых, вы всегда можете узнать конфигурацию компьютера, даже если он выключен. Во-вторых, можно с одного взгляда просмотреть всю конфигурацию компьютера, что не всегда возможно при работе с диагностическими программами. Единственный недостаток такого метода — необходимость постоянного обновления информации. Если этого не делать, все погибнет.

Ну, вообще-то, не совсем погибнет. Хотя исторически сложилось так, что диагностические программы не всегда оказываются на высоте, когда необходимо корректно идентифицировать ресурсы (в том числе IRQ), используемые каждым устройством, в Windows 95 ситуация изменилась. На вкладке Устройства (Device Manager) апплета Система (System) в Панели управления Windows 95/98, указываются ресурсы, используемые каждым устройством. Как показано на рис. 4. 5, достаточно выбрать устройство, о котором вам необходимо получить информацию, а затем щелкнуть на кнопке Свойства (Properties). На экране появится окно, содержащее значения параметров устройства. Выберите вкладку Ресурсы (Resources) и просмотрите список системных ресурсов, используемых конкретной сетевой платой (рис. 4.6).

На вкладке **Устройства (Device Manager)** можно не только увидеть текущую конфигурацию системы, но и провести ее реконфигурацию. Для изменения используемого устройством прерывания, щелкните на кнопке **Изменить настройку (Change Setting)** вкладки **Ресурсы (Resources)** окна свойств и введите новый номер прерывания из соответствующего диапазона. Если вы выберете номер прерывания, не поддерживаемый данным устройством, Windows 95 укажет вам на это и предложит иное значение. Если же выбранное прерывание поддерживается, но уже используется иным устройством, система предупредит вас о конфликте (рис. 4. 7). Если же вы допускаете конфликт устройств, Device Manager отобразит конфликтное устройство в списке прочих устройств, отметив его восклицательным знаком (рис. 4. 8).

Восклицательный знак возле значка устройства в списке установленных устройств не обязательно означает конфликт ресурсов. Он может извещать об иных проблемах устройства, которые не позволяют ему нормально работать.

Предупреждение

Пользователи Microsoft Windows могут использовать основанную на DOS программу MSD, как инструмент получения системной информации. Ее можно использовать для вывода информации о конфигурации системы. Однако чтобы эта информация была точна, программу следует запускать из DOS (но *не из окна DOS в Windows)* Обратите внимание: в предыду-

щем примере сетевой адаптер использует прерывание 11. После запуска на том же компьютере MSD, он сообщил, что IRQ 11 свободно и доступно для использования. Таким образом, вас ждет кошмарная работа по поиску неисправностей.

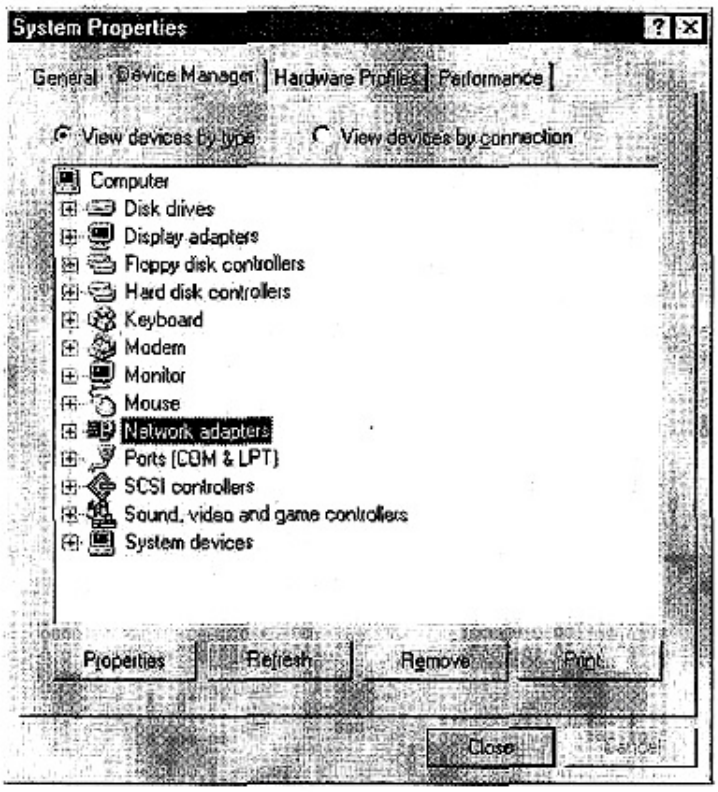


Рис. 4.5. Вкладка Устройства (Device Manager) Windows 95

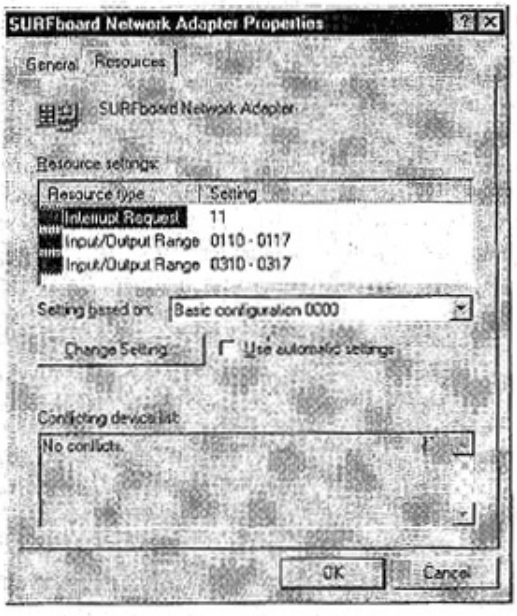


Рис. 4.6. Окно свойств сетевой платы

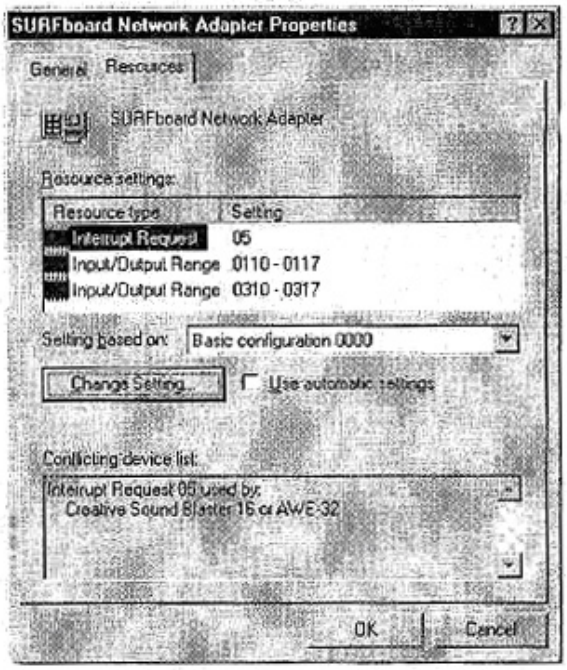


Рис. 4.7. Если вы назначите устройству прерывание, уже используемое другим устройством, Device Manager предупредит вас об этом

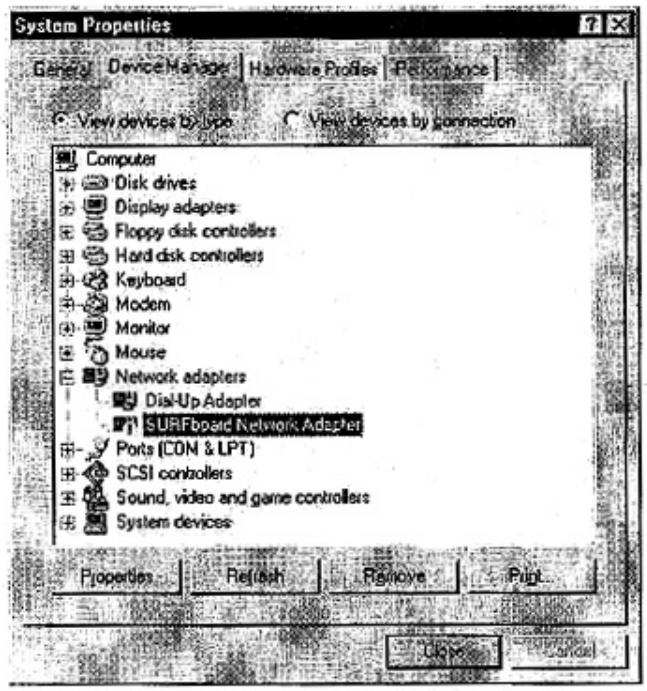


Рис. 4.8. Устройства, которые в настоящее время не работают, в списке отмечены восклицательным знаком

Куда направляются данные? Выбор базовых адресов ввода/вывода

Теперь вы знаете, каким образом сетевая плата привлекает внимание процессора, когда у нее есть информация, которую следует передать. Где же хранится эта информация?

И (вопрос, связанный с предыдущим) где хранятся инструкции, которые процессор передаёт периферийным устройствам?

Ответ на оба вопроса лежит в адресах ввода/вывода. По существу, это просто адреса почтовых ящиков, которые процессор может использовать как для размещения данных, ожидающих обработки, так и инструкций устройству, которому принадлежит адрес (диапазон адресов ввода/вывода). Каждое устройство должно иметь собственный адрес, ввода/вывода, для того чтобы процессор передавал соответствующие инструкции каждому устройству. Это позволяет избежать путаницы, при которой, например, процессор "приказал" бы сетевой плате воспроизвести звук. Поэтому, для избежания конфликтов, необходимо либо указать устройству, какие адреса ввода/вывода оно должно использовать, либо позволить системе самой себя сконфигурировать. *Базовым* адресом ввода/вывода называют тот, который задает нижнюю границу диапазона адресов ввода/вывода.

Примечание

Как правило, вам достаточно задать базовый адрес ввода/вывода, а остальные устанавливаются автоматически. Однако, некоторые платы требуют полного задания диапазона, позволяя выбрать один из поддерживаемых платой.

Зачем нужны буквы в адресах памяти

Адреса ввода/вывода и памяти компьютера записывают в шестнадцатеричном формате, подобном хорошо знакомой десятичной системе счисления. Это делают по различным причинам, но в основном потому, что компьютеры работают в *двоичной* системе счисления, а двоичные числа слишком длинны и громоздки для людей. Если же вы похожи на одну мою знакомую, которая может шутя переводить автомобильные номера в двоичную систему счисления, я снимаю перед вами шляпу. Если бы она, засмеявшись, не представила этому простое объяснение, я, вероятно, попала бы в аварию, начав преобразовывать числа во время поездки на автомобиле.

Чтобы облегчить работу с двоичными числами, программисты сначала использовали восьмеричную систему счисления, а сейчас – шестнадцатеричную. Она позволяет выразить числа в более удобной форме. Почему не используются десятичные числа? Главным образом из-за использования байтов (1 байт равен 8 битам). Десятичная система счисления не слишком удобна для работы с байтами, так как для этого предпочтительней такая система счисления, в которой проще выполнять деление на 4.

Однако в десятичной системе счисления тем более нет шестнадцати различных символов, необходимых для выражения шестнадцатеричных чисел. Поэтому для их выражения используют буквы алфавита – отсутствие шести цифр возмещают буквы A-F. Следовательно, вплоть до числа 9 шестнадцатеричные и десятичные числа одинаковы. Начиная с числа 10, они различаются. В шестнадцатеричной системе числу 10 соответствует буква A, 11-B, 12-C и т. д., вплоть до числа 16, когда запас букв кончается. 16 в десятичной системе соответствует 10 в шестнадцатеричной, 17-11 в шестнадцатеричной и т. д. Шестнадцатеричные числа часто записывают с буквой «h» в нижнем регистре в конце, так что вы можете распознать шестнадцатеричное число, например, 330h. Буква «h» в число не входит.

При желании вы сможете научиться вручную преобразовывать числа из одной системы в другую, но для большинства из нас простейший способ конвертирования шестнадцатеричных чисел в десятичные заключается в запуске калькулятора Windows в режиме Научный (Scientific). Убедитесь, что калькулятор установлен на отображение *исходной* числовой системы (например, шестнадцатеричной). Затем введите число и переключите текущую систему счисления на ту, в которую желаете преобразовать число. Это не столь головоломная задача, как конвертирование в уме, но вы же не обязаны сообщать всем, что используете калькулятор Windows!

Получение информации CPU - прямой доступ к памяти

Мы уже обсудили, каким образом сетевая плата привлекает внимание процессора, чтобы сообщить о наличии у нее информационного пакета. И, однако, даже если процессор узнал об этом, каким же образом информация *фактически* передается из процессора в оперативную память?

В первых персональных компьютерах, появившихся в начале восьмидесятых годов, передача данных от сетевой платы в оперативную память выполнялась процессором, чему последний отнюдь не радовался. Почему? Да потому, что когда информация передавалась из платы компьютера в основную память, она проходила через процессор по одному биту за раз (рис. 4.9). Этот метод передачи информации известен как *программируемый ввод/вывод (PIO)*. Метод PIO значительно загружает процессор, а это означает, что у процессора остается меньше времени на выполнение прочей работы.

В середине восьмидесятых годов появилась новая БИС, известная как микросхема контроллера *прямого доступа к памяти* (DMA), реализующая в компьютерах принципиально новый способ передачи данных. Как мы уже знаем, когда на компьютер поступает пакет, он направляется в память сетевой платы. В этот же момент сетевая плата направляет в процессор запрос прерывания, в котором просит сделать что-нибудь с только что принятыми данными. С установленной на системной плате микросхемой контроллера DMA процессору более не приходится прекращать работу и самому заниматься передачей данных. Вместо этого он может приостановить на мгновение вычисления какой-нибудь огромной электронной таблицы и сказать микросхеме контроллера DMA на материнской плате: "Пожалуйста, передайте эту нужную мне информацию и дайте знать, когда закончите". Реальная ценность прямого доступа к памяти заключается в том, что современные микросхемы контроллеров DMA передают информацию в любом направлении, не отвлекая процессор от вычислений.

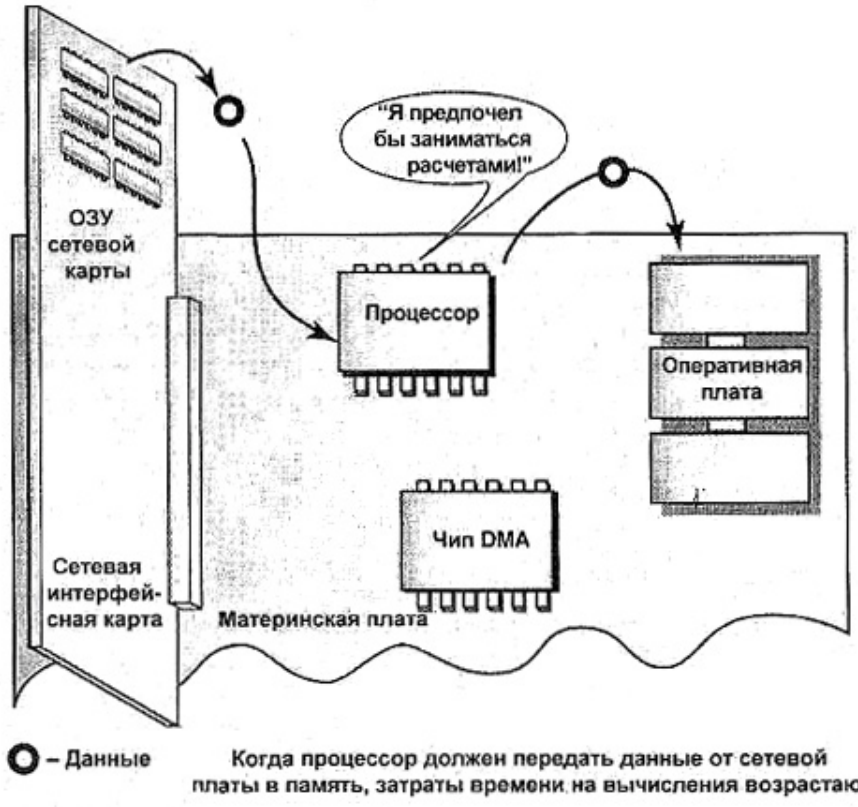


Рис. 4.9. Процессор передает данные сетевой платы в оперативную память

Когда микросхема контроллера DMA заканчивает передавать информацию, она сообщает процессору о выполнении задачи. Как показано на рис. 4. 10, установка микросхем контроллера DMA на системной плате повышает эффективность обработки и передачи информации в любой компьютерной системе.

На современные системные платы устанавливают две микросхемы DMA. Каждая микросхема контроллера DMA поддерживает четыре *канала DMA* (выделенных путей передачи информации). Таким образом, на материнской плате предусмотрены восемь каналов DMA, пронумерованных от 0 до 7.

Как и в случае с линиями IRQ, чтобы избежать заторов в передаче данных, и сбоев системы, каждое устройство, применяющее DMA, должно использовать уникальный канал DMA. К сожалению, нет программных утилит, позволяющих получить корректные данные. Лучший способ отслеживания реальной загрузки каналов DMA — документирование параметров ваших плат, выполненное при инсталляции. Поскольку большинство плат особенно новейших образцов - не используют каналы DMA, эта задача не столь сложна.

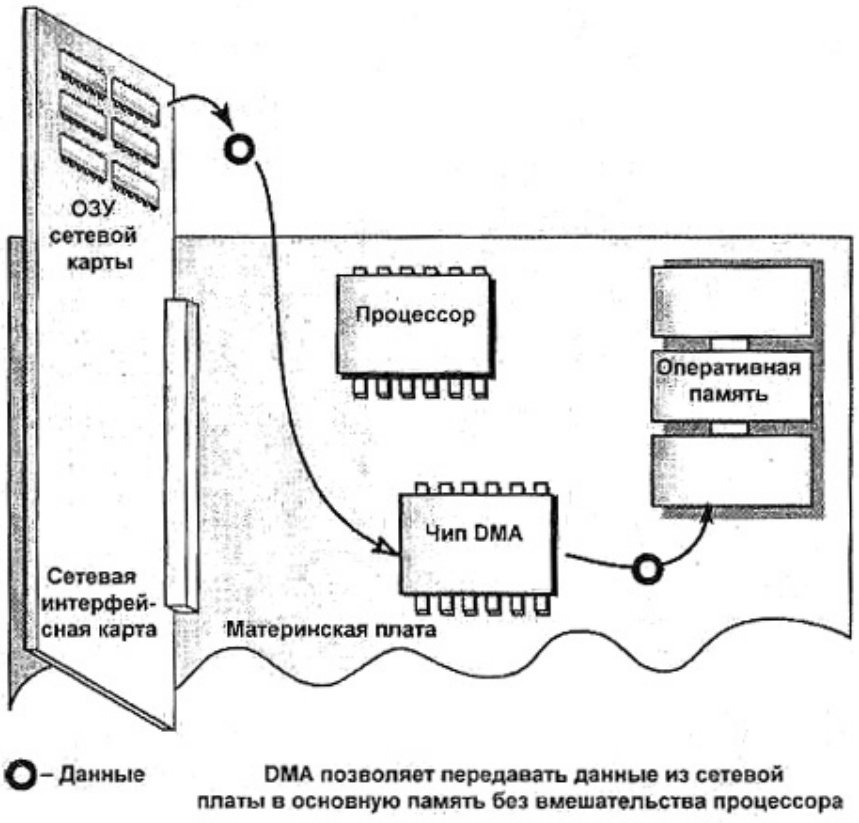


Рис. 4.10. Передача информации из памяти с помощью микросхемы DMA

DMA используют не только на системных платах. Некоторые сетевые ты специального типа, называемые *сетевыми интерфейсными платами с управлением шиной* (bus-mastered network interface card) — фактически, это может быть любая плата — тоже имеют в своем составе микросхемы DMA. Почему их называют платами с "управлением шиной"? Слоты, в которые Вставляют видео-, звуковую, SCSI-плату и т. д. называют *слотами расширения (expansion slots)* иди *слотами шины (bus slots).* Плата же, установленная в слот шины, должна контролировать, т. е. *управлять* передачей данных по собственному каналу DMA. Отсюда и произошло выражение "управление шиной" (bus-mastered). Платой с

управлением шиной (bus-mastered card) можно назвать любую плату, на которой установлена микросхема DMA. В настоящее время можно приобрести сетевые платы, платы контроллеров жёстких дисков и платы SCSI, в которых предусмотрено управление шиной.

В 1998 г фирма IBM выпустила несколько образцов плат с управлением шиной. Фирма уверяла, что размещение микросхем DMA на плате ускоряет как работу платы, так и передачу по каналу DMA в большей степени, чем при размещении двух микросхем DMA на системной плате. Как оказалось, фирма IBM была права. Используя собственные микросхемы DMA, сетевая плата с управлением шиной (ведущая плата) может связываться с оперативной памятью системы без вмешательства процессора (рис. 4. 11).

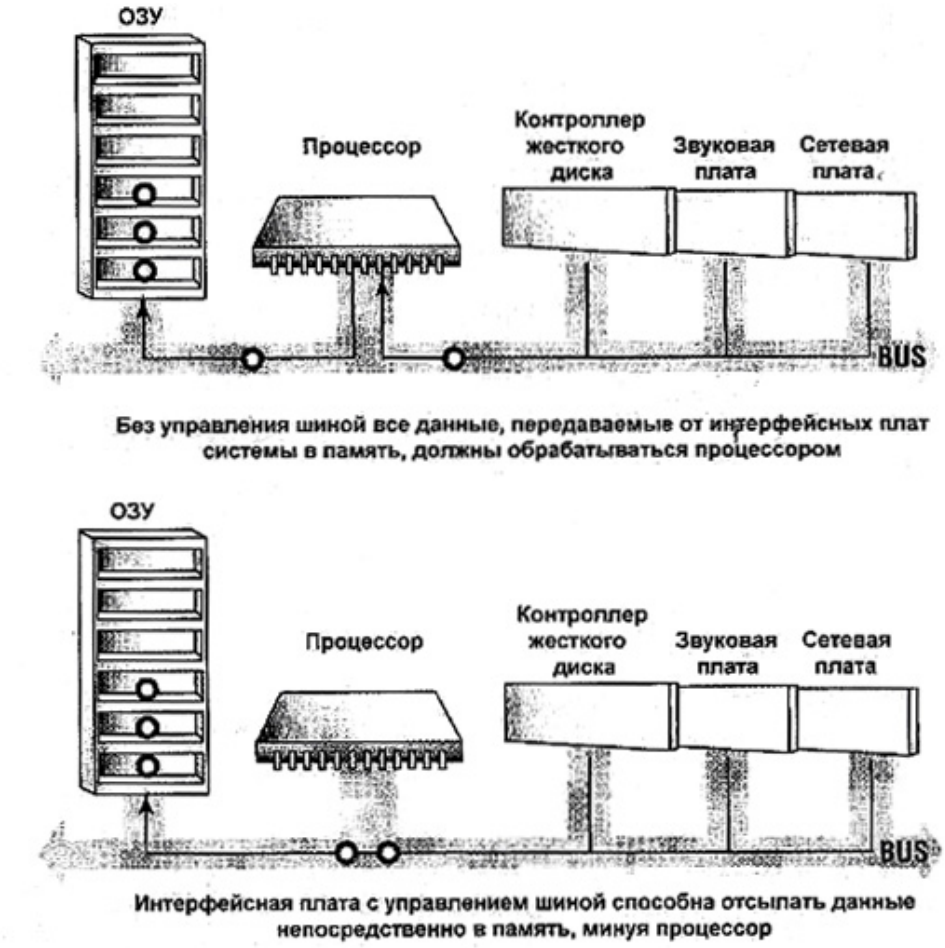


Рис. 4.11. Сетевые платы с управлением шиной могут передавать информацию без помощи процессора

Выводы

В этой главе рассматривались работы, связанные с монтажом кабельной сети и сетевых плат. Обе задачи несложны, однако без соответствующей подготовки затруднения неизбежны.

Самое главное при прокладке кабелей — планирование. Прежде всего, тщательно проработайте схему. Обеспечьте вашей системе гибкость. Чтобы впоследствии можно было расширить сеть, не поскупитесь на приобретение кабелей и прокладку как можно более широких кабельных каналов. Самая дорогостоящая часть сети — отнюдь не компьютеры,

а кабельная сеть. Её нелегко проложить, но еще труднее обновить. Спланируйте все так, чтобы выполнить эту работу раз и навсегда. И, наконец, тщательно документируйте всю сеть — когда придет пора искать причину сбоев, вы сразу найдете неисправный кабель.

Сетевые платы подобны всем остальным платам в компьютере. При установке вы должны сконфигурировать их, задав прерывания, адреса ввода/вывода и, возможно, каналы DMA для ускорения обмена данными между сетевой и материнской платами. И опять-таки, надлежащее документирование — либо на бумаге, либо с помощью диагностических программ — ключ к безотказной работе плат. В первых четырех главах мы изучили основные этапы создания локальных сетей. Прежде чем завершить обсуждение каналов, мы рассмотрим различные устройства, необходимые для их соединения и расширения: концентраторы, маршрутизаторы, мосты и т. д.

Упражнение 4

1. IRQ 5 и 7 в вашем компьютере не используются. Вы должны установить сетевую плату, которая поддерживает IRQ 10 и 1. 1. Возможно ли установить сетевую плату? Если возможно, то каким образом, а если нет, то почему? Что нужно сделать, чтобы установить плату?
2. Что из перечисленного ниже используется в современных сетевых платах? Выберите все, что используется.

    A. Базовые адреса ввода/вывода.
    B. Каналы DMA.
    C. IRQ.
    D. Ничего из перечисленного выше.

3. Если кабель прокладывают под полом, где лучше всего его проложить? Почему?
4. Можно ли использовать перекрывающиеся диапазоны адресов ввода/вывода двух плат адаптеров, если использовать разные базовые адреса ввода/ вывода. Да или нет?

Глава 5

Дополнительное сетевое оборудование

Создать отдельную сеть - это еще не все. Скорее всего, ее нужно будет сразу же подсоединить к другой сети, или к какому-либо другому узлу. Вот здесь как раз тот самый момент, когда начинается переход от простых сетевых топологий к более сложным. Об этом мы говорили в гл. 2, где было начато рассмотрение интра- и интерсетей, а также применяемых для них устройств.

Что же такое интрасетевые *и* интерсетевые устройства? Главное отличие между ними состоит в том, что *интрасетевые,* устройства расширяют *вашу* сеть, а *интер*сетевые — связывают две различные сети (или несколько сетей любой протяженности и размера). В некотором смысле это не вполне точное разделение, поскольку иногда сложно сказать, где кончается одна сеть и начинается другая. Некоторые устройства содержат средства и для расширения, и для связывания сетей, но, тем не менее, такое разделение устройств на интрасетевые/интерсетевые — отправная точка организации сетевого аппаратного обеспечения.

Совет

Чем выше уровень модели OSI, на котором функционирует какой-либо компонент сетевого оборудования, тем более вероятно, что он (компонент) предназначен для связывания или объединения отдельных сетей, а не для расширения одной сети. Например, концентратор связывает две части единой сети Ethernet, *а* маршрутизатор применяется для связывания локальных сетей Ethernet с Internet.

Вначале предполагалось, что в этой гл. будет описана привлекательная на вид, аккуратная модель, устанавливающая соответствие между сетевым аппаратным обеспечением и отдельными уровнями модели OSI (см. гл. 1). Это заманчивая идея, но она не очень применима на практике по одной простой причине. Хотя, в принципе и возможно разделить функциональные возможности сетевого аппаратного обеспечения по этим уровням (функциональные средства физического, канального уровней, и т. д.), сами устройства не поддаются такой классификации, поскольку выполняемые ими функции неоднозначны. Например, мосты в целом функционируют на канальном уровне, но большинство современных мостов могут работать и на сетевом уровне модели OSI. Модель OSI является удобным методом организации обмена информацией, описывающим все то, что происходит в сети, но она не всегда адекватна реальному миру, а в данном случае она вообще может оказаться малопригодной, поэтому в данной гл. не уделяется большого внимания результатам применения OSI для организации сетевого аппаратного обеспечения.

Теоретически можно разделить оборудование так, как это указано чуть ниже, и более детально описано в следующем разделе.

- Повторители — физический уровень.
- Мосты/концентраторы/коммутаторы — канальный уровень.
- Маршрутизаторы — сетевой уровень.

Модели сетевых функциональных средств

Некоторые аспекты функционирования сетевого оборудования можно описать в соответствии с достаточно простой моделью, если, конечно, не требовать слишком многого от этой модели.

Устройства физического уровня, подобно повторителям, работают как «удлинители» сетевых кабелей (точнее магистральные усилители телефонного или телевизионного сигнала. – Прим. ред.), передавая сигналы на большее расстояние, чем это можно было сделать без них.

Устройства канального уровня выполняют функции, специфические для сетей определённого типа, Ethernet и Token Ring. Степень сложности этих функций варьируется в зависимости от устройства. Например, концентраторы обеспечивают подключение клиентов сети равноправным образом; коммутаторы позволяют пересылать информацию только в отдельный сегмент, в котором может быть найден адрес места назначения кадра; мосты связывают две совершенно разные сети.

Канальный уровень модели OSI сам по себе не является монолитным, а подразделяется на два подуровня: управление доступом к среде передачи (MAC – Media Access Control) и связь логических каналов (LLC – Logical Link Control). Уровень MAC имеет отношение только к аппаратным адресам и передаче данных без логического соединения, в то время как на уровне LLC выполняется фактическое подключение перед пересылкой данных. Большая часть устройств канального уровня имеет, в основном, отношение к функциям на уровне MAC, но, как вы увидите далее, мосты могут использовать некоторые возможности, определённые на уровне LLC.

Устройства сетевого уровня, подобно маршрутизаторам, имеют дело с различными сетевыми протоколами, например, IPX/SPX или TCP/IP, но не с различными типами сетей.

Не задерживайтесь слишком долго на всех этих различиях, поскольку они не всегда справедливы. Например, современные мосты и маршрутизаторы "перекрывают" свои возможности; некоторые коммутаторы имеют средства, характерные для мостов; каждое устройство в сети Ethernet, подключенное к источнику питания, может рассматриваться как повторитель. Конечно, приведенной выше классификации сетевых устройств до некоторой степени можно доверять, Например, если вам просто требуется подключить сеть к Internet, вряд ли вы найдете нужные для этого функциональные возможности в концентраторе. Однако и это не совсем справедливо. Вместо рассмотрения модели OSI, подумайте лучше о том, какие средства вам необходимо добавить к своей сети, и выберите нужное для этого устройство. Это значит, что вам придется провести много времени, читая таблицы спецификаций и сравнивая функциональные возможности различных программ и устройств, но, так или иначе, делать это придется.

Повторители для расширения доступа к сети

Повторители — это устройства, регенерирующие электрические или световые сигналы для увеличения расстояния, на которые сигнал может распространяться (с заданным соотношением сигнал/шум. — Прим. ред.). Все повторители усиливают сигнал путем его "распаковки" и повторной передачи. Они не позволяют соединять несовместимые сети, фильтровать пакеты и маршрутизировать данные в другие подсети.

Единственная задача повторителей — устранение ослабления (затухания) сигнала. Ослабление сигнала кратко рассмотрено в гл.". *3*. Напомним приведенное, там утверждение: "При прохождении по линии связи сигнал становится слабее". Чем слабее сигнал, тем легче он "повреждается" другими сигналами. Это не новость для тех, кто пользовался радиоприемником при поездках на автомобиле. Скажем, вы едете по шоссе и слушаете музыку, передаваемую какой-либо местной радиостанцией. Как только ваш автомобиль приблизится к границе зоны уверенного приема, музыка не пропадет сразу, а начнет прерываться и перебиваться передачей спортивного состязания, осуществляемой радиостанцией, расположенной в новом месте. Музыка будет постепенно ослабевать, а спортивная передача — усиливаться. То, что происходит с радиосигналами, происходит и в сети, независимо от типа сигнала, степени экранирования кабеля или защищенности от помех. Рано или поздно сигнал будет ослаблен до состояния, когда он перестанет Выть "понятным" его получателям.

Для решения проблемы ослабления сигнала можно применить, два подхода. Первый: можно усилить сигнал, повысив его, уровень, как это делается на всех мощных радиостанциях. Это не повлияет на качество сигнала в пределах исходной области вещания, однако расширит зону уверенного приема. Сигнал все равно ослабеет, но более мощный исходный сигнал будет проходить большее расстояние, прежде чем это случится.

Второй подход, используемый в сетях (и заложенный в конструкцию повторителя), заключается в усилении сигнала перед его повторной передачей (ретрансляцией). (Такая ситуация возникает при трансляции одной и той же радиопрограммы (например общенационального канала новостей) на некоторой территории, размеры которой не позволяют одной радиостанции "покрыть" всю зону приема. Поэтому на всей этой территорий устанавливается сеть относительно маломощных радиопередатчиков; излучение которых "накрывает" область распространения сигнала электромагнитным полем, напряженность которого достаточна для уверенного и непрерывного приема сигналов..— Прим. ред.)

Что может сделать повторитель

Усиливая сигнал, повторители делают несколько полезных вещей сразу. Во-первых, в сетях Ethernet они устраняют конфликты или позволяют построить более протяженную сеть и избавить ее от конфликтов. Во-вторых, они могут предоставить вам возможность изолировать часть сети.

Примечание

Все сегменты сети, соединенные с помощью повторителей, должны применять одинаковые протоколы канального и сетевого уровня. Это значит, что нельзя использовать повторитель

для связи сетей Token Ring с сетями Ethernet, или связывать сеть Ethernet с протоколом IPX/SPX с сетью Ethernet с протоколом TCP/IP. Обе сети должны быть одного типа (Ethernet) и поддерживать один и тот же транспортный протокол.

Устранение конфликтов

Подобно другим широкополосным сетям, в сети Ethernet есть только один "путь", по которому данные могут путешествовать в текущий момент времени. Как было указано в гл. 3, в сетях Ethernet конфликты возникают тогда, когда две или более сетевых плат в персональных компьютерах одновременно начинают передачу данных в сеть. Поэтому перед тем, как компьютеры начинают передачу данных, они "прослушивают" сеть, чтобы удостовериться, что она свободна. Однако ПК могут только "слушать", поэтому если узел, находящийся слишком далеко от другого узла, чтобы его можно было там услышать (но в том же самом сегменте сети), также начнет передачу, то произойдет конфликт. По общепринятому соглашению, конфликты — "врожденное" свойство сети Ethernet, и их появление не является неожиданностью для корректно работающей сети, но они могут замедлить ее работу, поскольку требуют повторных попыток передачи. Итак, число конфликтов должно быть сведено к минимуму. Повторители могут помочь устранить лишние конфликты усилением сигнала, после чего сетевые ПК "услышат" друг друга.

Изолирование сегментов

Сегменты Ethernet, особенно построенные по физической шинной топологии (при которой все ПК совместно используют единственную магистраль), более всего подвержены простоям, вызванным разрывами кабельных соединений. Если какие-либо части сети больше других подвержены простоям, применение повторителя позволит "изолировать" эти сегменты, позволяя им "немного поостыть" и не мешать работать остальной сети. Например, в фирме, обучающей работе на ПК, хотят предоставить ее ученикам возможность попрактиковаться на компьютерах. Для этого вы устанавливаете некоторую часть сети отдельно и даете учащимся возможность поработать с рабочими станциями в сети и макетами серверов, заранее предвидя весь тот беспорядок, который при этом возникнет. В конце концов, самым худшим из того, что вам менее всего хотелось бы увидеть, будет некая персона, играющая с почтовым сервером в игру "Что случится, если я сделаю *это*?". Однако поскольку "учебный" сегмент изолирован от остальной части сети, то оборванные кабели, не завершенные сеансы и другие сетевые проблемы окажут малое воздействие на функционирование остальной части сети. Это тот случай, когда повторители могут вам очень помочь; даже если длина кабельных сегментов не превышает максимально допустимого значения 185 м и нет нужды в повторителях для расширения сети, имеет смысл использовать их для предотвращения воздействия "мертвых" частей сети на "живые".

Как работают повторители

Итак, теперь вы знаете, что функция повторителей заключается и регенерации сигнала с тем, чтобы он мог пройти большее расстояние. Строго говоря, это не совсем так. Вместо того чтобы просто усиливать сигнал, повторители "распаковывают" и повторно выполняют его широковещательную передачу. По сути дела, происходит следующее: когда пакеты данных поступают на повторитель, устройство принимает их и преобразует в ту форму, которую они имели перед отправлением. Повторитель фактически не воздействует ни на данные, ни на адресную информацию. Однако он заново создает сигнал с "ну-

левой отметки", а не просто пересылает исходный сигнал. Ранее уже говорилось, что в процедуру обработки сигнала не встроены средства контроля ошибок. Если пакет был поврежден при поступлении на вход повторителя, он таким и останется на его выходе.

Примечание

В сетях Ethernet любое устройство является повторителем.

Повторители и удлинители: сходства и различия

Вы, должно быть, уже уяснили, что повторители не просто повторяют сигнал, но фактически заново его упаковывают. Однако есть и устройства, которые *на самом деле* просто «повторяют» сигнал. Они называются *удлинителями* локальных сетей и выполняют как раз те функции, которые должны были бы выполнять повторители. Удлинители функционируют так же как и повторители в том смысле, что они позволяют «удлинить» сеть не увеличивая вероятность возникновения конфликта, и не увеличивая «число повторений» (repeater count). Что такое «число повторений»? Если в одной сети имеется четыре повторителя, то их количество и называется *числом повторений*.

Нет каких либо оснований *не* использовать повторители вместо удлинителей, за исключением того, что нельзя использовать в одной сети слишком много повторителей, а вот на количество удлинителей никакие ограничения не накладываются.

В приведенной выше вставке при сопоставлении повторителей и удлинителей вводится параметр — число повторений. Не следует устанавливать более четырех повторителей в одну отдельную сеть, иначе могут случиться большие неприятности (например, сбои сети или задержки в ее работе). Это происходит по двум причинам.

Первая: большое количество повторителей может увеличить число конфликтов в сети. Каждый раз, когда в повторителях происходит "разборка" и "сборка" пакета данных, работа сети немного замедляется. Эта задержка не так велика, чтобы иметь решающее значение, если пакет "разбирается" один раз, но чем больше повторителей в сети, тем больше становится таких задержек. В итоге задержки будут аккумулироваться, пока не возникнет ситуация, при которой посылающий узел будет слишком долго ждать возврата сигнала подтверждения успешной передачи и в какой-то момент начнет повторную передачу данных. Проблема здесь заключается в том, что когда посылающий узел начнет это делать, исходный пакет всё еще будет проходить по сети. Если посылающий узел повторно пошлёт данные в то время, когда исходный пакет будет все еще медленно двигаться к конечному месту назначения, оба пакета вступят в конфликт. Опять-таки напомним, что в сетях Ethernet предусмотрено возникновение конфликтов, но не следует стремиться к увеличению их количества.

Вторая потенциальная проблема, возникающая из-за слишком большого количества повторителей, состоит в повреждении данных. Каждый раз, когда повторитель "разбирает" и "собирает" пакет, имеется некоторая вероятность того, что он некорректно повторно соберет данные, заменив, скажем, 0 на 1 в некотором узле на линии связи. (И это не мелочь, как это могло бы показаться на первый взгляд: двоичное число 11001100 в десятичном виде соответствует 204, но 11101100 будет соответствовать 236. Значит, какая-то величина в данных внезапно возрастет.) Это напоминает старую игру в испорченный телефон (Gossip), в которую вы, вероятно, играли в школе. Участник игры А шепчет что-то на ухо участнику В, В шепчет то. что он услышал, на ухо С, и все это проходит по кругу. В завершении участник О должен сказать, что он услышал, и это, как правило, будет чрезвычайно искаженной версией того, что А сказал вначале. Это, конечно, забавно (по крайней мере, третьеклассники получают от этого большое удовольствие), но в действитель-

ности не очень хорошо, когда то, что получено в искаженном виде, — не просто непроизносимая фраза, а ваши сетевые данные.

Правило, ограничивающее число повторителей в сети четырьмя, не является высеченной в камне заповедью: "Сеть будет плохо работать с четырьмя повторителями и погибнет в пламени, если вы добавите пятый". Тем не менее, сеть становится более ненадежной при увеличении количества повторителей, и четыре ретранслятора сигнала — верхний предел, рекомендуемый для применения в одной сети.

Концентраторы и подключение устройств

Термин "концентратор" является общим названием устройств, связывающих сетевые компоненты друг с другом. Этими устройствами может Выть любое оборудование: от простых коммутационных панелей до сложных устройств, соединяющих сети различных типов или же подключающих локальные сети к глобальной.

Термин "концентратор" используется применительно к устройствам, установленным в сети Ethernet. В сетях Token Ring используются устройства MAU (Multistation Access Unit - устройство многостанционного доступа), которые, как и сами сети, функционируют не так как концентраторы в сетях Ethernet. Однако и концентраторы, и устройства MAU выполняют одну и ту же основную функцию, — подсоединяют персональные компьютеры к сети.

Типы концентраторов

Большинство концентраторов относятся к одной из трех разновидностей.

- Автономные (stand-alone).
- Наращиваемые (stacked).
- Модульные (modular).

Автономные концентраторы являются именно тем, на что указывает их название — устройствами, требующими (или, что бывает реже, не требующими) источников питания, в состав которых могут входить (а могут и не входить), средства для подсоединения к другим концентраторам с помощью коротких отрезков кабеля, например, оптоволоконного, или витой пары (в этом случае они называются наращиваемыми). На рис. 5.1 показаны автономные концентраторы.

Совет

Неуправляемые автономные концентраторы хороши тем, что они не дороги (например, LinkSys с пятью портами для ПК может стоить всего 59 $), однако следует учесть, что чем больше портов, тем они дороже. Если вам не требуются средства управления, то возможно дешевле купить два автономных концентратора и связать их вместе, чем покупать один большой.

Модульные концентраторы имеют встроенную объединительную плату, которая позволяет подключать к концентратору дополнительные платы, как это показано ни рис. 5.2.

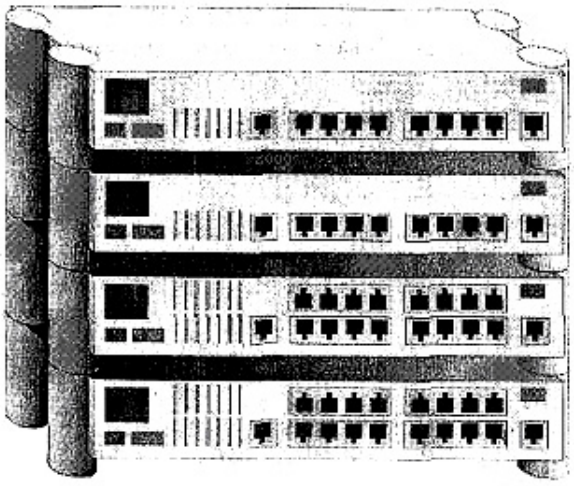


Рис. 5.1. Автономные концентраторы, используемые как отдельно, так и вместе с другими

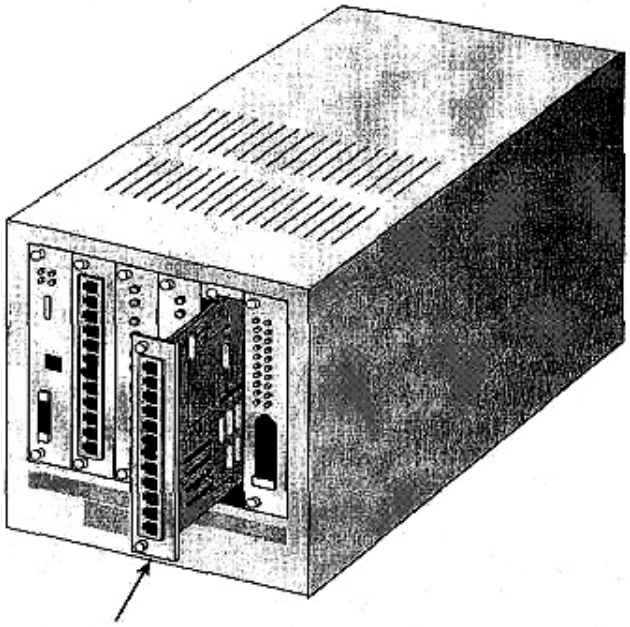


Рис. 5.2. Модульные концентраторы напоминают материнскую плату компьютера

Если встроенное устройство является "интеллектуальным" (см. следующий раздел), то концентраторы с модульной или наращиваемой структурой могут работать под управлением одного из концентраторов, называемого главным (master), в то время как остальные будут подчиненными (slave). Чем следует руководствоваться при выборе между модульным или наращиваемым концентратором? В основном это зависит от того, как вы планируете расширять свою сеть. Можете добавлять модули в стационарно установленный концентратор или же покупать наращиваемые концентраторы и распределять их по всему зданию, устанавливая там, где они нужны.

Сравнение концентраторов разных типов

Концентраторы выпускаются в достаточно широком ассортименте: от самых простых, работающих как устройства для стыковки кабелей, до таких, которые предоставля-

ют пользователю набор усовершенствованных технических средств управления. Теоретически можно разделить концентраторы на три категории:

- пассивные;
- активные;
- интеллектуальные, или управляемые (два термина, обозначающие одно и то же).

Пассивные концентраторы представляют собой устройства, не требующие питания, напоминающие коммутационные панели, для стыковки кабелей в передачи данных в обоих направлениях. Применение их ограничено. Например, они пригодны для разводки сетевых связей внутри здания, но, вероятнее всего, в большинстве сетей вы встретите активные и/или управляемые концентраторы.

Примечание

Все полностью пассивные устройства не требуют питания, в то время как концентратор, снабженный блоком питания, регенерирует сигналы и поэтому является активным.

Активный концентратор (любой концентратор с блоком питания) обладает свойствами повторителя, поскольку выполняет "распаковку и упаковку" сигнала так, как это описано в предыдущем разделе данной главы, посвященной повторителям. Во всех других отношениях активные концентраторы выполняют те же функции, что и пассивные. Они просто гарантируют, что помещенные в сеть данные посредством широковещательной передачи попадут в каждый подсоединенный сегмент, так что каждый узел, которому эти данные предназначены, сможет их прочитать. Другое их важное достоинство состоит в том, что большинство активных концентраторов снабжено *индикаторами состояния (status lights).* Если соединение ПК с сетью работает, то индикатор порта, к которому он подсоединен, будет включен. Если же ПК подсоединен к сети, то индикатор будет выключен. Другой индикатор состояния на концентраторе в случае конфликта загорается жутковатым красным гнетом, но напомним, что конфликты являются обычной ситуацией в сети Ethernet.

Интеллектуальные, или управляемые концентраторы имеют модуль, позволяющий им делать немного больше, чем просто перемещать данные по сети. Они могут использоваться для помощи при поиске или отслеживании неисправностей в вашей сети, имеющей звездообразную топологию. Если вы увидите в продаже концентратор с интерфейсом MDI (Managed Device Interface — интерфейс управляемого устройства), то это как раз и есть интеллектуальный концентратор.

В гл. 14 будут описаны протоколы сетевого управления. Суть идеи такова: протоколы управления, как и SNMP (Simple Network Management — простой протокол сетевого управления), состоят из двух частей. На управляющем сервере запускается программа-монитор, а на тех устройствах, которые допускают управление, — программы-посредники. Монитор и посредники могут связываться друг с другом. В протоколе SNMP (типичном протоколе управления) монитор запрашивает посредников и собирает поступающую от них информацию, в которой содержится следующее.

- Состояние концентратора и/или порта, а также информация об их активности.
- Статистика производительности работы по каждому порту.
- Сетевая схема всех совместимых с SNMP аппаратных средств, имеющихся в сети.
- Журнал регистрации сетевых ошибок и сетевой активности.

Можно использовать программные средства, предназначенные для управления устройствами, и выполнять следующие задачи.

- Вносить изменения в систему защиты сети, устраняя возможность несанкционированного доступа пользователей к концентратору.
- Устанавливать границы допустимой активности, уровней ошибок и производительности работы, с тем, чтобы в случае выхода параметра за установленные границы, получить об этом информацию.

Примечание

Приведенные выше сведения являются лишь примером той информации, которая может быть получена с помощью управляемых концентраторов, но это далеко не полный перечень всего того, что можно получить от них. Полная информация зависит от возможностей программы-посредника и может быть разной для различных моделей концентраторов.

Управляемые концентраторы не всегда необходимы. Если сеть имеет только один концентратор типа 5+1, и этот концентратор легкодоступен, то вы сможете проконтролировать его лично, причем для этого потребуется просто обратиться к программе диагностики. Чем больше ПК установлено в сети, тем сложнее получить доступ к концентратору и выполнить его диагностику. То, что очень просто делается в сети с одним концентратором, становится кошмаром в сети с 10 концентраторами, с 16 портами у каждого. В данном случае только применение специального программного обеспечения поможет вам справиться с работой, когда настанет время поиска неисправностей.

Совет

При выборе управляемого концентратора выбирайте такие управляющие модули, программное обеспечение которых записано во флэш-память. В этом случае, когда настанет время усовершенствования системы, вы сможете просто модернизировать модули вместо их замены.

Архитектура концентратора

В самом общем понимании концентраторы представляют собой устройства, позволяющие электрически соединять между собой кабели, которые не могут быть подключены друг к другу напрямую. Логическая топология сети и тип используемых кабелей (по определению) не имеют к этому никакого отношения, так же как и вид исполнения. Однако концентраторы являются составной частью сети, построенной по *физической* звездообразной топологии (рис, 5.3).

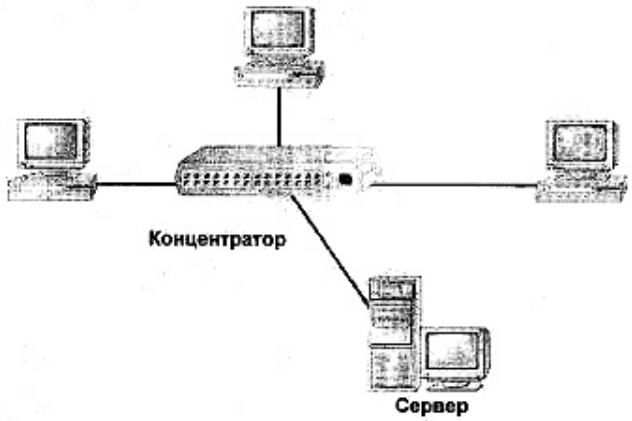


Рис. 5.3. Концентратор является центральным узлом в сети, построенной на основе физической звездообразной топологии

Порты, (в разъемы которых вы вставляете кабели для подключения компьютеров) являются существенной частью любого концентратора (рис. 5.4). Порты играют важную роль, поскольку они определяют следующее.

- Тип кабеля, который можно подключить к концентратору.
- Количество ПК, подключаемых к одному концентратору.
- Возможность наращивания концентратора и средства дистанционного управления им при отказе сети.

Как и в случае с сетевыми платами, конструкция разъемов портов концентратора зависит только от типа кабельных разъемов. Например, для тонкого коаксиального кабеля и кабеля UTP требуются различные разъёмы: разъёмы для кабеля STP отличаются от разъемов для оптоволоконного кабеля. Подобно другим сетевым устройствам концентраторы могут использоваться только с теми типами кабелей, на которые они рассчитаны. Подобно другим устройствам, если у концентраторов совпадают подключаемые сетевые кабели, то они логически совместимы. Это значит, что если вы купите концентратор, допускающий подключение разъема RJ-45, используемого для кабелей UTP, то вы сможете применить этот концентратор для своей сети 10BaseT независимо от того, в каком магазине он приобретен - на физическом уровне интерфейс останется прежним. Для создания работоспособного сетевого соединения концентратору следует обеспечить электропитание и подключить к нему все кабели.

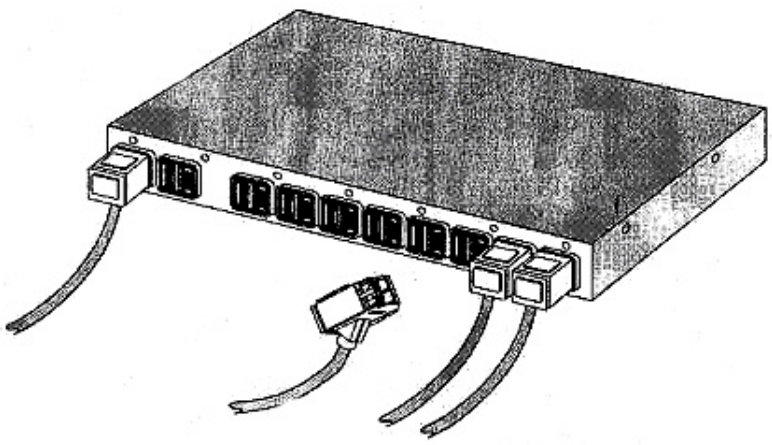


Рис. 5.4. Подключение кабелей к концентратору

Примечание

Некоторые концентраторы снабжены портами для кабелей различных типов. Это позволяет использовать их в сетях нескольких типов, так что вы сможете, к примеру, подключить компьютер AS400 к локальной сети 10BaseT, созданной на основе ПК. Также можно подсоединить концентраторы к сети с логической звездообразной распределенной топологией, в которой в качестве магистральных кабелей применяется толстый коаксиальный или оптоволоконный кабель.

Все эти порты сами по себе не приносили бы никакой пользы, если бы не подключенные к ним внутренние средства, которые позволяют пересылать пакеты из одного кабеля в остальную часть сети. Для того чтобы порты и подключенные к ним узлы могли обмениваться данными, в концентраторе используется внутренняя системная шина, обеспечивающая для каждого порта прием и передачу данных по подключенным линиям. Способ, по которому данные пересылаются между портами, зависит от типа сети. Например, в сети Ethernet выполняется широковещательная передача данных одновременно всем компонентам сети. Они должны сами определять, предназначены ли пакеты для них или их следует игнорировать. Таким образом, данные, приходящие на концентратор от ПК в сети Ethernet с помощью широковещательной передачи, пересылаются во все сегменты, подключенные к концентратору, как это показано на рис. 5.5.

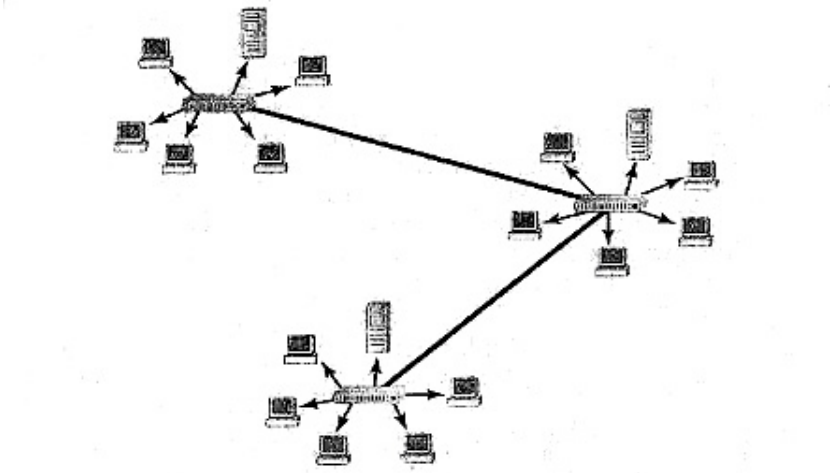


Рис. 5.5. Данные, пересылаемые по сети 10BaseT, передаются каждому ПК, подключенному к портам концентратора

Некоторые интеллектуальные концентраторы запоминают физический адрес сетевой платы, связанной с отдельным портом. Эти концентраторы могут быть заранее запрограммированы с помощью статического списка адресов, соответствующих ПК, или установить это соответствие самостоятельным поиском. Установленное соответствие статических адресов может воспользоваться для закрытия доступа к сети некоторым пользователям. Как показано на рис. 5.6, если концентратор имеет статический список соответствия адресов с портами, и ПК с данным физическим адресом, не указанным в этом списке, попытается подключиться к сети, то интеллектуальный концентратор сможет изолировать этот порт. После изолирования этот ПК физически не сможет подсоединиться к ПК, подключенному к, другому порту концентратора.

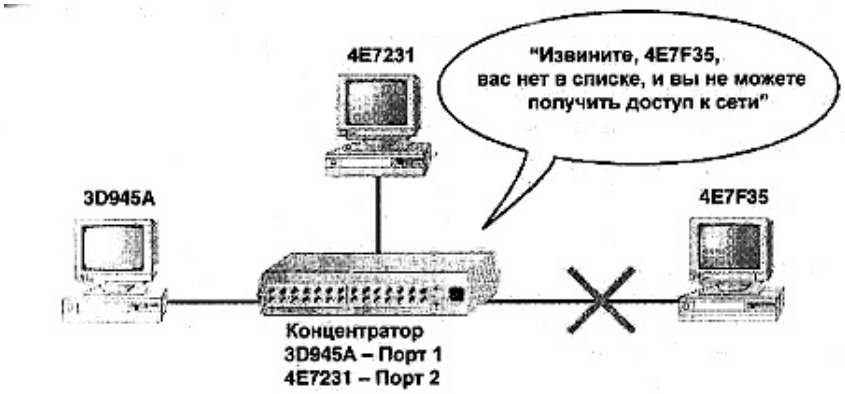


Рис. 5.6. Интеллектуальные концентраторы могут использовать статический список разрешенных физических адресов для закрытия доступа к сети некоторым ПК

Внутренняя шина концентратора работает с той же частотой, что и сеть, или, более точно, быстродействие сети, построенной по звездообразной топологии, частично определяется быстродействием концентратора. Поэтому если вы хотите работать с сетью на скорости 100 Мбит/с, требуется концентратор с внутренней шиной, способной поддерживать эту скорость.

Не все порты концентратора предназначены для подключения компьютеров. Одним из портов может быть так называемый *интерфейс сетевых устройств (AUI — attachment unit interface),* позволяющий подключить к концентратору другой концентратор или другое устройство типа моста или маршрутизатора, как показано на рис. 5.7.

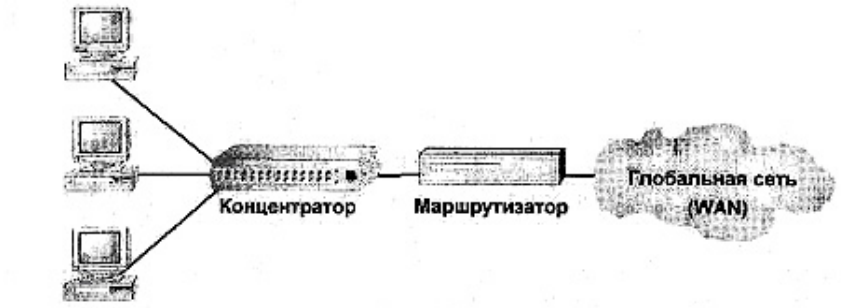


Рис. 5.7. Используйте дополнительные порты для соединения концентраторов друг с другом или с интерсетевыми устройствами

Модели концентраторов с портами AUI обычно описываются списком номеров портов (например, 5+1), означающим, что в концентраторе имеется пять портов для подключения ПК и один порт AUI. Тип кабеля, подключаемого к порту AUI, зависит от концентратора. В некоторых моделях применяют оптоволоконный или толстый коаксиальный кабель, в то время как в других можно использовать разъем RJ-45 и выглядеть этот порт будет как типичный порт ПК. Более дорогие концентраторы могут иметь порты AUI для подключения оптоволоконного кабеля. Однако даже дешевый концентратор ценой 59 $ можно подключить к другим концентраторам, работающим на скорости 100 Мбит/с, поскольку его порт AUI допускает подключение кабеля категории 5.

Совет

Чем больше концентратор имеет портов, тем он дороже, и расходы на его приобретение могут даже превысить стоимость другого концентратора с таким же количеством портов. Следите за своими расходами - может оказаться дешевле "связать" два концентратора через их порты AUI, чем покупать один концентратор с нужным количеством портов.

В дополнение к портам AUI некоторые концентраторы могут быть снабжены портом последовательного интерфейса. Этот интерфейс позволяет подключать концентратор к

ПК или модему, предоставляя тем самым средства удаленного администрирования, на работу которых не влияют отказы сети, не связанные с самим концентратором. Такое администрирование называется администрированием *по внешнему каналу (out of band),* поскольку оно выполняется независимо от обычной передачи данных по сети.

Коммутирующие концентраторы

Как вы могли заметить, некоторые интеллектуальные концентраторы не просто слепо переносят данные во все подключенные к ним сегменты сети. Вместо этого они фиксируют MAC-адреса сетевых плат, связанных с каждым портом, и могут определенным образом отличать порты, используя эти адреса. Коммутаторы еще больше расширяют возможности концентраторов, обеспечивая идентификацию MAC-адресов мест назначения и направление пакетов только в тот сегмент, в котором расположен узел с этим адресом.

Различие между обычными и коммутирующими концентраторами подобно различию между звонком оператору офисного коммутатора (принимающего входящий звонок и подающего сигнал персонального вызова для ответа на звонок) и звонком в нужный вам офис с прямой коммутацией телефонного вызова (рис. 5.8).

Зачем надо коммутировать сигнал вместо его широковещательной передачи? Одной из основных причин является управление сетевым графиком. Ведь во втором случае, пользуясь приведенной выше аналогией, при каждом телефонном звонке в офис оператор коммутатора подает слышимый всеми сигнал, по которому можно определить, кому следует отвечать на звонок. Ясно, что при этом пауза в работе офиса будет больше по сравнению с прямым указанием места назначения звонка. Аналогично, когда концентратор производит широковещательную передачу всех кадров во все присоединенные к нему сегменты, то каждый ПК в сети должен остановится и "послушать", не разговаривая при этом друг с другом, чтобы избежать конфликтов. Если же сигнал передается только в ту часть сети, куда он должен попасть, то остальная часть не будет активизирована этим сигналом. Фактически можно продолжать обмен данными с другими сегментами, не реагируя на такой сигнал.

Коммутация также делает возможным резервирование более широкой полосы пропускания для приложений, требующих интенсивного трафика. С помощью обычного концентратора или повторителя в сети с быстродействием 10 Мбит/с все порты совместно используют один и тот же канал на скорости 10 Мбит/с. С помощью же коммутации каждый порт может иметь собственный канал на 10 Мбит/с, свободный от трафика из других портов. Применение коммутации позволяет соединить вместе несколько сетей и воспользоваться преимуществами связи без помех, возникающих вследствие совместного использования полосы пропускания.

Роль коммутаторов сложнее, чем это может показаться на первый взгляд. Это не просто сетевое устройство, исполняющее функции концентратора со средними возможностями, плюс некая небольшая добавка. Как показано на рис. 5.9, обычно отдельные ПК не подключаются непосредственно к коммутатору. Как правило, к портам коммутатора концентраторы подключаются для того, чтобы каждый сегмент сети имел собственный порт. В зависимости от местоположения коммутаторов в сети, вы можете использовать их для изолирования частей сети на уровне рабочих групп, отделов или магистрали.

Примечание

Хотя коммутаторы чаще используются для соединения сегментов сети, к ним можно подключить и отдельные ПК, если требуется предоставить одному пользователю или серверу более широкую полосу пропускания.

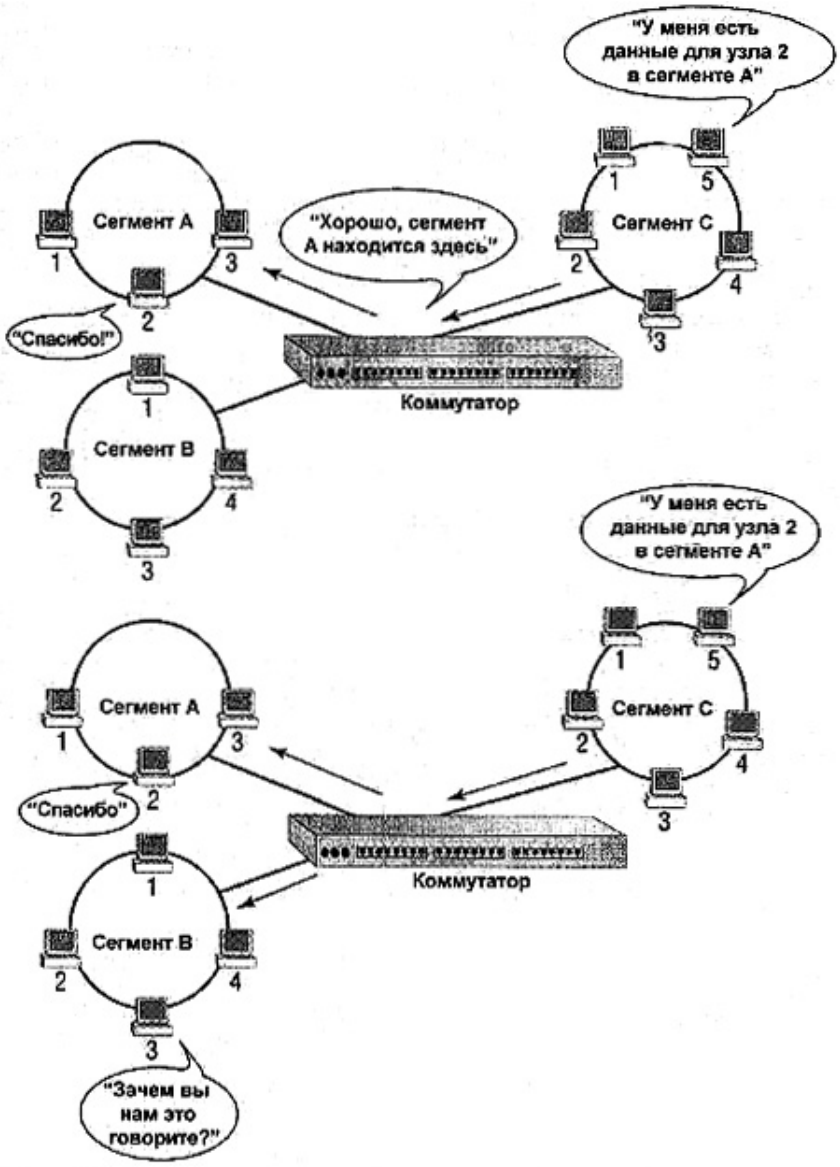


Рис. 5.8. Соединение с коммутацией сигнала и его отличия от соединения с широковещательной передачей сигнала

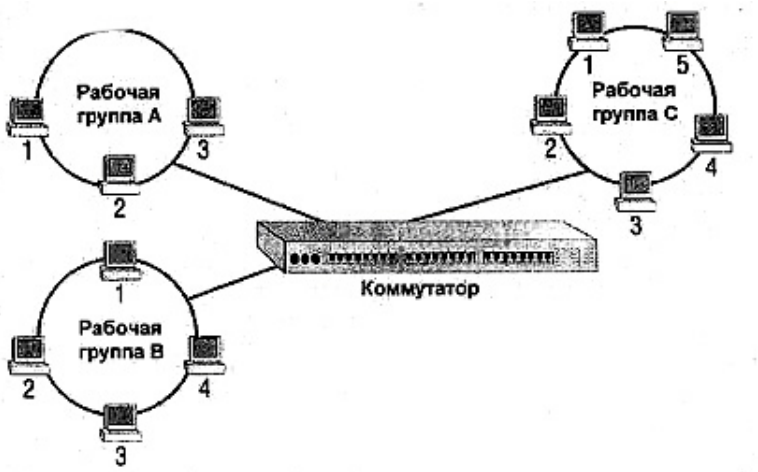


Рис. 5.9. Использование коммутаторов для изолирования различных частей сети (но не отдельных ПК)

Методы коммутации

В большинстве коммутаторов для выполнения рабочих функций используют два метода: сквозной коммутации и коммутации с промежуточным хранением. При *сквозной коммутации (cut-through switching)* коммутатор только читает MAC-адрес в коммутируемом кадре. Он начинает отправку кадра в тот порт, MAC-адрес которого был обнаружен в этом кадре, причем так быстро, как только коммутатор узнает, куда его следует посылать — обычно сразу после введения первых 20—30 байтов информации. (Напомним, что кадры Ethernet имеют длину около 1500 байтов, так что пауза в 30 найтов — это очень; небольшая задержка.) Таким образом, скорость сквозной коммутации равна, по существу, скорости линии связи.

Промежуточное хранение является методом, также применяемым в мостах. При этом сначала весь кадр принимается целиком, а затем обрабатывается с целью определения MAC-адреса места назначения и контроля ошибок кадра. Только корректные кадры направляются далее.

На рис. 5.10 показано различие между этими двумя методами.

Какой метод лучше? Сквозная коммутация в общем случае быстрее, поскольку кадры могут передаваться в соответствующий сегмент по мере их поступления на коммутатор. Однако этот метод таит в себе потенциальную опасность передачи искаженных кадров и, как следствие, увеличения сетевого трафика с непригодными битами. Коммутация с промежуточным хранением немного медленнее, так как каждый кадр должен быть проверен на наличие ошибок, но при этом вероятность распространения ошибок по сети меньше. Точнее говоря, он не намного замедляет работу сети, но использование коммутации с промежуточным хранением привносит некоторую задержку, которая отсутствует при сквозной коммутации, и чем крупнее кадр, тем больше время задержки. Это усложняет работу сетей с мостами.

Поэтому сквозная коммутация лучше всего подходит для сетей, нуждающихся, прежде всего, в высокой пропускной способности, а не в уменьшении вероятности распространения ошибки. Этот метод оптимален для небольших простых сетей. Коммутация с промежуточным хранением может потребоваться для более сложных сетей, для которых неприемлемы бесполезные потери времени на работу с испорченными кадрами, с какой бы малой вероятностью они не появлялись.

Примечание

Некоторые коммутаторы поддерживают оба метода. Обычно в них используется метод сквозной коммутации. При этом они "следят" за частотой появления ошибок без промежуточного хранения кадров. Если частота ошибок превышает определенное допустимое значение, коммутатор переходит на метод коммутации с промежуточным хранением.

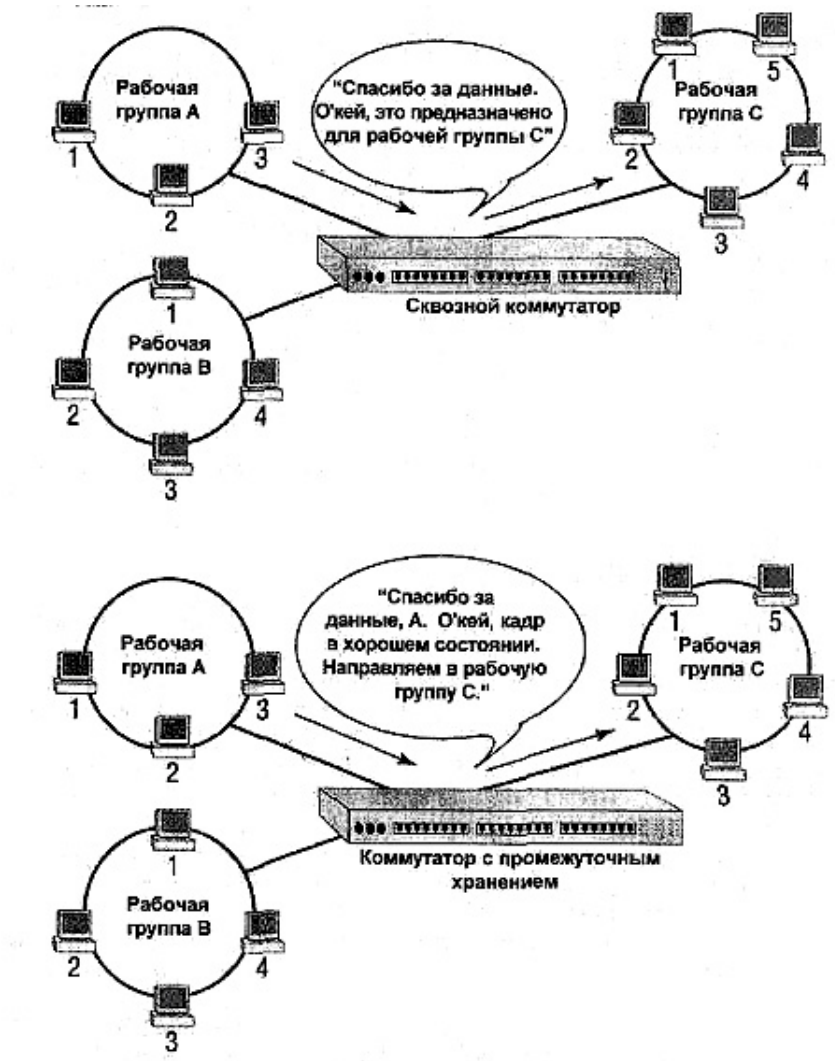


Рис. 5.10. Выбор метода коммутации зависит от того, что более важно для сети - отсутствие ошибок или скорость работы

Мосты для расширения сети

В предыдущем разделе было сказано о том, что, подобно коммутаторам, Мосты также выполняют маршрутизацию с промежуточным хранением кадров. Реальность такова, что граница между мостами и коммутаторами временами может быть весьма зыбкой. Можно различать эти устройства, исходя из выполняемых ими функций. Если идея *коммутации* заключается в разделении единой сети на отдельные (но все еще связанные) сегменты, то идея *организации моста (bridging)* — в комбинировании отдельных сетей в единую сеть. Точнее, организация мостов позволяет передавать данные между двумя (или более) различными сетями, обеспечивая в то же время для них раздельный трафик (см. рис. 5.1.1).

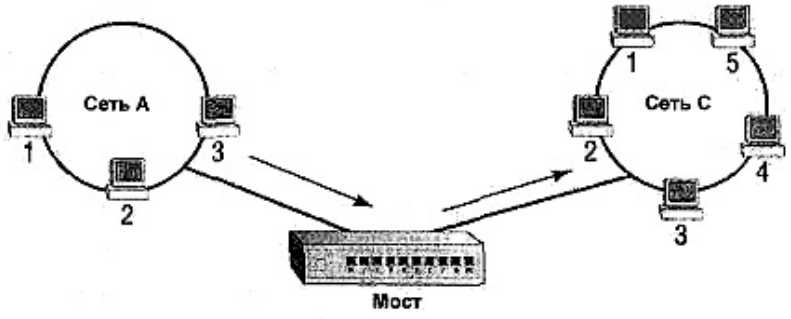


Рис. 5.11. Мосты позволяют передавать данные между двумя одинаковыми сетями

Мосты не зависят от типа используемых протоколов. Обычно их не касается, какой транспортный протокол используется — IPX или TCP/IP. Если мост может прочитать адрес источника и адрес места назначения пакета, значит он может определить, что ему следует сделать: отфильтровать или переслать пакет.

Примечание

Чтобы завершить мысль о зыбкости границ между различными типами сетевого оборудования, укажем, что некоторые мосты могут относиться по-разному к пакетам, использующим различные транспортные протоколы (например, IPX по сравнению с IP). Вообще, функционирование мостов относится к операциям канального уровня.

В приводимых далее примерах будет рассматриваться организация мостов в основном для сетей Ethernet (если не указано иное), но большая часть принципов применима также и к сетям Token Ring.

Как работают мосты

Каждый раз, когда в сети с мостами выполняется широковещательная передача кадров, мост, подобно любому другому устройству сети, "слышит" широковещательную передачу и "читает" MAC-адрес места назначения кадра. Основываясь на этой информации, мост определяет, адресован ли этот пакет одному из компьютеров в данном сегменте, или же он предназначен для другого сегмента. В первом случае мост ничего не должен делать — ПК, для которого этот кадр предназначен, его уже получил. Если же место назначения пакета находится в другом сегменте, мост пересылает его в этот сегмент. Единственным исключением из этого правила является широковещательная или групповая передача кадров, т.е. передача кадров, которые посылаются либо всей сети, либо нескольким получателям. Такие кадры передаются во все порты моста.

Примечание

Рассылка пакетов во все подсоединенные сегменты называется *лавинной маршрутизацией моста (bridge flooding)*. Иногда она проводится преднамеренно, иногда возникает случайно и должна быть устранена.

Как же все это реализуется на практике? Имеется два различных метода организации работы мостов, поэтому давайте начнем с самого простого, используемого в сетях Ethernet. Такой метод *называется прозрачный мост.*

Предположим, имеются две сети Ethernet с мостом между ними. Если требуется послать информацию с Узла А в Сегмент 1 для Узла В, то этот процесс будет выглядеть примерно так.

1. Узел А выполняет широковещательную передачу пакета для всей сети.
2. Когда пакет достигает моста, мост определяет адреса источника и места назначения пакета.
3. Если пакет предназначен для другой рабочей станции в том же сегменте сети, в котором он был создан (т.е. на той же самой стороне моста), то мост не станет выполнять широковещательную передачу пакета в сегмент 2. Этот процесс известен под названием *фильтрация* (рис. 5.12).
4. Однако если пакет предназначен для другого сегмента сети (как в данном примере), то мост направит его в этот сегмент, пропустив пакет так, как это показано на рис. 5.13.

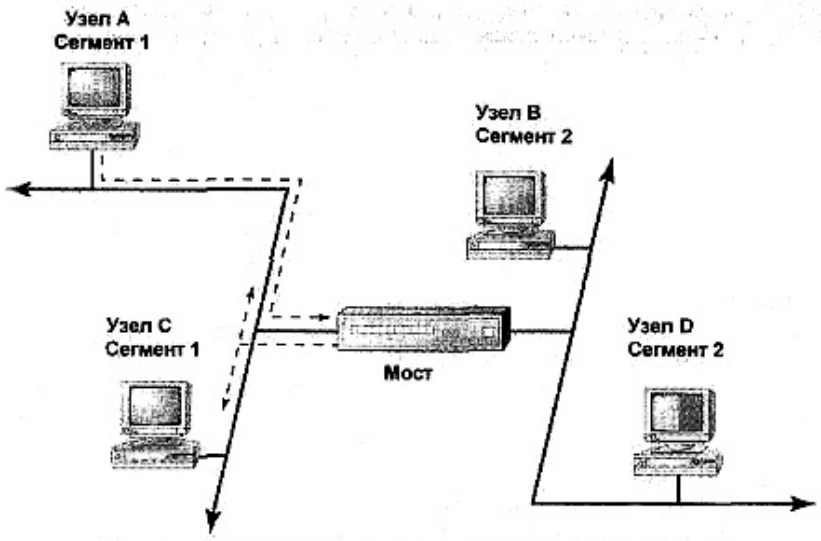


Рис. 5.12. Кадры фильтруются (отбрасываются), если их место назначения находится в том же самом локальном сегменте

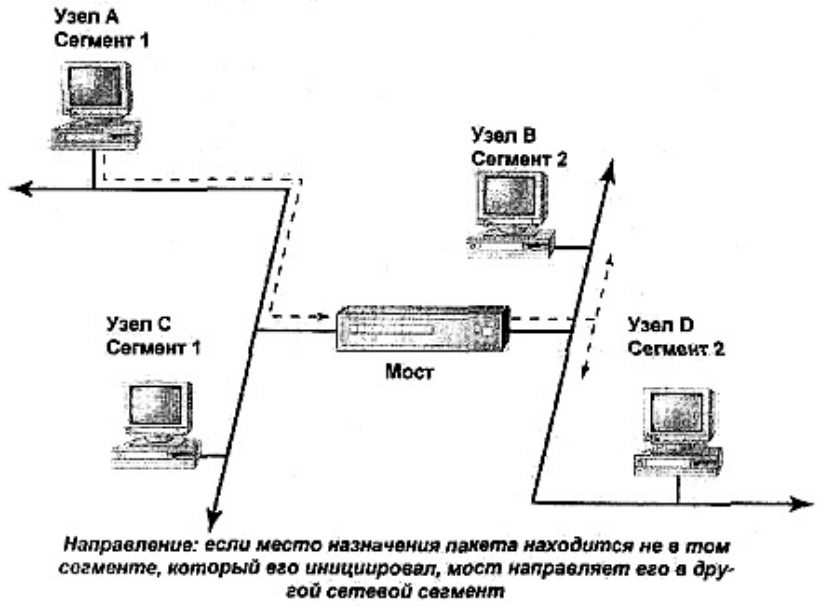


Рис. 5.13. Кадры, направляемые по адресу места назначения вне локального сегмента

Как же мост узнает, что искомое устройство с указанным физическим адресом находится в данном локальном сегменте? Ответ заключается в способе, которым сетевые платы "превращают" адреса компьютеров в адреса, используемые программой. Напомним, что имеются два различных уровня представления сетевых адресов: физический, на который работают сетевые платы и который "понимает" сеть, и логический, используемый в сетевых операциях высокого уровня, которые "не понимают" 48-битовые адреса Ethernet, если натолкнутся на них. Например, ПК, поддерживающие протокол TCP/IP, для отправки данных узлу сети нуждаются в некотором методе установления соответствия логических адресов с адресами компьютеров.

Указанное выше соответствие устанавливается специальным методом поиска. В этом методе может использоваться один из нескольких протоколов в зависимости от применяемого транспортного протокола сетевого уровня. Например, в протоколе TCP/IP для этого используется ARP (Address Resolution Protocol - протокол определения адресов). Все эти протоколы выполняют, в основном, одинаковую функцию. Когда сетевой ПК, поддерживающий протокол TCP/IP, пытается послать данные через сеть в первый раз после перезагрузки, он должен установить соответствие IP-адресок сетевого программного обеспечения с MAC-адресами, которые будут понятны в сети. Поэтому, предвидя последующую пересылку данных, узел выполняет широковещательную передачу (по сети) запроса ARP REQUEST, содержащего его IP-адрес. Узел с этим адресом (а каждый узел должен знать свой собственный IP-адрес) будет в ответ передавать свой собственный пакет REPLY ARP (ответ ARP), содержащий свой физический адрес. После того как запрашивающий узел получит ответ, он добавит сведения об установленном соответствии к таблице ARP и отменит передачу пакета запроса.

Главное здесь то, что происходит при направлении мостом запроса ARP всем другим сегментам. Поскольку для этого используется широковещательная передача, такое направление делается автоматически. Перед посылкой пакета в сеть, мост вставляет в часть пакета, хранящую сведения об отправителях, свой собственный MAC-адрес, поэтому он и может получить соответствующие ответы. Если другой запрос ARP изменит первоначально установленное соответствие, мост обновит таблицу.

Стандартные методы организации работы мостов

Если ваша сеть все больше и больше разрастается, то в какой-то момент времени вам нужно будет снова добавлять в нее мосты, и простой метод "прозрачных мостов" более не будет эффективен. Использование множества мостов может привести к *зацикливанию мостов,* т.е. такому состоянию, при котором на мост поступит две копии одного и того же пакета, что приведёт к беспорядку в его работе. Проблема в том, что в этом случае мост не знает, какой сегмент инициировал пришедший к нему пакет, и поэтому не сможет корректно обновить свою таблицу MAC-адресов. Проблема еще более усугубляется в случае, если между сегментами существует более одного пути. Например, пусть компьютер Aries расположен в сегменте Andromeda, имеющем два моста: Gamma и Beta. Мост Gamma подключен к сегменту Cassiopeia, а Beta к Bonham (рис. 5.14).

Всякий раз после перезагрузки, когда ПК Aries посылает пакет ПК Bonzo, в сегменте Bonham происходит несколько событий.

В сегменте Andromeda есть два моста, ни один из которых "не слышал" компьютера Aries со времени его загрузки. Таким образом, и они будут вовлечены в поиск пути с помощью широковещательного запроса ARP, и оба выполнят лавинообразную маршрутизацию пакета для компьютера Bonzo по своим сегментам. Это плохо по двум соображениям.

- Компьютер Bonzo получит две копии пакета ARP от компьютера Aries (и любых других пакетов), что приведет к непроизводительному использованию полосы пропускания.
- Более серьёзным является то, что мост Beta "слышит" пакет ARP, поступающий одновременно с двух направлений: сегментов Andromeda и Cassiopeia. Поэтому он не сможет решить, в котором сегменте находится компьютер Aries, чтобы корректно занести его параметры в свои таблицы MAC-адресов.

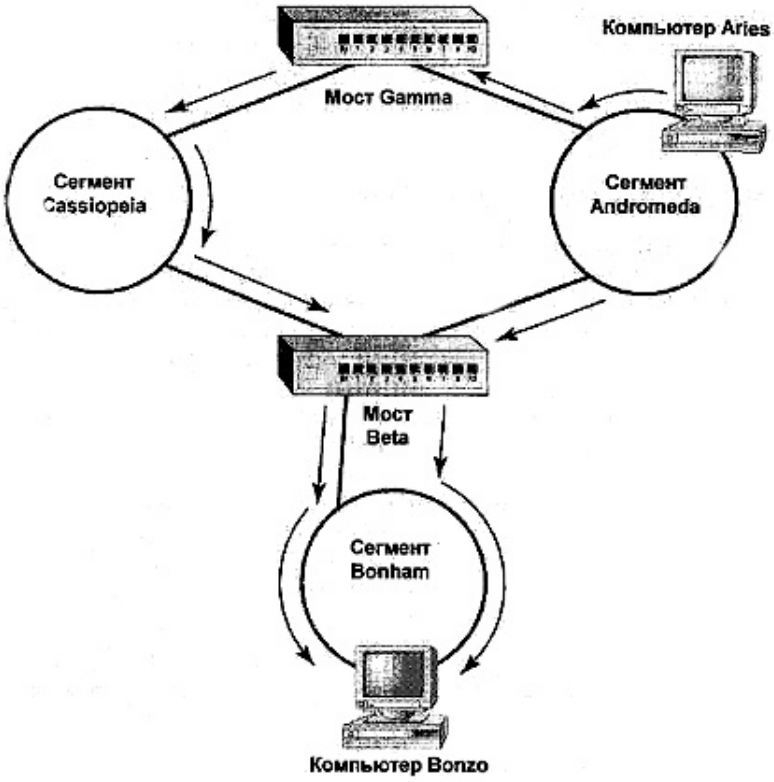


Рис. 5.14. Наличие нескольких мостов и сегментов между ними может привести к "зацикливанию" мостов

Для предотвращения некорректной работы электронного оборудования, необходимо выполнить определенного рода логическое упорядочение сети, и это как раз тот самый случай, когда используются алгоритмы организации работы моста. Эти алгоритмы организуют сетевой трафик таким образом, что каждому пакету, посылаемому по сети, для достижения его места назначения будет доступен только один путь.

Алгоритм связывающего дерева

Алгоритм связывающего (остовного) дерева (STA — Spanning Tree Algorithm) позволяет мостам определять оптимальный маршрут к указанному сегменту сети, а затем блокировать все другие возможные маршруты, применение которых менее желательно. Ясно, что поскольку теперь при поиске маршрута к любому сегменту будет доступен только один путь, то зацикливания моста не произойдет.

С помощью алгоритма STA каждый мост в сети идентифицируется у соответствии с его MAC-адресом. Вдобавок каждый порт имеет идентификатор, создаваемый сетевым администратором и состоящий из трех компонентов: приоритет моста, стоимость и иден-

тификационный номер. Эта информация позволяет более гибко выполнять поиск пути в сети, поскольку один из путей можно сделать предпочтительным. Если он будет разрушен, станут доступными другие, менее эффективные пути.

Примечание

В *Стоимость* является функцией числа транзитных участков, проходимых в процессе достижения пакетом места назначения. Меньшее количество транзитных участков означает меньшую стоимость пути.

Когда сеть включается, все мосты начинают широковещательную передачу мостовых протокольных единиц данных (BPDU — Bridge Protocol Data Units), содержащих информацию об их адресах и относительных приоритетах. Она продолжается до тех пор, пока не будет распознан мост с самым низким приоритетом, который становится *корневым (основным) мостом (root bridge)*. (Если два моста имеют одинаково низкий приоритет, то корневым становится мост с наименьшим MAC-адресом.) Все другие мосты определяют свои характеристики по отношению к корневому мосту. При использовании данного алгоритма в сети образуется (логически) топологическая древовидная структура (рис. 5.15).

Один мост становится корневым мостом, один порт каждого моста становится корневым портом, выбираемым на основании стоимости его подсоединения к корневому мосту. Точно так же, если два порта имеют одинаковую стоимость пути к корневому мосту, то корневым, или *направляющим портом (forwarding port)* данного моста становится порт с наименьшим приоритетом. Таким образом, для каждого сегмента сети определяется путь к наименьшей стоимостью доступа к корневому мосту, и именно, этот путь используется до тех пор, пока это возможно. Другие возможные пути блокируются (это означает, что соответствующие порты не будут передавать пакеты) до тех пор, пока путь, с направляющим портом, станет недоступным. В этом случае мост может установить какому-либо ранее блокированному порту (выбрав его из-за низкой стоимости или высокого приоритета) статус направляющего.

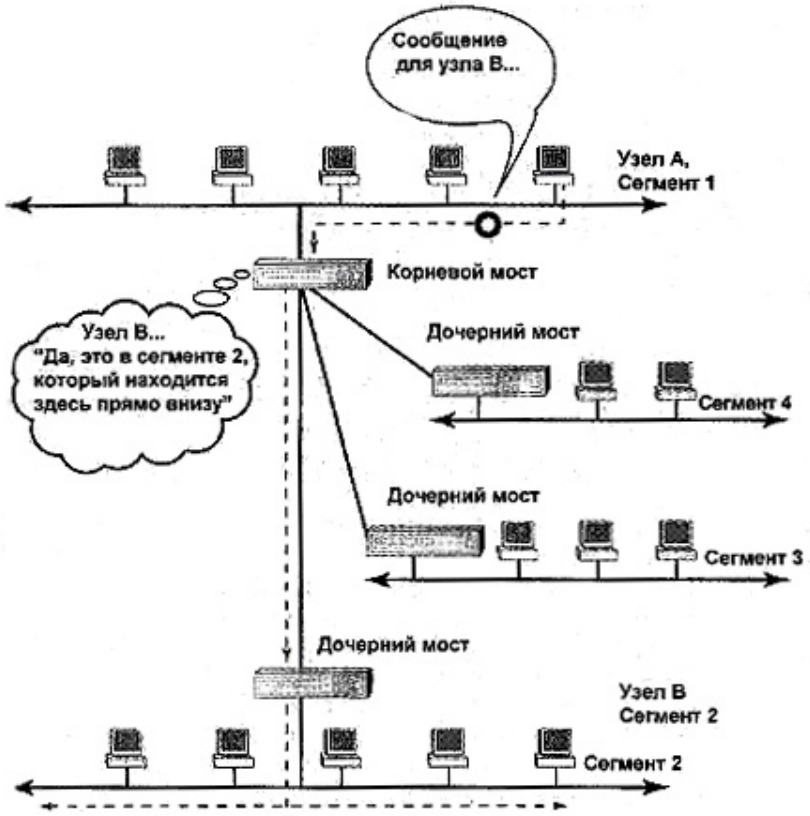


Рис. 5.15. При использовании алгоритма связывающего дерева приоритеты путей назначаются в соответствии с их эффективностью

Поскольку большинство параметров "ранжирования" сети при использовании алгоритма связывающего дерева задаются вручную (номер порта, его приоритет и стоимость пути), очень важно тщательно выбрать путь при конфигурировании моста. При построении пути следует гарантировать его максимальную эффективность. Если сделать это недостаточно тщательно, то можно прервать пересылку пакетов к местам их назначения, использовав сегменты, которые никогда не следует проходить, поскольку это не приведя к каким либо повреждениям сети, станет причиной неоправданного увеличение трафика в этих сегментах.

Организация работы мостов с маршрутизацией по источнику

Алгоритм связывающего дерева является статическим: он предусматривает обновление пути только тогда, когда найденные маршруты становятся недоступными. Имеется и другой метод, называемый маршрутизацией по источнику (SR — Source Routing), первоначально разработанный фирмой IBM для использования в сетях Token Ring с мостами. Этот метод более напоминает средства, применяемые при использовании маршрутизаторов, а не мостов, поскольку предусматривает выполнение динамического поиска пути на основе широковещательной передачи пакетов по сети. Используя информацию, собранную во время анализа маршрутов, узлы идентифицируют наилучший путь к указанному месту назначения и сохраняют запись об этом пути для своего собственного (внутреннего) пользования.

Сетевые узлы определяют путь к указанным местам назначения одним из двух методов.

- Маршрутизация всех путей посредством широковещательной передачи
- Маршрутизация связывающего дерева посредством широковещательной, передачи.

При использовании этих методов требуются данные о логической структуре сети.

Маршрутизация всех путей. Узел, сконфигурированный первым на указанных выше методов, начинает процесс отыскания путей путем широковещательной передачи кадров ARE (All Router Explorer — система поиска всех возможных маршрутов) или APE - (All Path Explorer — система поиска всех возможных путей). Это почти одно и то же. Разница заключается, в основном, в том, какой термин вы чаще употребляете в разговорах по поводу методов маршрутизации по источнику — "кадры APE" или "кадры ARE". Все кадры ARE для достижения места назначения используют различные пути.

Когда каждый из этих кадров проходит через мост, он добавляет к пакету следующее.

- Адрес *входящего кольца (incoming ring),* из которого поступает пакет (напомним, что маршрутизация по источнику применяется к сетям token Ring).
- Идентификаторы сегмента и моста.
- Адрес *исходящего кольца (outgoing ring),* в которое будет направлен паки при его следовании к месту конечного назначения.

Как показано на рис. 5.16, после того как мост добавит эту информацию к пакету, он снова посылает ARE на его "столбовую дорогу". Мост преднамеренно выполняет лавинообразную маршрутизацию ARE, вследствие чего множество таких пакетов появляется во всей сети.

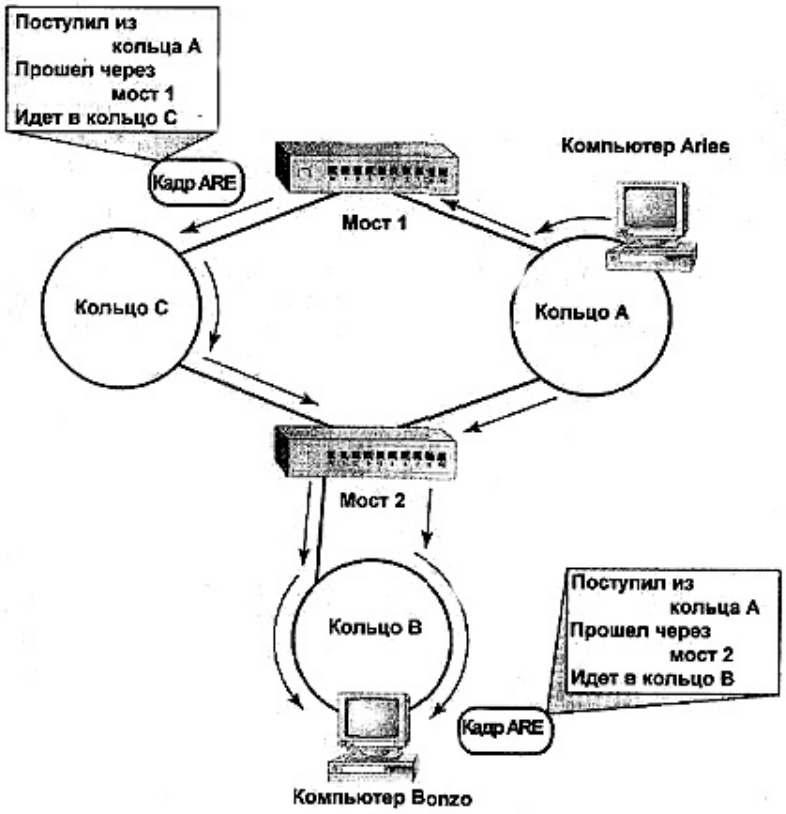


Рис. 5.16. При использовании метода маршрутизации всех путей сеть заполняется поисковыми пакетами

Этот процесс продолжается до тех пор, пока пакет ARE не прибудет в конечный пункт назначения. Таким образом, каждый пакет ARE будет включать в себя однозначно определенную информацию о пути от источника к месту назначения.

Маршрутизация связывающего дерева посредством широковещательной передачи. Метод STBR (Spanning Tree Broadcast Routing – маршрутизация связывающего дерева посредством широковещательной передачи) при поиске пути действует аналогично алгоритму STA. При этом узел генерирует кадры STE (Spanning Tree Explorer - система поиска связывающего дерева), но они направляются только в активные порты, т.е. порты, не заблокированные
от передачи пакетов. Таким образом, в сети будет существовать только единственный кадр STE, направляемый по единственному, заранее определенному, пути (рис. 5.17), В сущности, это аналог алгоритма STA для сетей Token King.

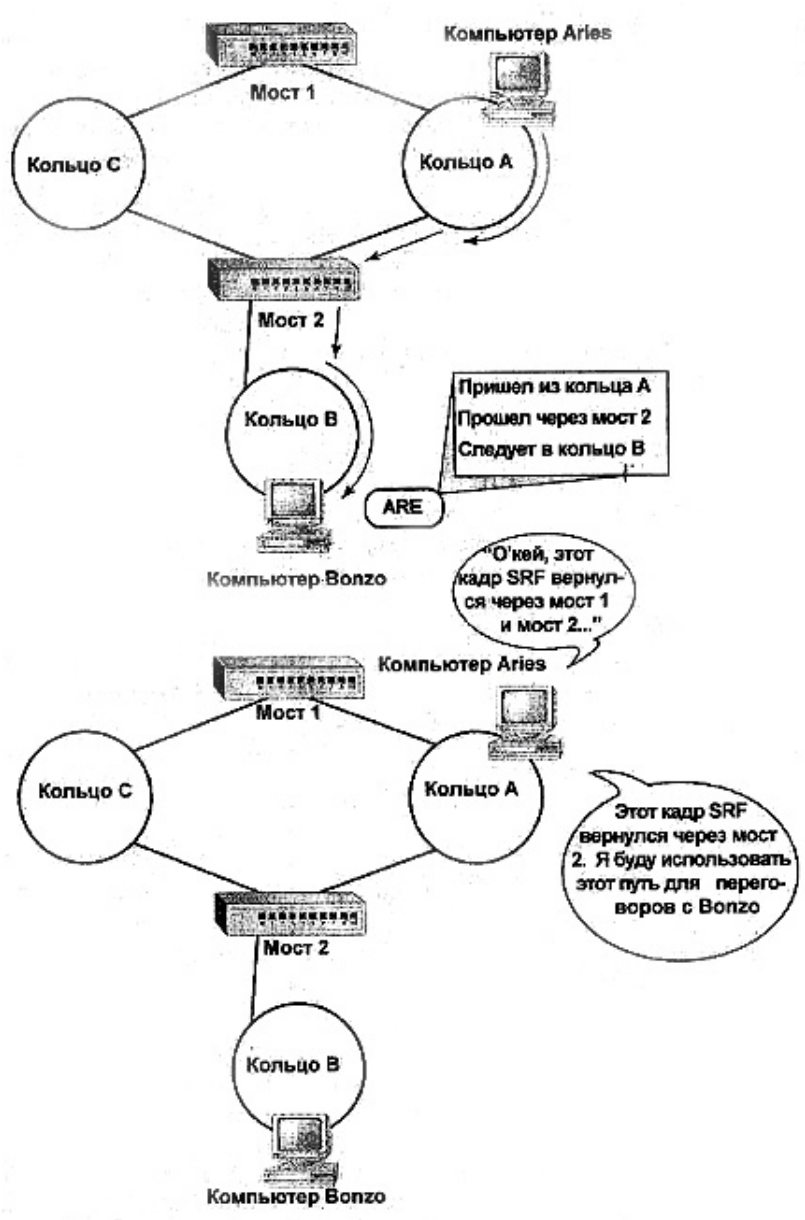


Рис. 5.17. Пакеты STE следуют единственным путем к месту их назначения

Примечание

Если сеть с мостами зациклилась, то мост, который послал пакет впервые, примет вслед за этим копию пакета ARE и отбросит пакет вместо его повторного направления.

Основное различие между методами STBR и STA заключается в месте их применения (STA - в сетях Ethernet, а STBR - в сетях Token Ring) и в приёмнике информации. При использовании метода STA узлы не отвечают за маршрутизацию пакетов. Она выполняется автоматически в зависимости от установленной сетевым администратором стоимости порта и приоритета.

Кадр со специальной маршрутизацией. В любом случае, когда одному узлу требуется передать данные другому сразу после перезагрузки, узел посылает их с дополнениями, требуемыми для поиска пути. Однако после того как узел примет пакеты ARE или STE, работа не завершится — посылающий узел все еще не будет осведомлен о том, каким образом пакеты достигли цели или какой путь является наилучшим.

Поэтому, когда узел получит кадр ARE или STE, он отвечает передачей так называемого кадра со специальной маршрутизацией (SRF — Specifically Routed Frame). Это значит, что передаче кадра STE соответствует единственный ответ, а передаче ARE — столько, сколько имеется кадров ARE. Каждый кадр SRF содержит информацию о маршрутах, взятую из исходного (поискового) пакета, на который он отвечает. Кадр SRF возвращается исходному отправителю кадра поиска, который, вслед за этим, вычисляет все пути, используя информацию, содержащуюся в принятых кадрах SRF, и кэширует предпочтительный путь для его использования во всех последующих передачах данных в соответствующий узел. Этот процесс показан
на рис. 5.18.

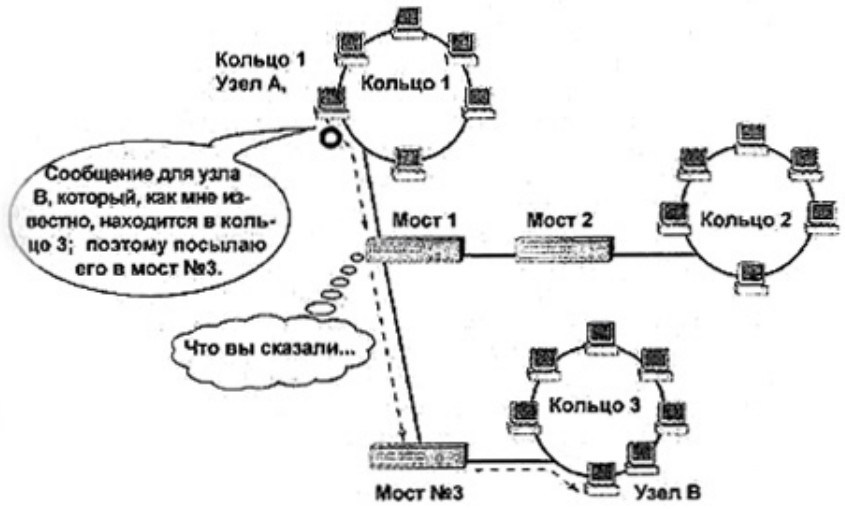


Рис. 5.18. Организация мостов с маршрутизацией по источнику (SR) управляет трафиком на уровне узлов, а не мостов

Замечание

Поскольку пакеты, посланные по сети при использовании метода маршрутизации по источнику, несут с собой "дорожную карту", они могут иметь различные размеры в зависимости от размера этой карты, которая, в свою очередь, может иметь длину до 18 байтов. В дорожной карте два байта отводятся для хранения информации о мосте и порте. В ней также должен быть указан адрес исходного порта. Дорожная карта может содержать описание пути длиной не более семи транзитных участков.

Метод маршрутизации по источнику при организации работы мостов используется не так часто, как метод прозрачного моста (рассматриваемый далее) или метод STA. Это обусловлено двумя причинами. Первая: как вы могли увидеть, здесь генерируется большой трафик. Вторая, быть может, более важная причина: сети Token Ring просто не име-

ют базы данных об установленных пользователях, которая создается в сети Ethernet. Поскольку маршрутизация по источнику была создана для локальных сетей Token Ring и FDDI, более высокие требования, предъявляемые к Ethernet, приводят к меньшим требованиям к маршрутизации по источнику. Как уже упоминалось, в сравнении с методом STA маршрутизация по источнику является более гибким средством, позволяющим выбирать путь способом, подобным способу, используемому маршрутизаторами.

Организация прозрачного моста

В локальных сетях Ethernet используется метод STA, в Token Ring - метод SR. При использовании STA с помощью мостов определяется, какой порт посылает пакет с данным адресом места назначения. Мосты с маршрутизацией по источнику знать не знают никаких инструкций по маршрутизации — они просто направляют пакет, используя информацию об установленном соответствии, которую посылающий узел включает в пакет. Так могут ли локальные сети Ethernet и Token Ring взаимодействовать друг с другом или же они обречены на взаимное непонимание?

Сети с мостами, использующими один из этих двух методов, могут взаимодействовать с помощью некоего дополнительного моста, поддерживающего функционирование алгоритма связывающего дерева и протокол преобразования пакетов. Этот алгоритм определяет порты, выделенные для выполнения такого взаимодействия, и пакет, пересылаемый через это порты, будет преобразован в формат, "понятный" в сети другого типа.

Ранее в этой главе уже было описано, как работает алгоритм связывающего дерева. При использовании описанных мостов в сети будет существовать еще один экземпляр этого дерева, работающий бок о бок со связывающим деревом, сформированным только для связей в сети Ethernet, но он не подменяет его. Каждый порт моста может быть переведён в одно из следующих состояний: заблокированное (blocking state), направляющее (forwarding state), или направляюще-преобразующее (forwarding and converting state).

Преобразование пакетов из формата сети 802.2 Ethernet в формат сети 802.2 Token Ring не вызывает затруднений. Как показано на рис. 5.19, кадры двух этих типов сетей очень близки друг к другу, за исключением того, что если кадры в сети Token Ring содержат поле информации о маршрутизации (RIF — Routing Information Field) переменной длины, то у кадров в сети Ethernet поле Length имеет постоянную длину. Это происходит потому, что оно содержит информацию, не относящуюся к маршрутизации. Когда пакет приходит на порт, находящийся в направляюще-преобразующем состоянии, поле преобразуется в формат, используемый доменом места назначения.

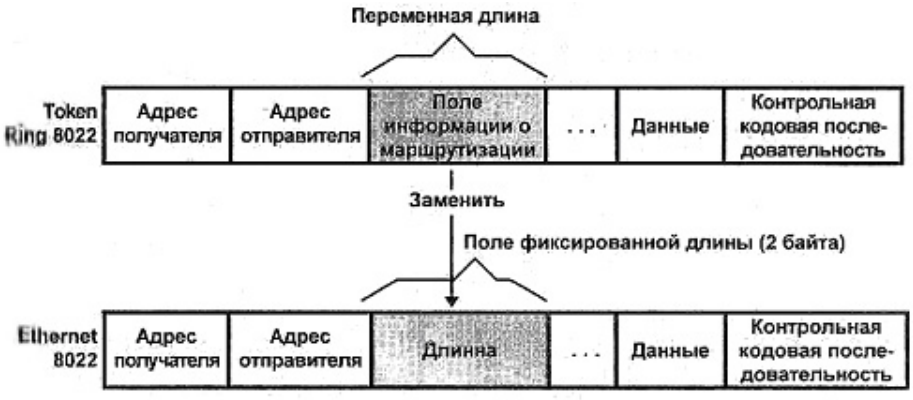


Рис. 5.19. Преобразование пакетов Ethernet и Token Ring

Примечание

Если в сети Ethernet используются пакеты стандарта 802.3, а не 802.2, их обработка немного усложняется и выполняется несколько иначе. Несмотря на это идея остается в основном прежней - информация о маршрутизации пакетов (или отсутствие таковой) редактируется так, чтобы была обеспечена возможность ее передачи в сеть иного типа.

Где же транслирующие мосты получают информацию, нужную им для преобразования пакетов? Необходимая информация для этого адреса хранятся о двух базах данных. *База данных переадресации (forwarding database)* содержит список адресов, доступных пакету при его направлении (переадресации). Например, запись в ней может означать: "Чтобы достигнуть адреса 12345, надо послать пакет в порт *A.". База данных RIF (Routing Information Field - поле информации о маршрутизации)* содержит информацию о маршрутизации для всех рабочих станций сети, независимо от того, на какой стороне транслирующего моста (translation bridge) они находятся. В предыдущем примере запись в ней могла бы означать: "Чтобы достигнуть адреса 67890, послать пакет в порт A, затем в D, затем в C". Когда транслирующий мост узнает адрес на стороне сети, использующей метод SR, эти две записи обновляется добавлением информации по маршрутизации к базе данных RIF, а информации об адресе и порте - к базе данных переадресации.

Информация, хранимая в этих двух базах данных, не является статической: в зависимости от конфигурации моста через определенные интервалы времени стирая информация стирается и заменяется новой. Если таймер установлен, скажем, на 15 минут, то каждый раз после подтверждения адреса (например, когда транслирующий мост принимает пакет из узла с определенным адресом.) таймер, соответствующий этому адресу перезапускается. Таким образом, не все записи удаляются автоматически по мере исчерпания "срока годности". Стираются только неподтвержденные адреса.

Итак, мосты, как и ожидалось, продолжают свою работу. Со стороны сети STA пакеты передаются в направлении порта, отправляющего их в конечный пункт назначения. На стороне сети SR сохраняется "дорожная карта", которая может быть присоединена к пакетам для определения конечного места назначения. Когда кадр SR перемещается на сторону сети STA, его поле с информацией по маршрутизации удаляется, а когда кадр STA перемещается на сторону сети SR, он получает "дорожную карту" с информацией по маршрутизации.

Связь сетей с помощью маршрутизаторов

Маршрутизаторы являются устройствами, работающими на сетевом уровне, которые позволяют связывать сети с широко распространенными маршрутизируемыми сетевыми протоколами. Если у вас есть удаленный доступ к Internet, то вы уже имеете некоторое представление о том, как пакеты перемещаются в маршрутизируемую сеть. Если для этого используется какая-либо версия Windows, то при конфигурировании удаленного доступа вам потребовалось указать шлюз, используемый по умолчанию. Этот шлюз фактически и является маршрутизатором. Он не посылает пакеты напрямую по их адресу, но выполняет широковещательную передачу в вашу локальную сеть. Как это будет вкратце описано далее в разделе "Шлюзы для мэйнфреймов", шлюз решает, адресован пакет узлу локальной сети, или нет. Если это так, то маршрутизатор игнорирует его. Если не так, - направляет его в следующую сеть, где происходит то же самое. Так будет до тех пор, пока пакет не достигнет конечного места назначения.

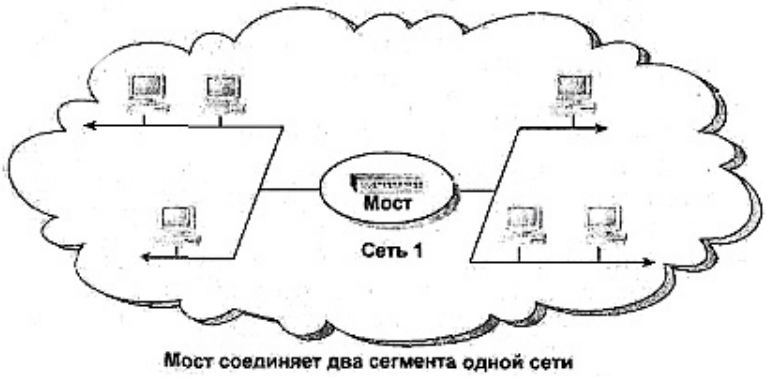
Примечание

Поскольку маршрутизаторы соединяют различные сети, соответствующая терминология немного усложняется. Все сети, связанные маршрутизаторами, имеют собирательное название *интерсеть (internetwork),* под которым можно понимать Internet в качестве наиболее известного примера.

Но вначале выясним некоторые детали. Во-первых, в данном разделе внимание сфокусировано на маршрутизации в сетях TCP/IP, поскольку это наиболее широко используемый протокол. Во-вторых, термин "маршрутизатор" относится к устройству, .выполняющему задачи, описанные далее. Этим устройством может быть черный ящик с мигающими индикаторами (аппаратный маршрутизатор), или компьютер с множеством установленных сетевых плат, работающий под управлением операционной системы типа Windows NT, поддерживающей маршрутизацию (программный маршрутизатор). В обоих случаях основные функции маршрутизатора остаются теми же.

КАК работает маршрутизатор

Как показано на рис. 5.20, все связи в интерсети создаются на базе маршрутизаторов, а не на отдельных узлах. Сети же связаны мостами, в которых организация связи базируется на использовании индивидуальных адресов, а мосты предоставляют информацию, помогающую пакету достичь конечного места назначения. Каждая область сети, отделенная от других областей маршрутизаторами, называется *сегментом* сети.



Мост соединяет два сегмента одной сети

Маршрутизаторы соединяют две различные сети

Рис. 5.20. Маршрутизаторы связывают две отдельные сети или сегменты одной сети, в то время как мосты расширяют эту сеть

Рассмотрим простой пример, в котором узел Argus в сегменте 1 хочет послать, данные узлу Cameron в сегменте 3. Соответствующий процесс выполняется примерно так.

1. Узел Argus выполняет широковещательную передачу данных в свой локальный сегмент, где его "слышат" все другие узлы сегмента. Его также "слышит" маршрутизатор 1, являющийся шлюзом по умолчанию для данного сегмента.

Примечание

Сеть может иметь более одного маршрутизатора, подключенного к другим сетям, но один из них должен быть определен как шлюз по умолчанию, и он будет управлять передачей данных. Единственное исключение из этого правила - случай, когда шлюз по умолчанию работает некорректно. При этом в работу включается альтернативный шлюз, если, конечно, он определен.

2. Маршрутизатор 1 проверяет адрес места назначения пакета и сравнивает его с содержимым *таблицы маршрутизации (routing table),* содержащей список адресов, расположенных в локальном сегменте. Он спрашивает себя: "Предназначен ли этот пакет кому-либо здесь?". Если ответом будет "Нет", то маршрутизатор 1 повторно упаковывает пакет и передает его в сегмент 2 — следующий сегмент, обрабатывающий пакет типа SEP (Somebody Else's Problem - чьи-то чужие проблемы).
3. При широковещательной передаче пакета в сегмент 2, маршрутизатор 2 слышит широковещательную передачу и проверяет адрес места назначения пакета. Опять-таки, поскольку место назначения расположено не в сегменте 2, маршрутизатор 2 повторно упаковывает пакет и посылает его в сегмент 3.
4. В сегменте 3 происходит то же самое, но теперь маршрутизатор 3, являющийся шлюзом по умолчанию сегмента 3, находит адрес места назначения в таблице маршрутизации. С этого момента маршрутизатор 3 более не несет ответственности за судьбу пакета. Теперь выполняется широковещательная передача пакета в сегмент. Узел Cameron слышит его и забирает себе. Все счастливо завершается.

В предыдущем примере маршрутизатору было несложно сделать свой выбор. В каждом сегменте есть один маршрутизатор, соединенный с одним из других сегментов, поэтому данные могут путешествовать по прямой линии к месту назначения. Однако многие маршрутизированные сети устроены не так просто. Internet представляет собой прекрасный пример чрезвычайно сложной, маршрутизированной сети.

Следовательно, маршрутизация сложной сети требует решения двух проблем.

- Если между источником и конечным местом назначения имеется несколько доступных для использования путей, по какому критерию следует выбирать один из них?
- Каким образом можно получить информацию о маршрутизации, и кто отвечает за ее хранение?

Читайте дальше, если хотите узнать, как маршрутизаторы решают эти проблемы.

Поиск наилучшего пути

Одним из важных моментов работы маршрутизированной сети является управление трафиком. Ясно, что широковещательную передачу пакетов и какие-либо сегменты, не содержащие конечного места назначения, .следует выполнять с минимизацией сетевого трафика. Не будем забывать, что в каждый момент времени передавать данные в сети будут сразу несколько узлов. Лучше всего было бы найти как можно более короткий (или самый быстрый) путь, чтобы освободить сеть так скоро, как это возможно. Поэтому при выборе пути с наименьшим числом транзитных участков итоговый путь пикета может от-

клоняться от некоей средней линии, для того, чтобы скомпенсировать изменения в трафике или работоспособности сети. Этим маршрутизированные сети отличаются от сетей с мостами, в которых путь предопределяется в начале передачи данных и предназначается для использования в процессе всей передачи, независимо от того, сколько задержек в работе сети при этом возникнет. Маршрутизация является более гибким средством.

Например, пусть узел Argus пытается связаться с узлом Diana, расположенным в сети 5 (рис. 5.21). Для перехода из сети 1 в сеть 5 пакет должен пройти через маршрутизаторы 1—4.

Однако когда пакет достигает маршрутизатора 2, этот маршрутизатор может оценить ситуацию и сделать вывод: "Хорошо, я могу передавать пакет на маршрутизатор 3, но в данный момент он перегружен. Почему бы мне вместо этого не передать его прямиком на маршрутизатор 5 в надежде, что этот путь сработает?". Такой альтернативный путь (рис. 5.22) фактически включает большее число транзитных участков, но он более эффективен, чем исходный путь, поскольку пакеты не посылаются на занятый в данный момент маршрутизатор.

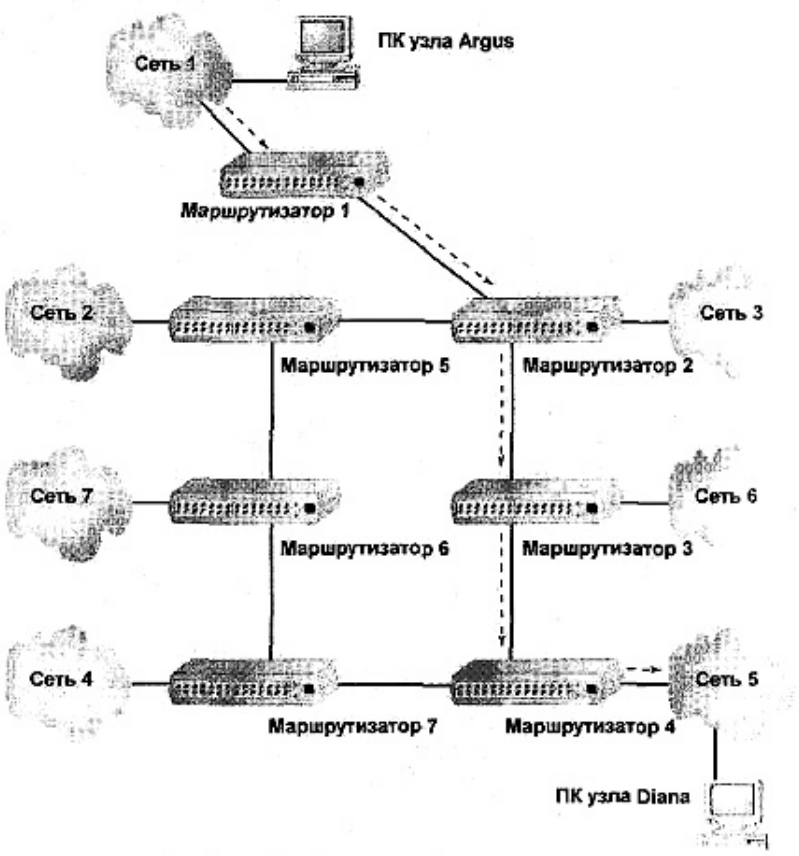


Рис. 5.21. Исходный путь между узлом Argus и Diana

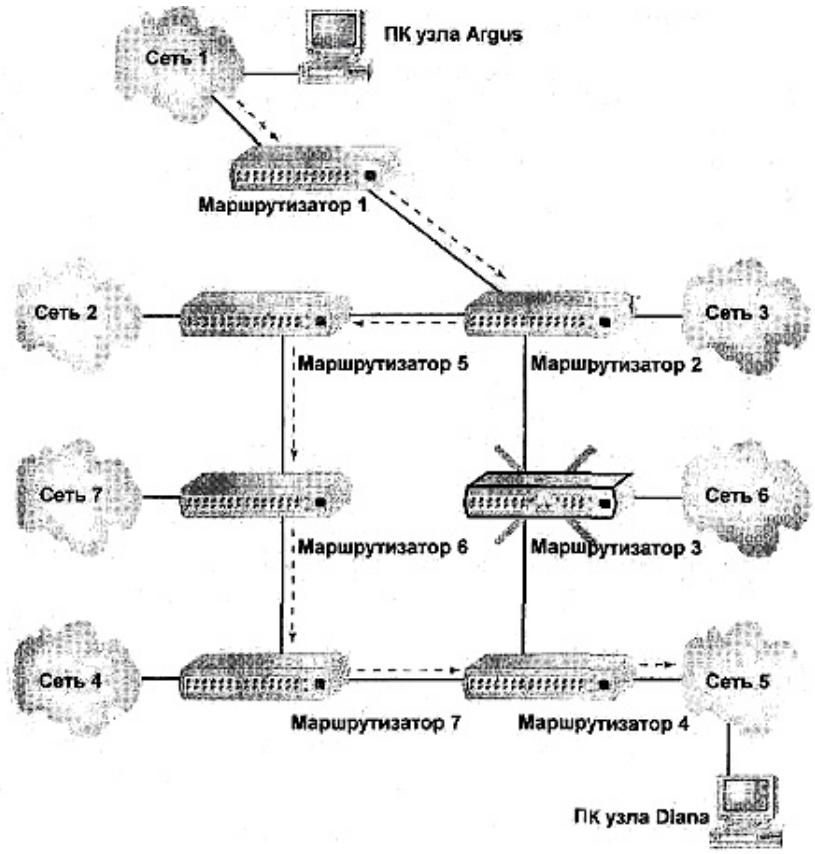


Рис. 5.22. Альтернативный путь между узлами Argus и Diana

Этот пример показывает, что маршрутизация потенциально может для немного больше, чем организация работы мостов, поскольку она более гибкая. Однако следует учесть одно простое соображение: так как каждый раз при встрече пакета с маршрутизатором необходимо определять состояние сети, то время, затраченное на это, должно быть добавлено ко времени "путешествия" пакета. Поэтому маршрутизация требует компромиссных решений. Если маршрутизатор может определить состояние сети для уменьшения излишнего сетевого трафика, или для поиска наименее занятого пути между источником и местом назначения, то все это очень хорошо, поскольку увеличит общую производительность сети. Однако возрастающее время ожидания означает, что было бы, в общем, неплохо минимизировать количество транзитных участков на пути пакета.

Кто позаботится о хранимой информации

Какая информация используется при определении пути пакета к месту назначения и кто отвечает за выбор этого пути? Все зависит от сетевых установок, от средств, поддерживаемых сетью данного типа и ее оборудованием.

Информация о маршрутизации может быть получена на основании данных об узлах. При этом исходный путь определяется информацией, хранящейся в передающем узле, или на основании данных о маршрутизаторах. Путь определяется с помощью информации, хранящейся в сетевых маршрутизаторах.

Примечание

Сети TCP/IP поддерживают узловую маршрутизацию. Сети IPX/SPX ее не поддерживают.

Узловая маршрутизация. Для передачи пакета в сеть с помощью узловой маршрутизации, узел сначала должен установить соответствие имени узла (например, Argus) интерсетевому адресу (например, 12.45.2.15), используя таблицу, получаемую с сервера, хранящего список соответствия имя/адрес. В сетях TCP/IP эту таблицу предоставляет сервер DNS, (Domain Name Service - служба имен домена). Интерсетевой адрес идентифицирует сеть, в которой расположен узел места назначения, а также предоставляет индивидуальный локатор самого узла, используемый после того, как будет найдена сеть.

После того, как интерсетевой адрес будет определен, или *разрешен (resolved),* хост-компьютер (host) сравнивает адреса, принадлежащие части сети, с адресом места назначения. При этом (в случае сети TCP/IP) хост-компьютер просматривает адрес места назначения через собственную маску подсети (см. гл. 3). Если источник и место назначения находятся в одной и той же сети, то источник может послать пакет в место назначения напрямую.

Если же они находятся в разных сетях, то у узла имеются две возможности.

- Послать пакет маршрутизатору сети и позволить ему действовать с данной отправной точки самому.
- Самому определить полный путь к сети места назначения.

В первом случае хост-компьютер посылает пакет на промежуточный маршрутизатор, выбрав его (если доступны несколько) с помощью одного из инструментов, приведенных в табл. 5.1. Хотя этот прием применяется не очень часто, но у узла имеется техническая возможность не только выбрать маршрутизатор для посылки пакета, но и указать весь путь от источника до места назначения. Такая возможность известна как *маршрутизация по источнику (source routing).* Например, в соответствии с протоколом IP, посылающий узел указывает весь маршрут, предоставляя все интерсетевые адреса маршрутизаторов, которые должны быть использованы. В каждом таком маршрутизаторе адрес места назначения IP-дейтаграммы будет обновляться и указывать на следующий маршрутизатор, куда дейтаграмма должна быть послана.

Таблица 5.1. Как хост-компьютеры выбирают маршрутизаторы

Метод	Описание	Дополнительная информация
Статическая таблица маршрутизации	Каждый хост-компьютер поддерживает список всех маршрутизаторов и тех из них, которые следует выбрать, чтобы достигнуть различных сетей	Этот метод быстро работает, но для крупных интерсетей требуются большие таблицы. К тому же эти таблицы трудно обновлять в случае изменений в сети
Динамически обновляемая таблица маршрутизации	Объект сетей TCP/IP, включающий протокол, позволяет маршрутизаторам периодически обновлять таблицы маршрутизации хост-компьютера с помощью своих собственных таблиц	Когда маршрутизаторы обнаруживают лучший путь к отдельному месту назначения, они посылают сообщение узлам своей сети, позволяющее хост-компьютерам обновить свои таблицы
Подслушивание	Некоторые сети поддерживают протокол, позволяющий узлам получать информацию по маршрутизации без использования широковещательной передачи	Сети Windows NT используют для этого протокол Silent RIP

Шлюз по умолчанию	Узел может иметь маршрутизатор, определённый как шлюз по умолчанию, используемый для организации всех интерсетевых связей	Если из соображений обеспечения надёжности работы будут определены несколько шлюзов по умолчанию, второй шлюз будет присоединён только в случае, когда первый шлюз не функционирует
Сетевой запрос	Когда узел готов переслать пакет, он выполняет широковещательную передачу сообщения в сеть, запрашивая наилучший маршрут к данному месту назначения	Все маршрутизаторы в сети будут отвечать на запрос, и, базируясь на их ответах, узел будет выбирать один из маршрутизаторов.

Обеспечить весь путь к каждому месту назначения в сети значительно сложнее, чем обеспечить путь к маршрутизатору, который направляет пакет по требуемому пути. Исходный узел должен либо уже знать путь и воспользоваться им, либо выполнить поиск пути, как это делается и SR организации работы мостов. Роль маршрутизаторов в этом случае аналогична мостам: они отвечают за хранение и направление пакетов, но не вносят каких-либо изменений в их путь.

Примечание

Метод организации работы мостов с маршрутизацией по источнику (SR) и метод узловой маршрутизации по источнику - различные методы, поскольку маршрутизация по источнику базируется на MAC-адресах канального уровня, а маршрутизация, описанная в этом разделе, основывается на IP- и IPX-адресах сетевого уровня.

Поскольку описанная выше маршрутизация по источнику требует интенсивного трафика и работает медленно, она используется не очень часто, за исключением случаев, когда сетевой администратор пытается найти отказавший маршрутизатор, или какую-либо часть сети.

Маршрутизация, базирующаяся на маршрутизаторах. Даже при использовании маршрутизации, базирующейся на узлах маршрутизации, применяются маршрутизаторы, вовлекаемые в нее тем или иным способом. Как только пакет покидает посылающий узел, маршрутизатор становится ответственным за обеспечение прохождения пакета к месту его назначения. Если узел места назначения находится в той же сети, к которой маршрутизатор подсоединен, его работа проста - маршрутизатор адресует пакет к узлу места назначения - и все в порядке. Если же это не так, маршрутизатор должен "проконсультироваться" с таблицей маршрутизации, чтобы из "соседей" выбрать маршрутизатор к которому он подключен, и который при этом выглядит наилучшим кандидатом на передачу пакета. Маршрутизаторы строят свои таблицы в процессе своеобразного "исследования".

Использование таблиц маршрутизации

Таблица маршрутизации может содержать путевую информацию, используемую для достижения как определенной сети, входящей в интерсеть, так и определенного узла интерсети. Таблица маршрутизации потенциально может также содержать информацию о маршрутизаторе по умолчанию, используемую тогда, когда недоступны другие пути. Это избавляет маршрутизаторы и хост-компьютеры от необходимости хранить точные инст-

рукции для достижения каждого возможного места назначения в сети. Если путь не указан, используется путь, заданный по умолчанию.

Табл. 5.2. содержит информацию, которую обычно можно найти в таблице маршрутизации. Названия полей могут не соответствовать указанным в вашей таблице маршрутизации, но информация останется той же.

Если вы работаете на компьютере с установленной операционной системой Windows в сети TCP/IP, то вы сможете проверить свою таблицу маршрутизации компьютера, введя в командную строку фразу ***route print*** (табл. 5.3).

Таблица 5.2. Содержимое таблицы маршрутизации

Запись	Описание
Network ID (ID-сети)	Если запись относится к сети, она содержит сетевой адрес; если – к отдельному узлу, - интерсетевой адрес этого узла
Subnet mask (Маска подсети)	В IP-сети поле содержит 32-битовый номер, используемый для идентификации подсети и отделения её от остальной части сети.
Forwarding address (Адрес направления)	Содержит адрес, по которому должны направляться пакеты, посылаемые данному узлу или сети, ли не содержит ничего, если узел сети подключен к маршрутизатору. Может быть указан адрес как физического, так и сетевого уровня
Interface (Интерфейс)	Идентифицирует порт, который используется для направления пакетов либо с применением номера (аппаратного) устройства, либо адреса сетевого уровня
Metric (Метрика)	Определяет степень предпочтительности отдельного маршрута. Если их (маршрутов) более одного, можно выбрать маршрут с наименьшей стоимостью. Поскольку метрика является функцией стоимости маршрута, то чем меньше ее величина, тем более вероятно, что данный маршрут будет использован. Метрики могут быть получены одним из нескольких способов: подсчетом количества транзитных участков, расчетом задержки (являющейся функцией скорости пути или степенью его перегрузки), вычислением эффективной пропускной способности пути или его надежности
Lifetime (Время жизни)	Используется для маршрутов, динамически обновляемых с помощью какой-либо информации. Указывает, как долго этот путь остается действующим перед тем, как он будет отменен, чтобы маршрутизатор смог реконфигурировать себя в соответствии с обстановкой в сети. Данным столбец может быть невидим в таблице маршрутизации

Таблица 5.3. Информация, выводимая по команде route print

Network address	Netmask	Gateway Address	Interface	Metric
0.0.0.0	0.0.0.0	24.48.12.136	24.48.12.136	1
24.0.0.0	255.0.0.0	24.48.12.136	24.48.12.136	1
24.48.12.136	255.255.255.255	127.0.0.1	127.0.0.1	1
24.255.255.255	255.255.255.255	24.48.12.136	24.48.12.136	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
224.0.0.0	224.0.0.0	24.48.12.136	24.48.12.136	1
255.255.255.255	255.255.255.255	24.48.12.136	0.0.0.0	1

Построение таблицы маршрутизации

Ранее уже описывалось, как хост-компьютеры строят свои таблицы маршрутизации, и установленные для хост-компьютеров требования к маршрутизации достаточно просты. В основном, все, что требуется от хост-компьютера — это знать, где можно найти маршрутизатор, подключенный к интерсети. Чтобы маршрутизация была эффективной, маршрутизаторы должны знать друг о друге. Некоторые из них дают о себе знать всей остальной глобальной сети с помощью так называемого *оповещения.*

Каждый раз, когда маршрутизатор "входит" в сеть, он сообщает другим маршрутизаторам свой адрес и сети, к которым подсоединен. При этом он, по сути, говорит следующее: "Привет! Я, — Маршрутизатор А. Если вы пытаетесь получить доступ в сети 1, 2 или 3, то я могу вам помочь". После того как данный маршрутизатор выполнит широковещательную передачу этой информации другим маршрутизаторам, они добавляют эту информацию в свои таблицы. Чем больше маршрутизаторов будет включено в сеть, тем обширнее у каждого из них должна быть таблица маршрутизации (рис. 5.23).

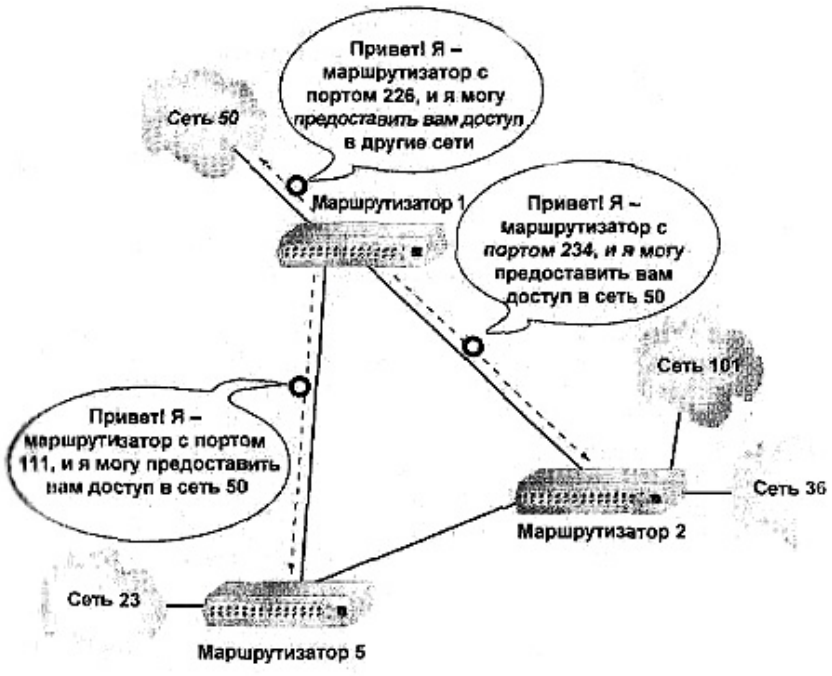


Рис. 5.23. Передаваемое маршрутизатором оповещение помогает другим маршрутизаторам определить, как им следует изменять трафик

Маршрутизаторы будут продолжать оповещать о своем присутствии через определённые интервалы времени после своего первого появления на сетевой «арене». Если возникнут какие-либо изменения в состоянии сети (например, отказ портов), то другие маршрутизаторы отредактируют свои таблицы маршрутизации, отображая изменения в логической структуре интерсети. В противном случае повторы ранее сделанных оповещений типа: «Я всё ещё Маршрутизатор А и я *всё ещё* могу предоставить вам доступ в сети 1, 2 или 3» - игнорируются.

Формат и содержимое таблицы маршрутизации задаются с помощью протокола маршрутизации определённого типа, который определяет, как именно будут генерироваться таблицы маршрутизации. Протокол так же позволяет отслеживать такие «мелочи», как способ конструирования таблицы, тип хранимой в ней информации, способ взаимодействия каждого отдельного маршрутизатора с остальными. Имеется несколько алгоритмов маршрутизации, но здесь их рассмотрение ограничивается двумя примерами протоколов, наиболее часто встречающихся в глобальных сетях: RIP и OSPF.

Протокол обмена данными между маршрутизаторами (RIP – Routing Information Protocol). Это старейший протокол маршрутизации, всё ещё находящийся в употреблении. Хотя в некоторых документах он называется устаревшим, его всё ещё широко используют в маленьких сетях. Компьютеры Windows NT, сконфигурированные для маршрутизации по протоколу IP, поддерживают и RIP.

По умолчанию поддерживающие RIP-протокол маршрутизаторы каждые 30 секунд Оповещают остальную часть сети о своём текущем статусе. Маршруты данной сети (идентифицированной сетевым номером и маской подсети) при условии, что они не обновляются каким-либо другим способом, считаются действующими на период времени ожидания (тайм-аута) 180 секунд. Если время ожидания будет исчерпано, то маршрут не удаляется немедленно из таблицы маршрутизации. Должно произойти шесть обновлений перед тем как маршрут будет окончательно удалён из таблицы маршрутизации. Когда же появляется новый маршрут, он не замещает немедленно аналогичные маршруты, уже существующие в таблице маршрутизации. Если такой маршрут ещё не был определён, он будет немедленно добавлен в таблицу маршрутизации. Если в таблице маршрутизации такой маршрут уже существует, то его замена на новый задерживается на определённый интервал времени (для его подтверждения). Длительность этого интервала зависит от того, исчерпал ли этот маршрут время ожидания, или он всё ещё действующий. Обычно маршруты с одинаковой метрикой, но определяющие другой путь, не замещают существующий маршрут, пока он не исчерпает своё время ожидания.

Следовательно, маршрутизаторы не всегда оперируют новейшей информацией. Хотя это ещё не обязательно конец света, но в принципе такая ситуация далека от идеала. Задержка на подтверждение информации может быть особенно существенна при потере маршрута или при его перегруженности.

Итак, в таблице маршрутизации должны быть отражены два изменения сразу после того, как они происходят: удаление маршрута и возрастание его метрики, т.е. рост стоимости маршрута. Когда случается одно из этих событий, рассматриваемый маршрутизатор выполняет *запускаемое обновление (triggered update).* Запускаемые обновления содержат всю информацию, которая была изменена за время, прошедшее после последнего регулярного обновления, но, в целях экономии полосы пропускания, не содержат не изменившуюся информацию. Этим они отличаются от регулярных плановых обновлений, при которых выполняется полная широковещательная передача всей информации о маршрутизации, независимо от того, изменилась она или нет.

Все эти широковещательные передачи, обновления, запускаемые обновления приводят к возрастанию трафика. Поэтому, в современной реализации протокола RIP не выполняется широковещательная передача информации более чем одному соседнему маршрутизатору (Рис 5.24). После её выполнения обновляющие пакеты исчезают. Это не мешает маршрутизаторам, отстоящим друг от друга на расстоянии в несколько транзитных участ-

ков, выполнить взаимное обновление таблиц, поэтому они продолжают совместно использовать свои полные таблицы маршрутизации. Однако для маршрутизатора 5 потребуется время для обновления данных в соответствии с информацией о состоянии маршрутизатора 10, поскольку обновляющая информация будет течь от маршрутизатора 10 по сети «тонкой струйкой».

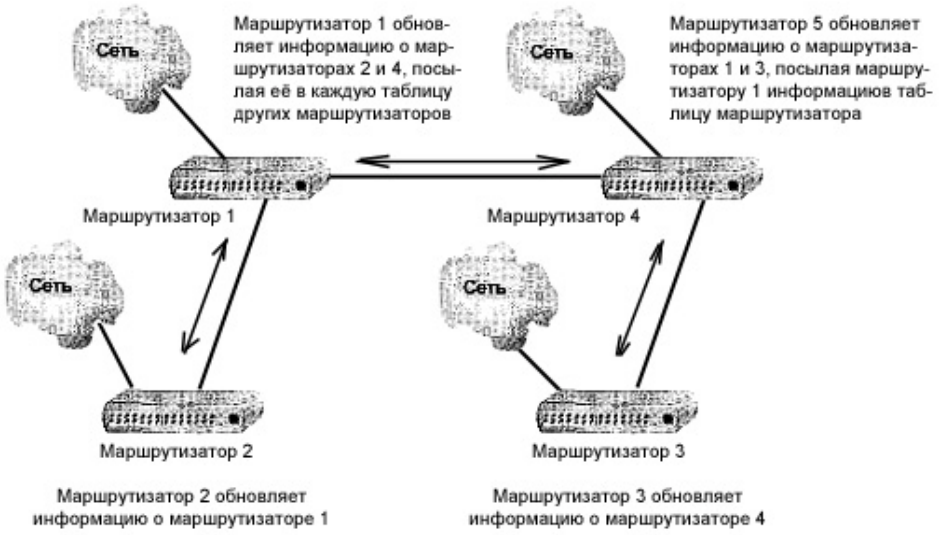


Рис. 5.24. Алгоритм RIP позволяет маршрутизаторам обновлять информацию только в смежных с ними маршрутизаторах в интерсети

Маршрутизация с предпочтением кратчайшего пути (OSPF – Open Shortest Path First). При использовании алгоритма OSPF каждый маршрутизатор в интерсети сразу после запуска объявляет о себе с помощью пакета Hello, впоследствии регулярно повторяемого. Маршрутизаторы, отдалённые на один транзитный участок, «слышат» этот пакет Hello и получают требуемые данные. Подобным образом маршрутизатор через некоторые интервалы времени объявляет свое состояние всем маршрутизаторам в интерсети, что позволяет им определить функционирующие маршрутизаторы и их загруженность.

Все остальные маршрутизаторы получают данные, характеризующие статус данного маршрутизатора и информацию о его таблице маршрутизации, после чего с помощью определенных алгоритмов, определяют *свои* кратчайший путь, или, точнее, путь с наименьшей стоимостью, к отдельной сети, идентифицированной сетевым номером и маской подсети. Идентификация кратчайшего пути не обязательно подразумевает детализацию всего пути. Вместо этого в ходе ее выполнения определяется указатель на маршрутизатор, который и должен обеспечить путь с наименьшей стоимостью. Если для использования доступно несколько действующих путей с одинаковой метрикой, маршрутизатор будет применять все эти пути, распределяя по ним свой трафик с целью равномерной загрузки сети. Такой способ отличается от применяемого в алгоритме RIP, при котором устанавливается только один путь от каждого источника к каждому месту назначения.

Несмотря на то, что маршрутизаторы совместно используют таблицы маршрутизации только с соседними (с ними) маршрутизаторами, свои состояния они изменяют применительно к состоянию всей сети. Для уменьшения трафика маршрутизаторы, использующие алгоритм OSPF, могут быть подразделены на группы, называемые *областями (area)*. При этом в сети выполняется лавинообразная маршрутизация только в пределах данной области с помощью магистральных маршрутизаторов, предназначенных для пересылки таблиц маршрутизации между областями, как показано на рис, 5.25. Вторичные маршрутизаторы области подключают каждую область к магистрали, поддерживая структуру связей в виде логического дерева.

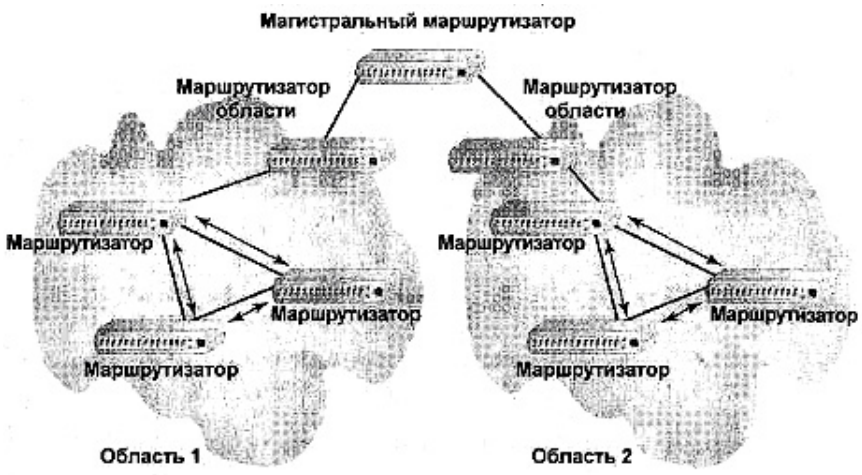


Рис. 5.25. Определяемые в соответствии с алгоритмом OSPF области уменьшают трафик сети

Поскольку каждый маршрутизатор предназначен только для определения кратчайшего пути к месту назначения, магистральный маршрутизатор должен поддерживать несколько версий алгоритма маршрутизации. Очевидно, что путь, кратчайший в одном случае, может не быть таковым в другом. Результаты обработки информации с помощью алгоритма передаются далее в соответствующую область.

Шлюзы для мэйнфреймов

Большинству читателей этой книги, скорее всего, никогда не приходилось обеспечивать связь с мэйнфреймами, однако если вы собираетесь это далось, то знайте, что вам потребуется устройство, называемое *шлюзом (gateway).* Шлюзы выполняют более сложную работу, чем мосты или маршрутизаторы. Мосты просто извлекают информацию из вашего пакета, просматривают адреса источника и места назначения, и передают пакет в требуемое, место. Маршрутизаторы просматривают информацию в пакете и передают пакет от одного маршрутизатора другому, изменяя адреса канала связи источника и места назначения вдоль пути, но не изменяя никакой другой информации внутри пакета. Шлюзы могут эффективно трансформировать информацию, записанную в формате одного стандартного протокола, в формат другого. Шлюзы обрабатывают данные, переносимые между сетями, использующими в корне отличные протоколы, с помощью одного из двух способов: *туннелирования и эмуляции терминала.*

Связь с помощью протокола туннелирования

Наиболее общим методом, требующим наименьшей загрузки процессора, является *туннелирование.* Оно выполняется инструментальными средствами, с помощью которых шлюз перемещает пакеты, принимая информацию из первой сети в одном формате, упаковывая ее во взаимно понятный формат и перенося в сеть, использующую другой формат. Концептуально туннелирование аналогично почтовой связи между офисами. Если вы получите служебное письмо, циркулирующее в вашем главном офисе, которое должен увидеть ваш коллега Том в каком-то филиале компании, то вы не сможете просто переслать ему по почте само письмо. Система адресации, используемая для писем (с указа-

ниями "Кому" и "От кого") прекрасно работает внутри офиса, но обычное почтовое отделение не будет знать, что с ним делать. Поэтому вам следует упаковать письмо в конверт, формат которого понимает и почтовое отделение, и филиал компании и вы сами. Когда письмо в конверте попадет в филиал, оно будет направлено Тому, он вскроет конверт и достанет ваше письмо.

Допустим теперь требуется послать пакет в соответствии с протоколом IPX фирмы Nowell из вашей сети, построенной на PC-компьютере, на компьютер Macintosh и сети AppleTalk. Обе сети — и NetWare, и AppleTalk — понимают TCP/IP, поэтому его можно использовать для передачи информации. Доставляя пакет IPX в сеть компьютеров Mac, сеть PC инкапсулирует пакет в "конверт" TCP/IP и посылает пакет в этой оболочке компьютеру Mac. Когда Mac его получит, он вскроет конверт TCP/IP. Заметим, что компьютер Mac все-таки должен выполнить некоторые преобразования, приводящие данные PC в понятную ему форму. Однако такое преобразование не является проблемой шлюза: раз данные перемещены из сети PC в сеть Mac, работа шлюза закончена. Принцип туннелирования показан на рис. 5.26.

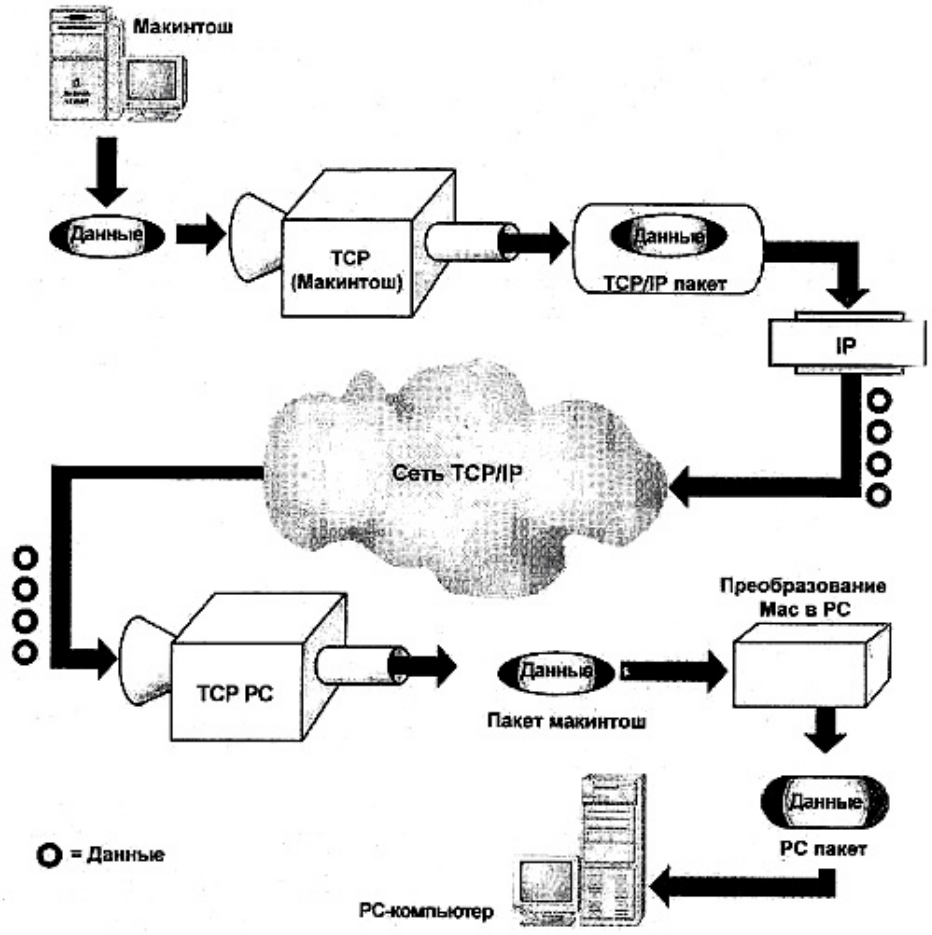


Рис. 5.26. Туннелирование в действии

Связь с помощью эмуляции терминала

Другой метод организации работы шлюза для переноса данных называется *эмуляцией терминала.* Мэйнфреймы изначально не проектировались для "переговоров" с персональными компьютерами. Они предназначались для связи с "неинтеллектуальными" (dumb) терминалами. Следовательно, когда ПК требуется связаться с мэйнфреймом, он

должен выдавать себя за неинтеллектуальный терминал. Существуют два метода эмуляций терминала: применение плат эмуляции и использование программ эмуляции типа Reflection или Attachmate.

Есть два способа успешной реализации эмуляции терминала в сетевом окружении: установка в ПК плат эмуляции терминала или создание шлюзов. В первом случае на каждом ПК, которому требуется обеспечить доступ к мэйнфрейму, следует установить плату эмуляции терминала. Их конфигурирование может оказаться непростым делом. На рис. 5.27 показана установка двух коммуникационных плат в систему, для которой может потребоваться одновременный доступ и к мэйнфрейму, и к сети, что приведет к аппаратным конфликтам и зависанию. К тому же это достаточно дорого.

Альтернативный метод заключается в выделений какого-либо ПК для управления всей эмуляцией, выполняемой в сети, так что этот ПК сам становится шлюзом (gateway server). Плата (или платы) эмуляции терминала будут установлены только на этом компьютере, как показано на рис. 5.28. Пользователи будут обращаться к шлюзу и мэйнфрейму, используя программное обеспечение каждой рабочей станции.

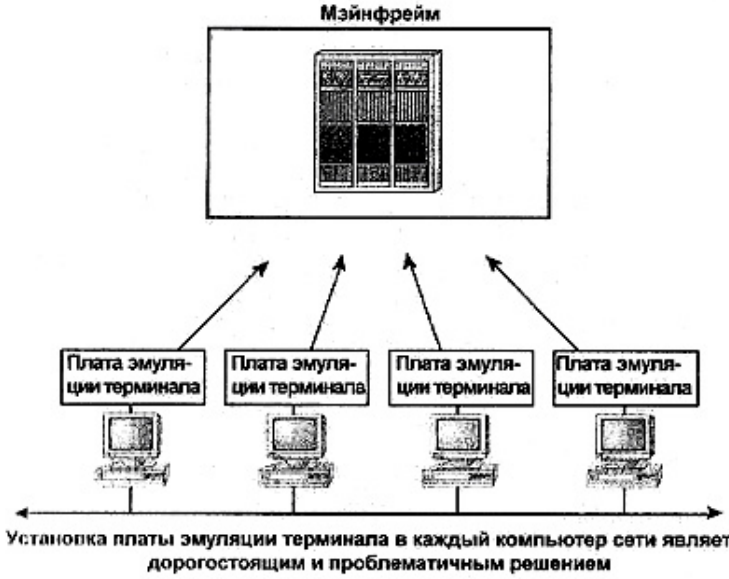


Рис. 5.27. Использование индивидуальных плат эмуляции терминала для доступа к мэйнфрейму

Рис. 5.28. Использование шлюзового компьютера и программного обеспечения эмуляции терминала для доступа к мэйнфрейму

Эмуляция терминала имеет три основных недостатка.

Она дорого стоит. Необходимо купить дополнительное оборудование и программное обеспечение, чтобы ваши ПК могли связываться с мэйнфреймами.

Она медленно работает. Всякий раз, когда одна операционная систему выдается за другую (эмулирует ее), это приводит к затратам времени.

Дополнительное оборудование и программное обеспечение будет причиной большего количества сбоев оборудования. Причина не в том, что платы эмуляции терминала более "конфликтны", чем какие-либо другие, а в том, что ваш компьютер имеет ограниченное количество прерываний и адресов DMA, доступных этим платам.

Познакомившись ближе с этими проблемами, вы, возможно, проявите интерес к использованию шлюза — выделенного компьютера, управляющего связями всех ПК с мэйнфреймом. Хотя, используя шлюз, вы и не избавитесь от этих проблем, но они будут ограничены одним компьютером, а не возникать на всех ПК, которым требуется доступ к мэйнфрейму. Компьютерам, подключенным к шлюзу, также будет необходимо программное обеспечение, но им не потребуются собственные платы эмуляции терминала.

Выводы

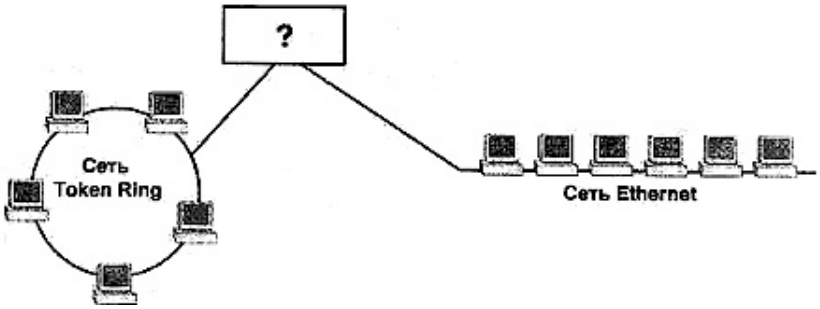
Как вы могли заметить, сетевое аппаратное обеспечение является достаточно сложным. Но, к сожалению, без него не обойтись. Даже в простейшей сети вам часто может потребоваться концентратор для связи между отдельными узлами сети. Как только сеть станет более крупной и сложной, вам будут нужны повторители для увеличения физической протяжённости сети, а также коммутаторы для управления трафиком, связями и фильтрацией пакетов. Поэтому вы будете искать устройства с функциональными возможностями нескольких устройств, сочетающими, например, концентратор/коммутатор или мост/маршрутизатор.

Завершающей задачей создания "нервной системы" вашей сети является использование некоторых интерсетевых устройств, рассмотренных в этой главе. В гл. 6 вы познакомитесь с глобальными сетями, в которых чаще всего используются маршрутизаторы.

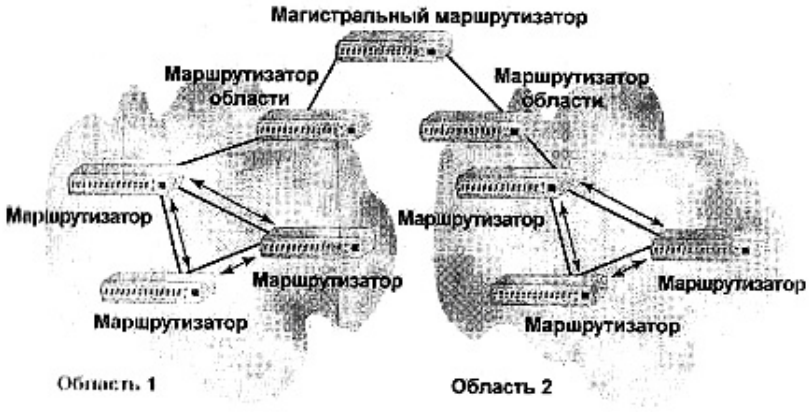
Упражнение 5

1. Вы пытаетесь связать между собой две локальные сети: Ethernet и Token Ring. Какое устройство требуется для этого использовать?

   A. Прозрачный мост.
   B. Маршрутизатор.
   C. Мост с маршрутизацией по источнику.
   D. Коммутатор.



2. Какие общие функциональные возможности у коммутаторов и мостов и каково их назначение?
3. Эта диаграмма иллюстрирует один из методов оповещения маршрутизатора. Каково его полное название?



Глава 6

Общие сведения О глобальных сетях

Точно так же, как локальные сети (LAN) позволяют расширить "область деятельности" отдельного компьютера глобальные сети (WAN) расширяют локальные. Глобальные связи требуются отнюдь не всем, но даже если в постоянных глобальных связях нет необходимости, их периодическое использование имеет такие достоинства.

- Совместное использование информации.
- Улучшенная связь с помощью электронной почты и программ оперативного планирования заданий (online schedule software).
- Централизованная система архивирования и защиты файлов.

Более того, глобальные сети, практически, имеют все возможности локальных — просто они дополнительно расширяют область их действия. Польза от их применения ограничена, главным образом, скоростью работы: глобальные сети работают с меньшей скоростью, чем локальные.

В гл. 8 описывается оборудование, необходимое для создания сервера коммуникаций либо организации прямого соединения любого компьютера с внешним миром. Давайте прямо сейчас рассмотрим технологии обеспечения сетей средствами связи с внешним миром как с помощью двухточечных соединений, так и путем создания частных глобальных сетей (worldwide private networking).

Технология глобальных сетей

Для описания локальных и глобальных сетей применяется схожая терминология, но для глобальных используют дополнительные, отчасти жаргонные, выражения, которые следует знать. Кроме того, отдельные понятия, применяемые при описании сети, охватывающей определенную область (штат, район, область и т.п.), имеют несколько иной смысл, чем понятия, применяемые к сетям, расположенным в пределах комнаты.

Представление данных

В большинстве современных сетевых технологий при описании передачи данных используют такое понятие, как *пакеты* (packets), в которых содержатся данные, и адресная информация. Пакеты удобно представлять в виде обычного письма.

- Конверт идентифицирует пакет как некую автономную структурную единицу в общем потоке корреспонденции и отмечает его как часть, отдельную от прочих сетевых данных.
- Адресная информация идентифицирует получателя и (обычно) отправителя пакета.
- В начале пакета содержится адресная информация, а собственно данные находятся в середине пакета.

Конверт - это структура пакета; он содержит данные записанные в формате, "понятном" линии связи. Точно так же, как почтовая система, использующая пакеты FedEx, не сможет обработать письма UPS Ground, в большинстве линий связи использует некоторый стандартный формат данных. Размер пакета определяется его типом. Так, в *сетях с ретрансляцией кадров* (Frame Relay) передаются пакеты, называемые кадрами (frames), имеющими разные размеры, а в *сетях с ретрансляцией ячеек* (Cell Relay), таких, как служба коммутируемой мультимегабитной передачи данных (SMDS), передают *ячейки* размером 53 байта.

Примечание

Пакеты разных типов отнюдь не идентичны. Как вы увидите далее, в сетях с коммутацией пакетов (packet-switched network) различного типа, пакеты могут включать дополнительную информацию. Так, в пакеты стандарта X.25 вводится информация по контролю ошибок, а в Frame Relay - нет.

Так же, как и в локальных сетях, пакеты, передаваемые ,по глобальной сети, для достижения места назначения необходимо снабдить некоторой адресной информацией. Даже если выполнить широковещательную передачу пакета во все каналы глобальной сети, но в нем не указать адреса назначения, предполагаемый получатель не распознает, что пакет предназначен ему. Если требуется какое-либо подтверждение приема, то в пакет следует включить адрес отправителя. В противном случае получатель просто получит пакет, и на этом все закончится. Пакеты, не требующие подтверждения приема, называют *дейтаграммами.*

Примечание

В большинстве современных линий связи глобальных сетей используют дейтаграммы, поскольку скорость их передачи выше, а для глобальных сетей это чрезвычайно важно. При работе по устаревшим, ненадежным линиям связи все еще используют связь с логическим соединением.

Чтобы по сети можно было передавать данные, необходим конверт и адресная информация. А вот формат передаваемых данных важен только для узла, который принимает пакет, "вскрывает конверт" и читает адресованную ему информацию.

Сравнение методов коммутации пакетов и коммутации каналов

Пакеты очень важны, поскольку глобальные сети, называемые *сетями с Коммутацией пакетов (packed-switched network),* построены именно по принципу использования пакетов. При таком методе коммутации нужны указания о том, каким образом данным следует искать путь от источника к месту назначения, подобно методам .маршрутизации (см. гл. 5).

В *сетях с коммутацией каналов (circuit-switched networks)* задается статический путь от одного пункта к другому. В начале каждого сеанса передачи данных между отправителем и получателем устанавливается соединение. Этот виртуальный путь используется в течение всего сеанса. По нему следуют все данные, передаваемые отправителем. Поскольку доступен единственный путь, нет необходимости вводить в данные обширную адресную информацию — пакеты не могут затеряться. Таким образом, можно использовать пакеты меньшего размера, так как в них содержится меньший объем данных. Досадным последствием этого метода является то, что установленный виртуальный канал дол-

жен использоваться в течение *всего* сеанса, даже если станет доступным другой, более эффективный путь.

Напротив, пакетная коммутация весьма напоминает маршрутизацию (см. гл. 5) тем, что между отправителем и получателем в этом случае *не* устанавливается виртуальный канал связи. Здесь не организуется единственный путь для данных. Сеть в этом случае можно представить себе как набор коммутируемых узлов (switching points), которые направляют данные по собственному пути. Это же предполагает и некоторую их задержку в коммутируемых узлах, поскольку в каждом таком узле должен быть определен наиболее эффективный его дальнейший путь. Конечно, по человеческим меркам задержка невелика. Однако сети с коммутацией пакетов не обеспечивают столь же высокого качества передачи в режиме реального времени,
как сети с коммутацией каналов. Если вы устанавливаете голосовую связь, используя технологию IP, то учтите, что звук будет передаваться хуже, чем по линиям с коммутацией каналов. Оба метода маршрутизации сравниваются в табл. 6.1.

Таблица 6.1. Сравнение коммутации пакетов с коммутацией каналов

Сетевое средство	Коммутация пакетов	Коммутация каналов
Тип соединения	Без соединения	Логическое соединение
Статический путь или динамическая маршрутизация	Не используется предварительное задание пути для всего сеанса. Пакеты маршрутизируются соответственно уровню трафика	На весь сеанс задаётся статический путь между узлами
Содержимое пакетов	Пакеты данных содержат информацию по маршрутизации	Пакеты данных содержат адресную информацию

Быстродействие и надежность сети

Нигде не сказано, что глобальная сеть *должна* работать медленнее локальной, однако это почти всегда так. Главным образом это обусловлено высокой стоимостью скоростных линий связи. На практике хорошее соединение глобальной сети работает на скорости около 2 Мбит/с, весьма далекой от 100 Мбит/с, доступной в современных локальных сетях Ethernet. До тех пор пока вы не потребуете от глобальной сети сделать больше, чем она может, это нельзя отнести к ее недостаткам, однако об этом следует помнить.

Быстродействие линии связи — не совсем корректная мера эффективности соединения. Реальная мера скорости сети — *пропускная способность* — рассчитывается с учетом двух факторов: доступной для использования полосой пропускания и сетевой скорости. *Полоса пропускания* описывает ширину полосы частот или количество каналов, а также объем данных, которые можно пропустить по каналу за единицу" времени. Усиление "конкуренции" за полосу пропускания замедляет работу соединения, поскольку пакеты должны ожидать своей очереди. Это несколько напоминает движение по дороге, забитой транспортом: в зависимости от плотности движения путешествие займет у вас разное время.

Сетевая скорость (network speed) является функцией, зависящей от скорости перемещения данных по каналу. Как указано в гл. 1, скорость передачи данных зависит от среды связи. Чем лучше канал защищен от помех, тем быстрее перемещаются данные. Соче-

тание полосы пропускания с сетевой скоростью и определяет реальную пропускную способность сети.

Примечание

Пропускную способность не всегда можно определить однозначно. В глобальных сетях используют как *полудуплексную,* так и *дуплексную* технологии - способы передачи пакетов, проходящих по каналу связи. При полудуплексной связи пер<> даются данные в единственном направлении, в то время как при дуплексной - в обоих. Для полудуплексной связи требуется большая полоса пропускания (поскольку каналы можно объединить), однако дуплексная связь более гибкая.

Другая, не менее важная, характеристика сети — надежность. Если каналы передачи данных подвержены помехам, то либо канал окажется не в состоянии управлять слишком "плотным" потоком данных, либо некоторые пакеты будут потеряны.

Кроме того, помехи могут исказить данные. Чтобы гарантировать идентичность переданных и принятых данных, необходим метод контроля ошибок. Напомним: в большинстве современных глобальных сетей передаются дейтаграммы и, следовательно, отправитель не получает подтверждения приема. Как же узнать о необходимости повторной отсылки пакета? И как исправлять ошибки? Отнюдь не во всех глобальных сетях предусмотрен контроль ошибок, однако в сетях спроектированных для передачи данных по ненадежным каналам, он используется обязательно.

Для контроля ошибок обычно используют методы, известные под общим названием *контроль с использованием циклического избыточного кода* (CRC - *Cyclic Redundancy Checking).* Прежде чем передать пакет, отправитель выполняет вычисления, основывающиеся на данных, содержащихся в пакете с помощью особого алгоритма, использующего данные и адресную информацию пакета в качестве переменных некоторого уравнения. Алгоритм и ожидаемый результат добавляются к содержимому пакета. Когда конечный узел получает пакет, он также выполняет вычисления по этому же. алгоритму. Если полученный ответ не совпадает с помещенным в пакет, получатель отсылает сообщение об ошибке отправителю. Затем он просит повторно прислать исходный пакет. Обратите внимание: получатель *не исправляет*
ошибки в пакете — технология CRC такого не предусматривает. Она просто позволяет получателю определить, не искажены ли поступившие данные и при необходимости запросить их повторно.

Примечание

Методы CRC обеспечивают высокую надежность связи, однако, поскольку они увеличивают объем пакетов, уменьшается пропускная способность сети. Поэтому их применяют для передачи данных по сетям, надежность которых невысока, скажем, Internet и X.25.

Сравнение методов передачи кадров и передачи ячеек

В разделе "Представление данных" было упомянуто, что пакет, т.е. "конверт", используемый в глобальных сетях, может иметь формат ячейки или кадра. Как известно, в сетях разного типа используются и пакеты разных типов. Вспомните: сети Ethernet и Token Ring взаимно несовместимы, поскольку их пакеты содержат не совсем одинаковую информацию, по даже одинаковая информация организована в них по-разному. В глобальных сетях различия более глубокие. Отличия сетей Ethernet и Token Ring, в основном, относятся к способам управления трафиком (главным образом, к исключению возможности одновременной передачи двумя узлами). В глобальных сетях основное внимание уделяют проблеме наилучшего использования ограниченного объема трафика (traffic space).

Выбор определённого метода влияет на выбор типов данных для использования в конкретной среде.

Технологии формирования кадров. Основная задача технологий формирования кадров заключается в достижении максимальной пропуск поп способности в пределах доступной полосы пропускания. Идея состоит в том, что чаще всего передача данных по сети происходит не непрерывно, а "скачками", если использовать соответствующий жаргон. Это справедливо для передачи как по глобальным, так и локальным сетям. Работая за компьютером, вы не используете сеть постоянно. Большую часть сетевых данных можно сохранять или кэшировать локально — сеть используется только короткое время, причем совсем необязательно занимать всю доступную полосу пропускания.

Высокие сетевые скорости в локальных сетях делают возможным "захват" всей сети единственным пользователем на весь сеанс. Это приемлемо из-за небольшой продолжительности сеанса. Если же возникают проблемы с трафиком, есть можно сегментировать. Однако в глобальных сетях все обстоит несколько иначе. Вообще говоря, эти сети работают медленнее и по ним передается большее количество данных, чем по локальным сетям. Более того, захват всех ресурсов глобальной сети каким-либо узлом локальной, скажем, для передачи письма, совершенно неприемлем. Поэтому при формировании кадров смешивают данные, передаваемые всеми пользователями сети, в одну "кучу" и отсылают их все сразу. Когда данные поступают на другой конец сети, они сортируются и маршрутизируются по месту (местам) конечного назначения. При этом используется весь канал целиком, причем одновременно несколькими устройствами. Таким образом, эффективная полоса пропускания сети, где используется технология сборки кадров, заметно превосходит фактический размер полосы канала (т.е. полосы, которую имел бы этот канал в локальной сети).

При данном методе передачи возникает несколько, проблем. Первая: если в какой-то момент времени понадобится полоса пропускания шириной, больше доступной для использования, некоторые пакеты будут пропущены. С помощью механизма, подробнее рассмотренного далее в разделе о ретрансляции кадров, пропущенные пакеты отыскиваются и посылаются повторно. Вторая проблема: не все пакеты прибывают по месту назначения в том же порядке, что отсылались. Из этих проблем вырастает третья: данные поступают по месту назначения не в виде хорошо сглаженного потока, а в том виде, в котором они были подготовлены и отсортированы в конце путешествия по сети с формированием кадров.

В большинстве случаев это не имеет значения: сервер интерпретирует запрос на открытие файла с перепутанной последовательностью данных (scrambled order) столь же легко, как и файла в исходном формате. Однако это имеет *решающее* значение при работе в режиме реального времени и здесь предпочтительно использовать технологию ретрансляции ячеек.

Технология ретрансляции ячеек. Технология ретрансляции ячеек была разработана главным образом для возможно более "гладкой" передачи данных различных типов. В этом случае максимальное использование полосы пропускания отходит на второй план. Все данные (текстовая, видео и звуковая информация и т.д.), передаваемые с ретрансляцией ячеек, разделяются на *ячейки* размером 53 байта и передаются по сети непрерывным потоком, причем данные, требующие передачи в режиме реального времени, являются первоочередными. Когда данные поступают в место назначения, они принимаются в том же порядке, в котором передавались.

Удаленный доступ к сети

Когда вы слышите выражение "глобальная сеть", первое, что вам приходит в голову — карта, на которой показан главный офис в Чикаго и филиалы по всей стране. Однако отнюдь не все глобальные сети предназначены для связывания офисов. Иногда задачи такой связи намного скромнее — это может быть обеспечение служащего-надомника средствами обмена электронной почтой с офисом или находящегося в командировке коммивояжера доступом к базе данных заказчиков. Если все это уже есть в офисе, вы, вероятно, захотите воспользоваться такими возможностями и вне офиса.

Те, кому не по плечу создание сложной глобальной сети либо необходимы более гибкие средства, чем предоставляемые глобальной сетью с проложенными раз и навсегда кабелями, весьма полезен удаленный доступ, реализованный в той или иной форме. В настоящее время известны три основных вида организации удаленного доступа.

- Удаленное присутствие в сети (удаленный доступ).
- Дистанционное управление главным компьютером.
- Удаленный доступ к компьютеру, работающему под управлением многопользовательской операционной системы.

Во всех этих случаях в системах организации удаленного доступа используют три общих элемента. Во-первых, на сетевом компьютере должно быть установлено программное обеспечение, позволяющее устанавливать с ним связь по телефонным линиям. Это программное обеспечение называют *серверным элементом.* Во-вторых, на клиентом компьютере (выходящим на связь по телефонной линии) должно быть установлено программное обеспечение, позволяющее набрать номер и установить связь с другим компьютером. Это программное обеспечение называют *клиентным элементом.* В-третьих, клиент должен поддерживать, не только сетевой протокол, позволяющий связаться с сетью после установления удаленного соединения, но также и дополнительный, называемый *протоколом линии связи,* который нужен для соединения с сервером удаленного доступа (dial-up server). В качестве протокола линии связи обычно используют протоколы SLIP (Slip Line Protocol — протокол последовательной межсетевой связи) или PPP (Point to Point Protocol — протокол двухточечной связи). Большинство серверов поддерживают протокол PPP, поскольку он производительнее и проще в установке.

Защита в системах удалённого доступа

Защита глобальных и локальных сетей подробно рассмотрена в гл. 15. В данный момент вам следует знать, что удалённое управление и удалённый доступ приводят к появлению проблем защиты, которые отсутствуют в локальных сетях. Причём это связано именно с тем, что с помощью средств удалённого доступа локальные сети могут стать частью международной *и* не защищённой сети. Если вам не понятно, задумайтесь: проникновение в локальную сеть, не соединённую с внешним миром, требует физического доступа к сети. Для дистанционного управления (или удалённого доступа, если на то пошло) физический доступ не нужен. Более того, физический доступ так же значительно облегчается, поскольку к локальной сети оказывается подключенной вся телефонная сеть. В этом нет ничего нового, если мы вспомним вездесущую сеть Internet, однако над этим следует задуматься. В системы удалённого доступа и дистанционного управления встроены определённый средства защиты от несанкционированного доступа, и вы обязательно должны их использовать.

Системы дистанционного управления имеют дополнительные системы защиты. Они предоставляют удаленному пользователю доступ к главному компьютеру, а также позволяют запускать на нём приложения без санкции лиц, постоянно следящих за исполнением приложений и отображением каких-либо файлов на экране. Проблемы с людьми, которые не имеют намерений подсмотреть что-либо, а просто любят отвлекаться на посторонние занятия, можно решить, отключив монитор. А вот чтобы помешать потенциальным злоумышленникам, следует использовать программное обеспечение дистанционного управления, которое всё отображает на мониторе клиентного компьютера и *ничего* – на главном. Эта проблема не существенна для систем удалённого доступа, поскольку в них не используется сетевой компьютер, а просто выполняется вход в сеть по особому соединению. Точно так же, это не имеет большого значения для тонкого клиента, поскольку сеанс работы пользователя не отображается на экране сервера.

Системы дистанционного управления

Программное обеспечение дистанционного управления позволяет на расстоянии "захватить" компьютер (автономный или сетевой) и управлять им с помощью клавиатуры или мыши. Как показано на рис. 6.1, вся обработка данных при этом выполняется главным компьютером, а, клиентному остается только предоставить область ввода и отображать на экране то, что происходит в главном компьютере, установленном в офисе. Кроме того, программное обеспечение дистанционного управления часто используют для передачи (и синхронизации) файлов.

Рис. 6.1. Линия связи дистанционного управления компьютером

Как указывалось в предыдущем разделе "Защита в системах удаленного доступа", программное обеспечение дистанционного управления позволяет запустить компьютер,

просто позвонив по телефону. Во время сеанса дистанционного управления щелчки мыши или нажатия клавиш передаются на сетевой (главный (host)) компьютер, а изображения на экране - на удаленный компьютер (гость).

Для дистанционного управления необязательно выполнять идентификацию в сети, однако одна из машин должна быть выделена для работы в качестве главной. Вы не можете дистанционно управлять машиной, на которой в данный момент кто-нибудь уже работает. Хотя, в принципе это возможно, но это допустимо при поиске и исправлении неполадок в компьютере. Например, можно установить на свой компьютер, а также компьютер своих родителей программное обеспечение дистанционного управления. Теперь вам будет значительно проще устранять сбои в работе электронной почты на их компьютере. Однако на дистанционно управляемом компьютере не могут одновременно работать два человека.

Программное обеспечение дистанционного управления состоит из двух частей.

- Программное обеспечение дистанционного управления главной машиной, которое загружается в офисный компьютер.
- Программное обеспечение дистанционного управления клиентной машиной, которое загружается в клиентный компьютер, используемый для дистанционного управления главной машиной.

Эти части не всегда отделены друг от друга. Даже если вы загрузите в оба компьютера одинаковое программное обеспечение, то будут установлены оба компонента.

Совет

В некоторых пакетах допускается разделение компонентов главной машины и клиента, т.е. их раздельная загрузка, что четко разделяет их роли. Если вам необходимо, чтобы с одного из компьютеров можно было управлять другими, но никогда - наоборот, это будет очень полезно.

После подключения к главному компьютеру, вы можете использовать его точно так же, как будто сидите перед ним. Программы для дистанционного управления обычно поддерживают передачу и даже синхронизацию файлов, с тем, чтобы вы могли автоматически обновлять файлы на клиентном компьютере. Используемые приложения не обязательно загружать на клиентную машину. Необязательна даже их поддержка. Так, вы можете запустить 32-битовую программу на клиентной машине, работающей под управлением 16-битовой операционной системы, скажем, Windows 3.x. Самое главное, чтобы клиентная машина отобразила информацию, поступающую от главной машины.

Тип соединения, используемого для дистанционного управления сетевым компьютером, не обязательно должен совпадать с применяемым для непосредственной работы на нем. Модемное соединение обычно поддерживает скорость около 40 Кбит/с. Модемы, рассчитанные на 56 Кбит/с, фактически никогда не передают данные с такой скоростью. Это намного меньше скорости 100 Мбит/с, достижимой в локальной сети, что весьма существенно, даже если вам необходимо передавать по линии только видеоизображения и иногда - файлы. Поэтому программное обеспечение для удаленного доступа обычно поддерживает на клиентной стороне кэширование точечных рисунков (bitmap caching). Это позволяет избежать повторной загрузки изображения ранее загруженных компонентов рабочего стола главного компьютера при каждом перемещении мыши. Точно так же, чтобы избежать перегрузки файлов, программное обеспечение для дистанционного управления должно поддерживать обновление файлов, при котором (и отличие от их замены) загружаются только изменения, внесенные в файл, но не весь файл. Для текстовых файлов это несущественно, однако любой менеджер, обновляющий базу данных о клиентах с помо-

щью программ дистанционного управления, оценит возможность пересылки только измененных записей базы данных, а не всей базы.

Системы удаленного доступа

В отличие от программы дистанционного управления, позволяющей удаленному компьютеру управлять сетевым, программное обеспечение организации удаленного доступа предоставляет *непосредственный* доступ в сеть с помощью процедуры удаленной идентификаций. Иными словами, клиентный компьютер сам становится частью сети, только он соединяется с ней по телефонной линии (через модем), а не кабелем "витая пара", допускающим скорость передачи до 100 Мбит/с, с которой работают остальные сетевые компьютеры (рис. 6.2). Точно так же (как если бы вы сидели за столом в офисе, расположенном за несколько миль от вас) данные загружаются с файлового сервера в память удаленного компьютера для дальнейшей обработки. Все запущенные приложения используют ресурсы *клиентного* компьютера.

Рис. 6.2. Линия связи системы удаленного доступа к сети

Для организации удаленного доступа к локальной сети, вам необходимо:

- программное обеспечение сервера удаленного доступа, запущенное на главном компьютере;
- клиентное программное обеспечение для организации удаленного доступа, установленное на клиентном компьютере;
- учетная запись в сети.

Если все это есть, то дозвонившись на сервер, входите в сервер удаленного доступа, и вы — в сети. Установив соединение, можете делать в сети все, на что имеете разрешение: редактировать файлы, принимать/отсылать электронную почту, копировать файлы и т.п. Набор прав может быть точно таким же, что при обычном входе, но может быть ограничен: например, вы можете работать только с сервером удаленного доступа, но не со всей сетью.

При дистанционном управлении количество главных и клиентных компьютеров совпадает. В то же время при удаленном доступе единственный сервер может поддерживать сотни удаленных соединений. Точное число зависит от возможностей программного обеспечения. Так, сервер удаленного доступа Windows 98 поддерживает единственное соединение, а Windows NT- до 256.

Поскольку удаленный доступ позволяет включить компьютер в сеть, поддержка программных средств, необходимых для обработки, данных возлагается на клиентную машину. Таким образом, клиент удаленного доступа должен располагать большими ресурсами, чем клиент системы дистанционного управления, который может "опираться" на ресурсы главного компьютера.

Многопользовательские соединения

Прямой удаленный доступ третьего типа, приобретающий популярность в последнее время, обеспечивает соединение с многопользовательским сервером (multiuser server), позволяя запускать на нем приложения, используя тонкий клиентный протокол (thin client protocol) (рис. 6.3). Напомним: в тонкой клиентной сети приложения выполняются сервером, а результаты отображаются на экране клиентного компьютера. Как и при дистанционном управлении, щелчки кнопкой мыши и нажатия клавиш передаются на сервер и им же интерпретируются.

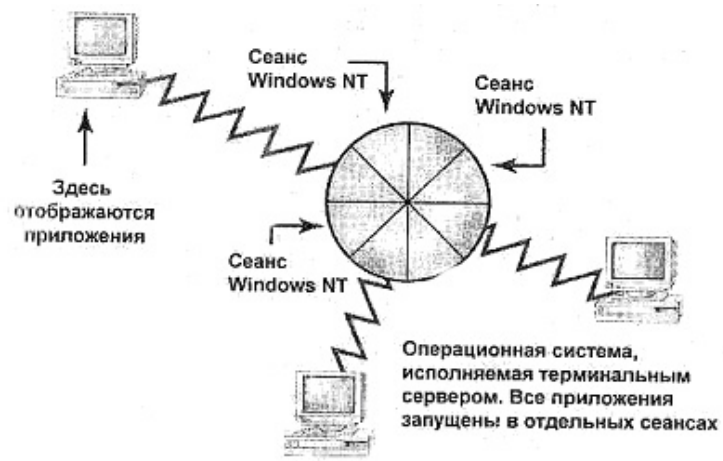


Рис. 6.3. Удаленное соединение с многопользовательским сервером Windows

Все это выглядит примерно так. Сетевой сервер работает под управлением многопользовательской версии какой-нибудь операционной системы, скажем, Windows NT. Каждый тонкий клиент звонит на сервер и устанавливает соединение с ним. После этого сервер организует для данного соединения виртуальную машину, работающую под управлением Windows NT, которая используется исключительно данным клиентом. Таким образом удаленный доступ может получить большое число клиентов — ограничения на их количество налагаются только количеством лицензий, объемом требуемой памяти и тактовой частотой процессора (CPU cycles).

Такая система напоминает дистанционное управление машиной в том смысле, что в ней осуществляется удаленное выполнение приложений. С другой стороны, она напоминает удаленный доступ, поскольку клиентный компьютер (участвующий в удаленном соединении) является в некотором роде отдельной сетевой машиной. Он соединяется с сервером точно так же, как и локальный компьютер, только по телефонной линии, а не по сетевому кабелю.

Из всех трех типов удаленного доступа, я считаю этот метод самым простым. Установка и настройка системы удаленного доступа нередко вызывают затруднения, а дистанционное управление требует наличия свободной машины. В то же время тонкий клиент, установивший связь с многопользовательской версией Windows, сразу начинает работать, причем ему не нужна машина, ожидающая соединения с ним.

Конечно, недостатки есть и в этой системе. Во-первых, все это слишком дорого для случайного или эпизодического использования. Чтобы система работала, на сервере следует установить многопользовательскую версию Windows, а это стоит недешево. Машина, которая в состоянии поддерживать множество пользователей, должна иметь мощный про-

цессор и большую оперативную память, что также поднимает ее цену. Наконец, для каждого сеанса, организуемого на многопользовательской машине под управлением Windows, вам следует приобрести *отдельную* клиентную лицензию, а это в зависимости от необходимого числа лицензий существенно увеличивает расходы.

Во-вторых, не все протоколы обслуживания дисплея одинаковы. Например, терминальный сервер Windows (WTS - Windows Terminal Server) фирмы Microsoft поставляется вместе с протоколом удаленного дисплея (RDP - Remote Display Protocol). Он предназначен для загрузки изображений и приема вводимой пользователем информации во время сеанса. Однако протокол RDP работает лучше при локальном, а не удаленном входе в тонкую клиентную сеть. В принципе, он работает и во втором случае, однако регенерация изображения на экране выполняется замедленно. Более быстрый протокол, например, ICA (Internet Computing Architecture - вычислительная архитектура Internet), предоставляемый надстройкой Metaframe фирмы Citrix, отличается от него совсем немного.

Виртуальные частные сети

Общий недостаток всех описанных выше методов удаленного доступа заключается в использовании для организации соединения телефонных линий. Это значит следующее.

- Пакеты передаются по незащищенным сетям (подробнее о последствиях см. гл. 14).
- Если сервер и клиент удалены друг от друга на большое расстояние, то оплата телефонного соединения может быть значительной.
- Для каждого соединения необходима отдельная линия.

Единственный путь обойти эти проблемы — создать виртуальную частную сеть (VPN - virtual private network) внутри другой сети, скажем, Internet. Для пользователя это будет выглядеть аналогично соединению с главной сетью (host network) (рис. 6.4). Однако в данном случае соединение туннелируется через общедоступную сеть, т.е. проходит внутри нее, но в то же время автономно (в определенной степени, — Прим, ред.) от нее. Подробнее об этом далее, в разделе "Механизмы туннелирования".

Рис. 6.4. Клиент получает доступ к локальной сети фирмы через VPN

VPN-сети можно использовать для разных целей. Отдельные пользователи могут связываться с сетью организации и использовать удаленный доступ или дистанционное управление. Можно соединить целые сети, можно даже применить VPN для соединения с отдельной машиной, чтобы использовать в сети ее ресурсы, не включая в локальную сеть саму машину.

Примечание

В большинстве случаев VPN создают с помощью Internet. Это объясняется тем, что Internet - самая доступная сеть общего пользования. Поэтому я буду приводить её и в дальнейших примерах. Однако в качестве магистрали VPN в принципе можно использовать *любую* общедоступную сеть.

Поскольку виртуальные частные сети предназначены для организации доступа к частной локальной по общедоступным сетям, к сетям VPN предъявляют строгие требования с точки зрения безопасности.

- Поддержка идентификации пользователя, с тем чтобы личность пользователя можно было установить с помощью базы данных учетных записей. Кроме того, в целях защиты входы в сеть и доступ к файлам должны заноситься в файл журнала.
- Клиенты виртуальной сети должны иметь адрес, используемый в частной сети, и этот адрес должен быть ограничен частной сетью.
- С целью защиты информации должно поддерживаться шифрование данных. Кроме того, программное обеспечение VPN должно быть в состоянии генерировать и обновлять ключи шифрования.
- VPN должна поддерживать транспортные протоколы, используемые в общедоступных сетях.

Короче говоря, сети VPN представляют собой защищенное, недорогое и простое средство, открывающее множество маршрутов для доступа к сети, причем как одному пользователю, так и целым локальным сетям, расположенным в другом месте. Единственный недостаток VPN заключается в том, что ее трафик конкурирует с остальным трафиком в общедоступной сети.

Механизмы туннелирования

Как же все это работает? Вспомните: при удаленном соединении клиенты удаленного доступа и дистанционного управления используют соответствующий протокол линии связи, чаще всего — PPP. Помимо PPP, компьютеры VPN должны использовать еще один протокол для переноса данных частной сети по сети общедоступной. С этой целью используется технология *туннелирования.* При использовании этой технологии пакеты данной сети "укладываются" в пакеты другой. Это напоминает помещение почтового конверта в обертку из простой коричневой оберточной бумаги. "Обертка" отнюдь не предназначена для сокрытия информации: ее добавление фактически означает добавление маршрутной информации, которая необходима для отсылки исходного пакета по сети, в которой такие пакеты не поддерживаются. Когда пакет достигает места назначения, скажем, локальной сети организации, дополнительная информация "срывается" с заголовка пакета, и он предстает в исходном виде.

Зачем нужна такая инкапсуляция? Как указано в гл. 3, для передачи пакетов по сети необходимо использовать протокол, который поддерживается этой сетью. Туннелирование работает как средство "маскировки" пакетов. Например, при прохождении пакета по сети, поддерживающей протокол IP, пакеты IPX могут принять вид IP (точнее, PPP). Как только пакет покидает сеть IP и переходит в сеть, поддерживающую протокол IPX, пакет снимает маску IP и возвращает исходный формат. Для инкапсуляции и восстановления исходного формата пакетов как раз и предназначен протокол Туннелирования.

Протоколы туннелирования: настоящее и будущее

Технология Туннелирования известна давно. Так, она некоторое время применялась для создания туннелей в сетях IP с помощью протоколов TCP/IP и SNA (Systems Network Architecture — системная сетевая архитектура, служащего для связи персональных компьютеров с мэйнфреймами IBM) в операционной системе NetBIOS. Приведем несколько примеров более современных протоколов туннелирования.

- Протокол туннельной двухточечной связи (PPTP — Point-to-Point Tunneling Protocol).
- Протокол Туннелирования 2-го уровня L2TP (Layer 2 Tunneling Protocol).
- Режим защищенных туннелей IPSec (IP Security).

Работа протоколов Туннелирования на канальном и сетевом уровне несколько различается: В протоколах канального уровня предусматривается использование связи с логическим соединением. Это означает, что прежде чем выполнить Туннелирование, конечный узел должен дать согласие на создание туннеля, и задействовать совместимые средства шифрования, сжатия и прочие опции. Кроме того, возможности этих протоколов в значительной степени зависят от возможностей средств защиты, предоставляемых протоколом PPP или другим протоколом сетевого уровня. С другой стороны, протоколы туннелирования сетевого уровня не требуют обязательного создания туннеля до начала сеанса. Напротив, они предполагают, что все приготовления уже выполнены без их участия. В основном эти протоколы предназначены для шифрования и инкапсуляции пакетов, выполняемых за счет включения дополнительных заголовков. Поэтому все узлы VPN должны использовать единый протокол сетевого уровня.

Протокол PPTP. Этот протокол можно рассматривать как проект стандартного протокола канального уровня, используемого для Туннелирования пакетов по сетям поддерживающим IP-протокол, например, Internet. И хотя его можно использовать в любых сетях, поддерживающих протоколы NetBEUI, IPX/SPX (или совместимые), TCP/IP, он спроектирован для создания интерсетей именно с протоколом IP. Для передачи данных и управляющей информации во время сеанса (session control information) протокол предусматривает использование, двух каналов. Один из них предназначен для передачи данных, второй — информации управления сеансом. С этой целью используется протокол с логическим соединением — TCP, входящий в набор протоколов TCP/IP.

Протокол PPTP распространен достаточно широко. Главным образом он используется фирмой Microsoft, однако проект стандарта разработан фирмой Ascend Communications. Фактически же, реализация протокола, используемая Microsoft, несколько отличается от той, что предлагает рабочая группа инженеров Internet (IETF). Это объясняется тем, что фирма Microsoft усовершенствовала средства шифрования по сравнению с исходным стандартом.

Протокол L2TP. Несмотря на широчайшую поддержку, протокол PPTP постепенно вытесняется L2TP. Это скоростной протокол Туннелирования, в основе которого лежит PPTP. L2TP также относится к протоколам канального уровня. Он спроектирован для поддержки протоколов NetBEUI, IPX/SPX (и совместимых), а также TCP/IP и предназначен для использования во всех сетях, поддерживающих передачу дейтаграмм UDP (сеансы без установления логической связи), например, Frame Relay, ATM, X.25 или IP.

Как указано выше, протокол L2TP постепенно вытесняет PPTP с его позиций основного протокола. Почему? Во-первых, его поддерживает Microsoft. Современные операционные системы Windows не поддерживают этот протокол, однако в следующем поколе-

нии Windows NT поддержка предусмотрена. Даже без такой поддержки L2TP имеет потенциальные возможности стать более быстрым протоколом по сравнению с PPTP, поскольку он предусматривает одноканальные дейтаграммы UDP, а не двухканальные, используемые в PPTP. В принципах организации L2TP не предусмотрено установление логического канала связи, что уменьшает надежность протокола. Однако в настоящее время надежность имеет меньшее значение, поскольку (по крайней мере, в США), качество каналов связи значительно улучшилось и контроль ошибок уже не столь важен. Большое значение имеет преимущество пакетов UDP перед GRE, поскольку большинство брандмауэров поддерживают обработку пакетов UDP, а не GRE. Кроме того, L2TP более гибок по сравнению с PPTP, поскольку обеспечивает поддержку архитектуры большинства глобальных сетей, а не только Internet.

Примечание

На конец 1998 г. стандарт протокола L2TP все еще не был выпущен. На рассмотрение IETF представлен предварительный вариант стандарта, хотя окончательный стандарт пока еще разрабатывается. PPTP вообще никогда не описывался как законченный стандарт, так что его отсутствие не препятствует распространению L2TP.

Хотя L2TP и позволяет использовать встроенные функции защиты PPP, в нем предусмотрено взаимодействие с протоколом IPSec, а PPP используется только в том случае, если этот протокол сетевого уровня недоступен.

Протокол IPSec. В то время как протоколы L2TP и PPTP относятся к числу стандартных протоколов Microsoft, протокол IPSec относится к категории "прочее", Он представляет собой протокол сетевого уровня, определяющий процедуру шифрования пакетов IP и назначения новых заголовков, с помощью которых они отсылаются по сети IP. Весь процесс идентификации выполняется с помощью *сертификатов* (вложений) в передаваемые данные, идентифицирующих отправителя. Компьютер, инициирующий сеанс, отсылает сертификат по общедоступной сети в место назначения. Конечный узел принимает сертификат и подтверждает его идентичность собственному сертификату. Затем два компьютера используют свои открытые ключи (public keys) или секретные ключи (private keys) чтобы определить параметры (установки) сеанса, в том числе тип шифрования и сжатия, которые должны использоваться на протяжении всего сеанса.

Как указывалось выше, для обеспечения защиты в L2TP применяется (по умолчанию) протокол IPSec. Почему нельзя просто использовать IPSec и покончить с этим? Главным образом он необходим для поддержки удаленного доступа из различных мест. Природная форма (native form) протокола IPSec обеспечивает защиту только на уровне машины, но не на уровне пользователя. Обратите внимание: для взаимной идентификации машины на обоих концах соединения используют сертификаты, специфические для каждой машины. Обычно в различных реализациях IPSec используются соответствующие расширения (дополнения), позволяющие идентифицировать собственно пользователей, однако они не входят в стандарт.

Для защиты на уровне пользователя необходимо использовать один из протоколов Туннелирования канального уровня, позволяющих выполнить идентификацию на уровне пользователя, а затем применять алгоритм шифрования сетевого уровня. Если пользовательская база данных компьютеров вашей VPN статична, а сетевая операционная система (NOS — networking operating system) поддерживает IPSec, рекомендуем выбрать именно этот протокол.

Примечание

Если вам не совсем понятно, Что такое защита на уровне пользователя, и чем она отличается от других форм защиты, обратитесь к гл. 15.

Образец сеанса PPTP

Допустим, вы хотите начать сеанс в VPN с клиентом удаленного доступа. Сеанс тунелирования (tunneling session) между компьютерами VPN начинается следующим образом.

1. В процессе работы в соответствии с PPP используется протокол управления каналом (LCP) для инициализации сеанса связи между двумя узлами VPN. LCP отвечает за выбор режима связи, а также используемые коэффициенты сжатия, однако фактически на этом этапе он не используется.
2. Клиент (узел, инициирующий соединение) представляет серверу для идентификации свои "верительные грамоты". С этой целью используется один из нескольких протоколов идентификации — это делается для того, чтобы не дать третьей стороне выдать себя за клиента или перехватить пароль. Сервер либо идентифицирует доступ клиента, либо прерывает связь, если не может его идентифицировать. При желании сервер может прервать соединение и перезвонить клиенту по предварительно заданному номеру. Это удваивает гарантию, что вызывающая сторона — именно клиент сети.

Примечание

Протоколы идентификации паролей рассматриваются в гл. 14.

3. Клиентной машине назначается адрес, а также методы сжатия и шифрования данных, выбранные с помощью протокола LPC.

С этого момента связь установлена: клиент идентифицирован, все параметры сеанса выбраны и реализованы. Теперь можно без опасений начинать передачу данных.

Всегда ли использование сетей VPN предпочтительнее других методов удаленного доступа? Не обязательно. Конечно, сети VPN позволяют сэкономить деньги при передаче на дальние расстояния, однако имеют один недостаток: поскольку клиенты VPN используют в качестве среды передачи общедоступную сеть Internet наравне с множеством других пользователей, производительность сети может быть невелика. Да, ваш трафик останется тайным, но даже в своей коричневой оберточной бумаге он должен: конкурировать за полосу пропускания с трафиком остальных клиенток.

Сети с коммутацией пакетов

Как указано в разделе "Сравнение методов коммутации пакетов и коммутации каналов", глобальные сети работают не так как сети локальные. Здесь мы рассмотрим два примера реализации глобальной сети, основанные на методе коммутации пакетов.

X.25. Устаревшая технология, используемая для передачи данных по ненадежным (некачественным) сетям. Он все еще используется при работе на устаревших линиях связи.

Frame Relay. Более современная технология, предпочтительная при организации новых глобальных сетей, поскольку обеспечивает наиболее эффективное использование полосы пропускания.

Обе технологии работают во многом аналогично. Основное различие состоит в наличии дополнительной информации о контроле ошибок, включаемой в любой пакет X.25 что не предусмотрено в Frame Relay.

Стандарт X.25

X.25 представляет собой протокол доступа для сетей с коммутацией пакетов, в соответствии с которым устанавливается виртуальный канал между двумя, узлами сети. Его реализация выглядит примерно так: на сетевой плате установлено несколько физических портов, каждый из которых может поддерживать множество виртуальных каналов. Когда вы посылаете пакет, он следует к месту назначения по одному из этих каналов.

По современным стандартам протокол X.25 не слишком скоростной: скорость передачи составляет всего 64—256 Кбит/с. За пределами США этот тип глобальных сетей весьма популярен по двум причинам: в тех местах, где используется исключительно проводная связь, его можно использовать без каких бы то ни было ограничений. Кроме того, он весьма надежен, даже если сама линия связи надежностью не отличается. Поскольку связь в целом работает медленно, а, кроме того, протокол предназначен для сетей с коммутацией пакетов, он не позволяет передавать непрерывные данные, например, видеоинформацию. Однако он великолепно подходит для "пульсирующего" обмена, т.е. для передачи файлов, сообщений электронной почты и записей баз данных.

Вообще-то, стандарт X.25 описывает не тип сети, а метод прохождения пакетов данных в глобальных сетях с коммутацией пакетов, а также прохождение той информации, которая должна сопровождать данные, Протокол X.25 работает на трех нижних уровнях модели OSI.

- ***Физический* уровень.** X.25 предусматривает использование последовательного соединения (порта) RS-232. Поэтому все маршрутизаторы сети с протоколом X.25 должны поддерживать этот тип соединений.
- ***Канальный* уровень.** Данные, отсылаемые по глобальной сети, должны быть упакованы в кадры (frames) для обеспечения установки соединения.
- **Сетевой уровень.** Выполняется одновременная передача данных и кода контроля ошибок, что гарантирует их передачу до места назначения единым блоком. Если происходят ошибки, отправитель заново отсылает данные.

Для контроля ошибок в сетях X.25 используется информация CRC, которая включается в состав кадра. Когда кадр прибывает на другой конец сети X.25, выполняется тест CRC. Если результат проверки не совпадает с ответом, включенным в состав кадра, получатель просит отправителя повторно переслать данные. Если ответ правильный, получатель подтверждает, что данные поступили единым блоком. В любом случае до подтверждения о получении отправитель готов "отбросить" данные.

Другой аспект надежности протокола X.25 заключается в способности системы отслеживать ход сеанса. Во-первых, если виртуальный канал, внезапно прерывается и сеанс заканчивается, то можно зафиксировать статус сеанса на момент его окончания. Когда же виртуальный канал устанавливается вновь, сеанс можно продолжить с момента окончания, и отослать все пакеты, которые остались неотправленными после "обрыва" связи. Во-вторых, в протоколе X.25 предусмотрен механизм *управления потоком информации (flow*

control). Он гарантирует, что абонент *никогда* не получит пакетов больше, чем он в состоянии обработать одновременно. Если успешное получение кадра не подтверждается, отправитель прекращает отсылку кадров до тех пор, пока не получит какое-либо подтверждение. В некоторых случаях получатель действительно может отослать явное сообщение отправителю, предлагающее прекратить передачу до особого уведомления.

Такова X.25 — медленная, но надежная технология сетей с коммутацией пакетов. Если же качество линии связи лучше, предпочтительнее использовать технологию ретрансляции кадров. Первоначально предполагалось, что технология Frame Relay заменит на время технологию выделенных линий связи, пока не появится что-нибудь более совершенное. Однако в конечном итоге в новых глобальных сетях она стала самой популярной технологией доступа.

Улучшение использования полосы пропускания с помощью ретрансляции кадров

Ретрансляция кадров — наилучшая технология создания глобальных сетей. Почему именно ретрансляция кадров? Тому есть следующие причины.

- Ретрансляция кадров хорошо известна. Эта технология существует уже много лет.
- Такая технология пригодна для пульсирующей передачи данных именно того типа, который все еще используется в большинстве сетей, например, для передачи файлов.
- Высокая эффективность использования полосы пропускания.
- По сравнению с исходной реализацией скорость передачи в существующих версиях значительно повышена. Поэтому сети Frame Relay могут поддерживать потоки данных с высоким уровнем требований к качеству передачи.

Первоначально технология Frame Relay разрабатывалась как временное средство. Ее предполагалось использовать до завершения разработки жизнеспособной альтернативы выделенным линиям. *Выделенная линия* — это специальная частная линия связи для двухточечных соединений между компонентами глобальной сети (рис. 6.5). Каждому филиалу (B—E) необходима линия связи с сервером корпорации, расположенным в офисе A.

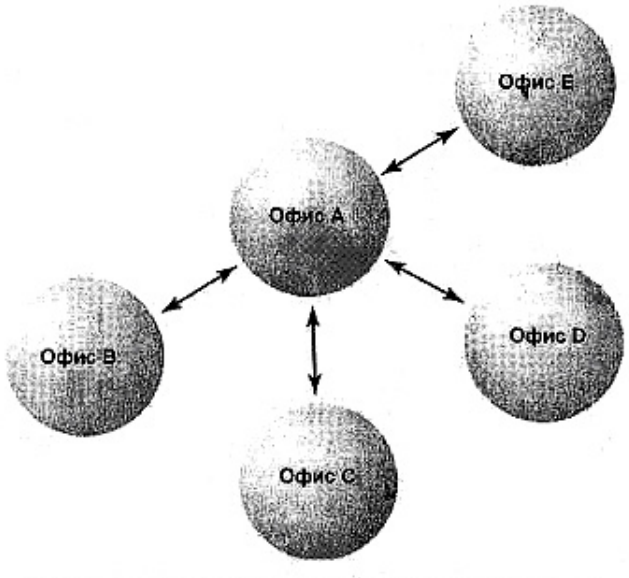


Рис. 6.5. Соединение офисов выделенными линиями

Выделенные линии обеспечивают великолепную связь, однако (и это их единственный недостаток) чрезвычайно дороги, и чем их больше и выше скорость работы, тем выше стоимость. К тому же эти дорогостоящие линии никогда не используются постоянно, так что вам придется оплачивать немалую часть бесполезной (незанятой) полосы пропускания. Более медленные линии связи дешевле, но в этом случае вас ждут проблемы с производительностью.

Территория Соединенных Штатов охвачена высокоскоростной проводной сетью. Почему бы не дать доступ людям к ее части совместно с прочими подписчиками, чтобы эффективнее использовать полосу пропускания? Именно в этом и состоит идея ретрансляции кадров — предоставить людям доступ к высокоскоростным линиям связи, позволяющим передавать данные с той же скоростью, что и по выделенным линиям. Однако они должны использовать их совместно, отсылая данные по виртуальным каналам, с тем чтобы два подписчика не мешали друг другу: Здесь нет физического двухточечного соединения, как в выделенных линиях, но; как показано на рис. 6.6, выглядит данное соединение точно так же. Фактически же, более эффективное использование полосы пропускания при ретрансляции кадров значительно повышает качество соединения в линиях с одинаковой пропускной способностью.

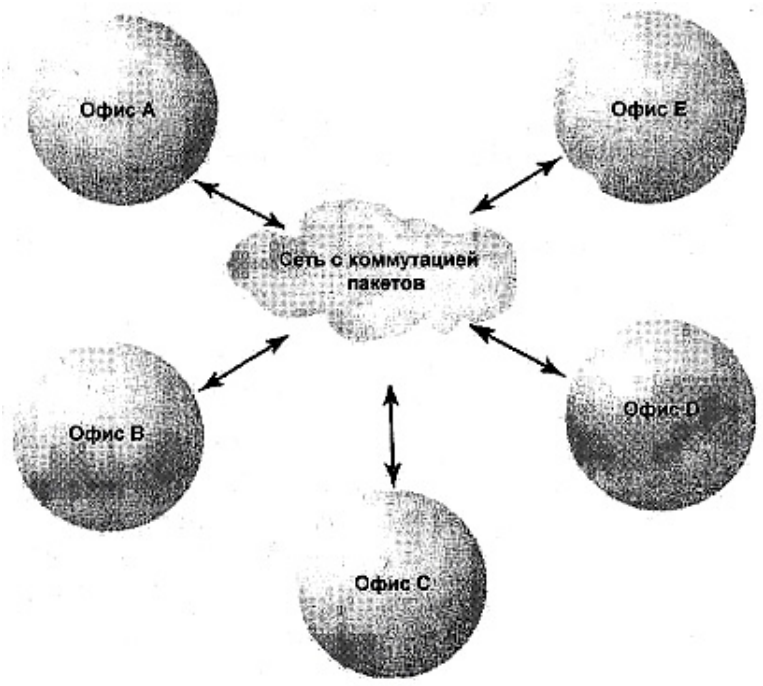


Рис. 6.6. Соединение офисов сетями Frame Relay

Благодаря более эффективному распределению полосы пропускания, сети с ретрансляцией кадров (frame relay networks) обеспечивают, по сравнению с выделенной линией, примерно двукратное ускорение передачи данных. Точное значение скорости зависит от фактической полосы пропускания канала. Чаще всего технология Frame Relay используется в линиях связи Т1 (1,55 Мбит/с) или 56К (56 Кбит/с), однако испытывалась она и на линиях Т3 (45 Мбит/с). Доступность услуг со скоростями Т3 — это вопрос из совершенно другой области, но сама технология существует.

Соперники Frame Relay

Ранее уже упоминалось, что технология ретрансляции кадров первоначально рассматривалась как переходная, временно применяемая взамен технологии выделенных линий. В качестве альтернативы предполагалось использовать службу коммутируемой мультимегабитной передачи данных (SMDS – Switched Multimegabit Data Service). Технология SMDS имела множество достоинств. Она была скоростной, допускала передачу данных до 45 Мбит/с, не требовала установки логического канала связи (чем достигалась большая гибкость сети) и хорошо приспособленной для передачи потоковых данных (streaming data). С другой стороны, технология Frame Relay допускала несколько меньшую скорость, предусматривала установку логического канала связи и более всего подходила для пульсирующей передачи (bursting transmission). В конце концов, даже средства речевой связи по сетям Frame Relay всё ещё разрабатываются.

Тем не менее, технология Frame Relay победила в сражении протоколов для глобальных сетей. И не потому, что имела лучшую архитектуру, а из-за низкой стоимости. Хотя SMDS не намного дороже, чем Frame Relay (если учесть доступную полосу пропускания), однако SMDS намного дороже в абсолютном выражении. Многие полагают, что высокая скорость соединения в глобальных сетях не стоит потраченных денег, поэтому ретрансляция кадров победила по определению.

Внутри облака

Технология Frame Relay предусматривает распределение полосы пропускания сети с помощью *статистического мультиплексирования* (statistical multiplexing). В этом случае полоса пропускания распределяется между пакетами, а не между пользователями. Различие заключается в следующем: если один канал разделяется на несколько виртуальных, то каждый из них занимает часть полосы пропускания, независимо от того, используется он, или нет. В большинстве случаев данные передаются по сети короткими пакетами, что делает использование значительной части полосы пропускания неэффективным (рис. 6.7).

Если же вместо разделения канала распределить полосу пропускания соответственно сетевому трафику, то получатель, которому необходима широкая полоса пропускания, получит ее. Кроме того, пользователи, которым не требуется широкая полоса, заполучить ее. не смогут (рис. 6.8).

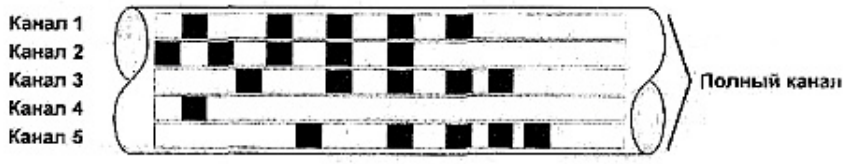


Рис. 6.7. Распределение полосы пропускания по каналам

Рис. 6.8. Распределение полосы пропускания по пакетам

Если кадры всех подписчиков перемешаются в одной и той же сети с коммутацией пакетов, как же их рассортировать для отправки? Каждый кадр фиксируется согласно идентификатору соединения канала передачи данных (DLCI - Data Link Connection Identifier). Идентификаторы DLCI работают как "погрузочная платформа", поскольку кадры направляются не по назначенному адресу, а в место, указанное DLCI. Когда кадр туда поступает, телефонная станция (telco box), соединяющая подписчика с сетью, исследует содержимое DLCI и определяет, соответствует ли DLCI адресу, который доступен подписчику. Если адрес доступен, пакет пересылается по конечному назначению. Если же кадр попал сюда по ошибке, он отбрасывается.

Управление перегрузкой сети

Как видите, ретрансляция кадров позволяет более эффективно использовать полосу пропускания, чем разделение физического канала на множество логических. Однако переполнение канала данными имеет свои недостатки. Именно поэтому, когда сеть одновременно использует множество подписчиков, работа замедляется. Провайдеры Frame Relay предлагают линии с согласованной скоростью передачи информации (CIR — Committed Information Rate), представляющую собой среднюю пропускную способность. Вы можете, например, получить соединение с CIR, равной 50 Кбит/с, но фактически работать со скоростью 100 Кбит/с. Однако провайдер гарантирует, что ваша скорость передачи никогда не упадет ниже 50 Кбит/с. Кадры, скорость передачи которых ниже этой величины, фиксируются, и вам сообщается, что они выходят за гарантированную пропускную способность канала. При перегрузке линии, отмеченные кадры отбрасываются в первую, очередь.

Фактическое значение предлагаемой CIR зависит от качества обслуживания. В принципе, провайдер может предложить значение CIR, равное 0, что означает отсутствие любых гарантий. Это, однако, маловероятно. Как правило, чем меньше значение CIR, тем дешевле связь, но это уменьшает эффективную пропускную способность.

Выводы

Применяемые в настоящее время типы архитектуры глобальных сетей, в основном, реализуются не на базе двухточечных соединений, а на общедоступных, сетях — с коммутацией пакетов, в которых выполняется маршрутизация данных к месту назначения по виртуальным каналам, Наибольшее применение в современных глобальных сетях (WAN) нашла технология ретрансляции кадров (Frame Relay). Вероятно, на втором месте стоят частные сети (VPN), которые имеют меньшие скорости передачи, но могут работать на больших расстояниях. Здесь не был приведен полный обзор всех типов глобальных сетей. Рассмотрены были только наиболее известные и те, с которыми, вероятно, вам придется работать.

На этом мы завершаем обсуждение каналов локальных сетей (а также внешних каналов). В ч. 2 ("Детали головоломки"), мы перейдем к описанию программного обеспечения (операционных систем и приложений серверов) •и вдохнем жизнь в вашу локальную сеть. Кроме того, мы рассмотрим "объекты" (серверы и серверные компьютеры), которые, собственно говоря, и образуют эту сеть.

Упражнение 6

1. При каких обстоятельствах использование протокола X.25 предпочтительнее ретрансляции кадров?
2. В офисе установлен компьютер Pentium 200 с оперативной памятью 64 Мбайт. Дома у вас компьютер 386 с памятью 8 Мбайт. Предположим, у вас есть все необходимое оборудование и программное обеспечение. Какой тип удаленного доступа вы можете использовать для связи с вашим офисом, чтобы запускать дома те же приложения, что и в офисе? Укажите все, что пригодно для этой цели.

   A. Удаленный доступ.
   B. Дистанционное управление.
   C. Тонкий клиент.
   D. Виртуальная частная сеть.

3. Какой протокол используют для поддержки виртуальной частной сети и сети с ретрансляцией кадров?
4. Какова согласованная скорость передачи информации (CIR) для соединения с ретрансляцией кадров на скорости 56 Кбит/с?

ЧАСТЬ II
Детали головоломки

Глава 7

Общие сведения О глобальных сетях

В предыдущих главах было затрачено немало времени на рассмотрение различных методов, которые можно использовать для соединения друг с другом сетевых компьютеров. Кроме того, были описаны различные средства, необходимые для создания сети: кабели, протоколы, сетевое оборудование и т.п. Теперь поговорим о роли компьютеров в сети. Какая конфигурация компьютеров оптимальна для их работы в сети? И какие еще устройства, помимо компьютеров, должны входить в состав сети? В этой и последующих главах ч. II "Детали головоломки" я расскажу о различных типах клиентных и серверных машин, а также о периферийных устройствах, которые следует использовать в сети.

Что такое сервер

Сервером называют любой сетевой компьютер, обслуживающий другие сетевые компьютеры. Обслуживание может заключаться в решении одной или двух задач, таких как хранение файлов, печать или совместное использование приложений. Однако для описания сервера большее значение имеет не тип предоставляемых услуг, а расстановка акцентов в той роли, которую он играет.

Примечание

Как указано в гл. 10, для решения возлагаемых на сервер задач необязательно даже выделять отдельный компьютер. В одноранговых сетях такие компьютеры должны играть роль и клиентной машины, *и* сервера.

Тип сервера зависит от выполняемых им функций в сети. Однако основные компоненты всех серверов одинаковы — диски, память, CD-ROM и т.д.

По определению, сервер должен работать не только на себя, но также и на остальные сетевые компьютеры. По этой причине в серверах необходимо использовать самые быстродействующие и высококачественные компоненты. То, что приемлемо для работы отдельного клиента, может работать с совершенно неудовлетворительной скоростью при обслуживании запросов от 60 пользователей. Остановимся подробнее на понятиях скорость и мощность.

Выбор компонентов сервера

Если вы интересуетесь развитием оборудования, вам должно быть известно, что новое оборудование намного более совершенно, чем прежнее и устаревает очень быстро. Поэтому не стоит сегодня приобретать новейшие и самые быстродействующие компоненты, поскольку через шесть месяцев они устареют. Если вы захотите приобрести самые быстрые микросхемы/диски/память/CD-ROM, то вы не купите *ничего*. Хорошим стимулом дожидаться выпуска более скоростных компонентов является то, что после него цены на предыдущие образцы немедленно падают.

Вместо ожидания появления «Наилучшего Сервера», приглядитесь к уже опробованным компонентам компьютеров, которые пригодны для ваших *сегодняшних* нужд, и убедитесь, что в последствии их можно будет обновить. Когда придёт время (если оно придёт) и когда компоненты, закупленные в 1999 г, уже не будут способны обслуживать вашу сеть, вы сможете заменить их. А сами тем временем не сходите с ума, стараясь устанавливать в вашу сеть любое, только что выпущенное оборудование. Эта задача не разрешимая.

Между прочим, полного руководства по всем компонентам, представленным на рынке, просто не существует. Например, за время подготовки к печати этой книги одна только фирма Intel выпустила шесть новых типов процессоров. (Вообще-то, это преувеличение, но вы поняли суть). Однако, зная то, что здесь написано, вы будете в состоянии оценить новые изделия, даже если они поступят в продажу после выхода книги.

Процессоры

Поскольку вы знаете компьютеры достаточно хорошо, по крайней мере, в той части, что касается сетей, то вам, должно быть, известно, что *процессор* представляет собой "мозг" компьютера. Он управляет всей работой компьютера, начиная с обработки запросов на считывание данных с жесткого диска и вплоть до их перемещения из памяти в буфер обмена для выполнения расчетов, например, электронной таблицы. Если процессор неработоспособен, то компьютер становится "безмозглым", вроде человека, у которого вынули мозг. При этом вы можете подавать на компьютер электропитание, но он все равно ничего не будет делать.

Процессоры CISC и RISC

Одно из фундаментальных различий между процессорами разного типа находится на самом нижнем уровне: оно заключается в методе обработки процессором команд. В этом отношении процессоры можно разделить на два типа: с полным набором команд (CISC) и с ограниченным набором (RISC). Разница между ними видна уже из названий.

Чем различаются алгоритмы?

В микросхемах CISC множество низкоуровневых команд объединяют и одну для создания одного программного модуля, встроенного в управляющую логику микросхемы. Напротив, управляющая логика микросхем RISC функционирует на уровне отдельных команд. Благодаря различиям в конструкции, в микросхемах CISC обычно используется более обширная система Команд (набор команд, встроенных в логическое устройство микросхемы), чем в RISC. Именно поэтому при решении поставленной задачи в CISC каждая команда работает сама по себе, а в RISC можно комбинировать и подгонять различные команды для достижения требуемого результата. В некотором смысле это похоже на разницу между латинским алфавитом (позволяющим с помощью 26 букв написать любое слово на данном языке, хотя каждая буква мало что значит, пока не соединена с остальными буквами) и тысячами китайских иероглифов, каждый из которых представляет собой отдельное слово.

Что такое система команд

Система команд (instruction set) – это набор инструкций, встроенных в микросхему. На заре появления компьютеров системы команд жёстко «зашивались» в процессор. Поскольку такие процессоры не тратили время на интерпретацию команд, они работали чрезвычайно быстро. Но в то же время замена программы требовала внесения изменений в структуру процессора (и наоборот). Чтобы несколько повысить гибкость системы, разработчики компьютеров создали язык программирования, встроенный в управляющую логику процессора, который позволял выполнять те же действия, что и при подаче жёстко встроенных команд и назвали его *микрокодом*.

Но даже если оставить в стороне гибкость, применение микрокода давало множество преимуществ над жёстко встроенными командами. Во-первых, программы, работающие с микрокодом, могли быть короче применявшихся ранее команд, поскольку могли вызывать более сложные функции, встроенные непосредственно в процессор. Во-вторых, более короткие программы предъявляли меньшие требования к объёму оперативной памяти, что было весьма кстати из-за её дороговизны.

Тем не менее, по мере усложнения системы команд стали возникать проблемы. Не все команды требуют одинакового времени на своё исполнение: понятно, что чем сложнее команда, тем больше времени занимает её исполнение. Поэтому когда ситуация чрезвычайно усложнилась, некоторые производители микросхем попробовали иной подход: размер каждой команды был сделан таким, чтобы она могла быть выполнена за один цикл тактового генератора. По существу, это напоминало модульный подход к вычислениям. Новый образец микросхемы получил название RISC. Именно тогда микрокод стали называть CISC-кодом. Однако и поныне CISC-код «жив и здоров». Новый подход отнюдь не отменил полностью старый.

Насколько изменилась со временем система команд? Очень мало. У современных процессоров Pentium она во многом сходна с той, что использована в микросхемах 386 (поэтому оба процессора входят в «семейство x86») с дополнительными командами, улучшающими обработку видео информации с помощью средств MMX. В настоящее время функции MMX включены в базовую систему команд Intel

Говоря проще, там, где микросхема CISC выполняет одну сложную задачу, RISC выполняет пять очень простых задач, но, в конце концов, обе микросхемы доведут до конца

одно и то же дело. Запутались? Приведем пример. Если вы используете микросхемы CISC и RISC и хотите, чтобы каждая накрыла обеденный стол, вы должны отдавать им приказы различным способом. Микросхеме CISC достаточно приказать: "Накрой стол", — и этого довольно. Так происходит потому, что в поднабор команд Set Table (Накрыть стол) входят все компоненты, необходимые для накрытия стола - так запрограммирована микросхема. Однако эта же команда собьет с толку микросхему RISC — приказ накрыть стол для нее ничего не значит. Вместо этого вы должны приказать ей: "Поставь на стол тарелки! Разложи столовое серебро! Положи на стол салфетки!" и т.д. В конечном счете, оба процессора выполнят задачу с тем же конечным результатом, однако придут к этому разным путем.

Почему используют два подхода? Они отражают разные методы разработки схем. Вплоть до середины восьмидесятых годов, в новых моделях процессоров использовали только структуру CISC. По мере роста вычислительной мощности микросхем их конструкция быстро усложнялась. Это было обусловлено тем, что в управляющую логику процессора встраивалось все большее число команд, так что в микросхему приходилось добавлять все большее число транзисторов. Конструкторы микросхем RISC пришли к выводу, что упрощенные команды будут быстрее исполняться *и* будут не так сложны, как команды в CISC. Это объясняется тем, что для повышения "интеллекта" микросхемы RISC достаточно всего нескольких дополнительных команд. Поэтому такие микросхемы должны быть дешевле.

Вечный вопрос - что лучше?

Какой подход лучше? Ответ зависит от конкретных условий. Технология RISC не всегда подходит для применения в тех случаях, когда набор задач ограничен. Например, для сетевого оборудования встроенные вычислительные средства RISC, как правило, не подходят, поскольку большинство ситуаций, в которых вы можете оказаться, можно предвидеть, а использование для их решения множества небольших команд замедляет работу устройства. Технология CISC предпочтительна при решении большинства задач, так или иначе относящихся к серверам (например, совместное использование файлов и принтеров), поскольку требования к процессорам в данном случае легко предвидеть. С другой стороны, технология RISC предпочтительна в "непредсказуемых" случаях, например, при обслуживании баз данных и приложений.

Примечание

Микросхемы RISC используются во многих компонентах сетевого оборудования, и том числе и терминалах Windows, рассматриваемых в гл. 12.

Иногда выбор типа процессора зависит от используемой технологии Для "перемалывания" чисел годятся оба подхода. Однако программное обеспечение разрабатывается для преобразования программ в машинные команды только одного типа, но никогда — двух. Поэтому весьма вероятно, что вам придется выбирать тип микросхемы, ориентируясь на используемый тип программного обеспечения, которое иногда может быть представлено версиями как для RISC-, так и CISC-процессоров. Например, вы можете приобрести Windows NT, и установить его на сервере с процессором DEC Alpha (микросхема RISC) либо Intel Pentium Pro (микросхема CISC). Однако на каждой машине будут установлены операционные системы разного типа. Невозможно просто скопировать уже установленные файлы с одной машины на другую, даже если в остальном отношении оборудование серверов идентично.

Примечание

Существует программное обеспечение, эмулирующее работу приложений RISC на машинах CISC (и наоборот). Однако Производительность приложений при этом заметно снижается.

Вообще, на работу с процессорами RISC рассчитаны операционные системы UNIX и Macintosh. Операционные системы персональных компьютеров, в частности, Windows 9x, рассчитаны на работу с микросхемами CISC. В ранних версиях операционной системы Windows NT, помимо работы с процессорами x86 (CISC), предусматривалась поддержка процессоров RISC. Однако в связи с ограниченным спросом на микросхемы RISC в операционной системе Windows NT 4 поддержка микросхем Power PC и MIPS в настоящее время не предусмотрена. Сегодня в этой системе поддерживается единственная микросхема RISC — процессор Alpha, разработанный фирмой Digital Equipment Corp (ныне входит в Compaq). Другими словами, если вы хотите использовать машины Macintosh, то должны установить в них RISC-процессоры. Если же вам необходимо использовать одну из версий Windows, желательно установить в машинах CISC-процессоры.

Определение скорости работы процессора

Как уже упоминалось ранее в этой главе, выбор процессоров (RISC или CISC) для компьютера не во всем зависит от вас. Я советую выбирать процессор в зависимости от приложения, вместо того чтобы подбирать приложение под процессор. В любом случае, вы должны представлять, с какой скоростью процессор выполняет поступающие команды. Скорость работы процессора определяет следующее.

- Число рабочих циклов, выполняемых за секунду. Количество одновременно обрабатываемых команд.
- Количество команд, одновременно передаваемых в процессор для обработки.
- Размер буфера, в котором сохраняются последние команды для повторного использования.

Примечание

Вплоть до появления процессора Intel 486 на скорость работы также влияло и наличие математического сопроцессора. Однако в настоящее время математический сопроцессор - стандартная часть процессора. Он позволяет процессору напрямую выполнять сложные математические операции, например, умножение, вместо того чтобы интерпретировать их как многократное сложение. Эти операции можно выполнить и без сопроцессора, но это займет больше времени: между операциями 5x6 и 6+6+6+6+6 есть разница.

Тактовая частота

Основная характеристика, которая дает грубое представление о скорости работы процессора — тактовая частота. "Грубое", поскольку это число описывает единственный аспект производительности: число циклов тактового генератора в секунду, но оно ничего не говорит о количестве команд, выполняемых за один цикл. (Позвольте уточнить: это справедливо, если только речь не идет о процессорах RISC — в этом случае соотношение равно 1:1. Однако вы по-прежнему не знаете, сколько команд необходимо для выполнения одной конкретной операции.) Тем не менее, при прочих равных условиях, чем выше частота тактового генератора, тем быстрее работает микросхема. Когда писалась эта книга, самые быстрые микросхемы CISC работали с внутренней частотой 400 МГц.

Удвоение частоты

Выше приведён термин *«внутренняя частота»* по отношению к числу 400 МГц. Следует учесть, что тактовая частота системной шины на материнской плате не превышает 60-66 МГц. На практике это означает, что тактовая частота оборудования (включая контроллер для обмена данными с оперативной памятью) не превышает 66 МГц (в новейших платах – 100 МГц). В то же время *внутренние* операции, такие как вычисления и переходы, выполняются с тактовой частотой 400 МГц. Это различие стало возможным благодаря применению технологии, называемой *удвоением частоты*, появившейся в середине 90-х гг. и применяемой поныне (она используется «подпольно»).

В основе удвоения частоты лежат конструкторские проблемы, затрудняющие разработку системной платы, работающей на частоте, превышающей 66 МГц: системные шины не могут работать на больших частотах. Однако на внутренней работе процессора это ограниче7ние никак не сказывается – процессор может работать на частотах, многократно превосходящих пределы 60 или 66 МГц.

Таким образом, процессор 486 на 33 МГц, которым я всё ещё пользуюсь (как видите, для решения моих задач такой медленный процессор вполне подходит), работает с той же частотой, что и системная плата. А вот различие скоростей работы процессора Pentium Pro на 200 Мгц и его системной платы разительно: системная плата работает на частоте 66 МГц, т.е. втрое медленнее. (Конечно, 66x3 не равно 200, но такое округление нравится продавцам.)

Является ли проблемой несоразмерность внутренней тактовой частоты процессора и внешней частоты шины? Не обязательно. Да, оперативная память не может «разговаривать» с процессором с той же скоростью, с которой процессор «разговаривает» сам с собой. Но это означает только то, что при выполнении внутренних расчётов производительность машины выше, чем при «общении» с периферийными устройствами. Удвоение частоты – относительно недавно появившаяся возможность, но её наличие весьма желательно.

Длина слова

Еще один фактор, определяющий скорость работы процессора — *длина слова,* или количество данных, которое процессор может обрабатывать одновременно. Чем больше длина слова, тем больше данных обрабатывается одновременно и, следовательно, тем быстрее работает машина. (Люди тоже используют слова разной длины.) Например, при поездке по запутанному маршруту без письменных инструкций, вы можете запомнить "в уме" два поворота и светофор. Затем придется остановиться, и попросить кого-нибудь указать остальной путь. В данном случае ваша "длина слова" недостаточно велика, чтобы обработать все множество данных одновременно.

Шина данных

Длина слова определяет, с каким количеством данных процессор может работать одновременно. Но как быстро эти данные могут поступить в процессор для обработки? Ответ на этот вопрос дает разрядность (size) *шины данных* процессора (data path). Образно говоря, шина данных представляет собой "ворота" в процессор. Чем шире шина данных, тем больше данных может поступить в процессор за единицу времени. Размер шины данных не обязательно совпадает с длиной слова. Воспользуемся прежним примером: в про-

цессоре 386SX используется шина данных шириной 16 бит и слово данных длиной в 32 бит. Хотя процессор и в состоянии обрабатывать 32 бит данных, одновременно в него могут поступить только 16. Кроме того, следующие 16 бит поступают в процессор с небольшой задержкой. Поэтому процессор 386DX с шиной данных шириной в 32 бит работает намного быстрее, поскольку слово данных может поступать в него целиком.

Кэширование

До сих пор мы обсуждали скорость, с которой процессор может "думать". Однако сколько данных он может "обдумывать" одновременно, и как быстро может переходить к "обдумыванию" чего-либо другого? Последняя деталь головоломки заключается в том, сколько недавно обработанных данных он может помнить. Это определяется объемом кэш-памяти (кэша).

Вероятно, в общих чертах вы знакомы с концепцией кэширования. Во многих частях компьютера информация, которая, вероятно, вскоре будет использоваться повторно, хранится в буфере, называемом *кэшем.* Точно также кэш имеется и в процессоре. Фактически, в процессорах используются два кэша. В старых процессорах использовался единственный внутренний кэш, называемый кэшем L1. Современные процессоры имеют как внутренний кэш L1, так и *внешний* кэш большего объема, который представляет собой статическое ОЗУ (статическое RAM (SRAM)). Внешний кэш называют кэшем L2. В обоих хранится информация (как коды, так и данные), только что использовавшаяся процессором. Идея заключается в том, что эта информация возможно вскоре опять понадобится процессору (рис. 7.1).

Рис. 7.1. Кэш L1 и L2

Примечание

SRAM представляет собой память, в которой запоминается все от момента, когда данные поступают в память, вплоть до их удаления (либо отключения машины). В отличие от динамической памяти (DRAM), на которой в основном и построена системная память, содержи-

мое SRAM не требуется регенерировать каждые 4 мс, поэтому она работает намного быстрее DRAM. Кроме того, она стоит дороже.

Поскольку кэш L1 встроен в процессор (и, стало быть, работает с той же скоростью, что и процессор), он работает быстрее кэша L2. Поэтому последние использовавшиеся данные сначала сохраняются в L1. (Быстродействие SRAM достаточно велико, однако меньше внутреннего быстродействия процессора.) В то же время внутренний кэш невелик по объему (8—64 Кбайт в зависимости от модификации процессора), поэтому, когда его емкость исчерпывается, дополнительные данные поступают в. кэш L2. Объем L2. намного больше — в некоторых случаях он достигает 1 Мбайт.

Примечание

Кэш L2 процессора Pentium Pro только наполовину можно назвать внутренним: он помещен в одном корпусе с процессором, но в дополнительном модуле, а не на одной, подложке с процессором.

Большая тактовая частота не обязательно означает больший объем кэша. Например, процессор Pentium Pro работает с внутренней тактовой частотой 200 МГц, однако имеет только кэш L1 объемом 8 Кбайт. В процессорах Celeron (266 и 300 МГц) кэш L2 не предусмотрен вообще. Поскольку для производительности процессора в целом наличие средств кэширования важнее тактовой частоты, на это следует обращать внимание. Так, если вы покупаете сервер с процессором конкретного типа, выбирайте тот, в котором предусмотрен достаточно емкий внутренний кэш, а также большой внешний.

Объединение процессоров

Сегодня мультипроцессорные системы стали жизненно, важны не только для компаний из списка "Fortune 500", но также для организаций куда меньшего размера. Мультипроцессорные системы полезны потому, что позволяют соединить в одной машине мощность (производительность) нескольких процессоров.

Примечание

Работа с мультипроцессорными системами поддерживаются не во всех операционных системах, однако в современных сетевых операционных системах такая поддержка предусмотрена. Таким образом, при желании, вы можете использовать их в своих серверах. Чтобы определить число поддерживаемых процессоров, просмотрите документацию на операционную систему. Например, Windows NT Server поддерживает четыре процессора.

Имеются две концепции поддержки мультипроцессорной обработки: симметричная мультипроцессорная обработка (SMP — Symmetric Multiprocessing) и несимметричная (AMP — Asymmetric Multiprocessor): Различие между ними понятно из названия. В системах SMP обработка сравнительно равномерно распределяется между всеми доступными процессорами, а новые задания обычно передаются наименее занятому процессору. В системах AMP один из процессоров обычно выделяется одному "семейству" программного обеспечения (например, операционной системе) для монопольного использования. Другие программы "конкурируют" за использование остальных процессоров, даже если процессор, операционной системы свободен.

Как и ранее, ваш выбор определяется в основном не пожеланиями, а характером программного обеспечения. Поскольку же чаще поддерживается
симметричная мультипроцессорная обработка (SMP), рекомендуем применять машины, реализующие этот алгоритм.

Насколько влияет быстродействие процессора на производительность сервера

Хороший вопрос. Конечно, скорость (быстродействие) процессора важна, однако производительность сетевого сервера зависит не только от нее. Действительно, в работающем сервере клиентам доступна *вся* машина, а не только процессор. Соответственно, скорость работы сервера с быстрым процессором, но медленными периферийными устройствами, невелика.

Таким образом, если вы прицениваетесь к серверу и подыскиваете нужные компоненты, уделите внимание не только процессору, но и остальным компонентам. Как вы увидите далее, сервер состоит из множества компонентов, а не только из одного процессора.

Типы шин

Некоторые основные вопросы устройства шин рассмотрены в гл. 1, где обсуждались сетевые платы, составляющие основу сетей. На практике в современных серверах используют шины двух типов: ISA и PCI.

Возможно, вы припомните, что ISA (Industry standart architecture — стандартная промышленная архитектура) представляет собой 8- или 16-битовую шину, работающую на частоте 8 МГц. Эта частота — предельно возможная рабочая частота исходной шины AT, на основе которой разработана шина ISA. ISA мало изменилась с 1984 г., когда она (главным образом по соображениям совместимости) была расширена до 16 бит. Слоты ISA-шины показаны на рис. 7.2.

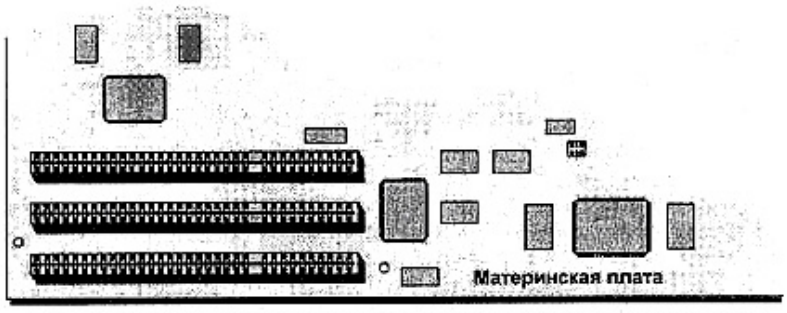
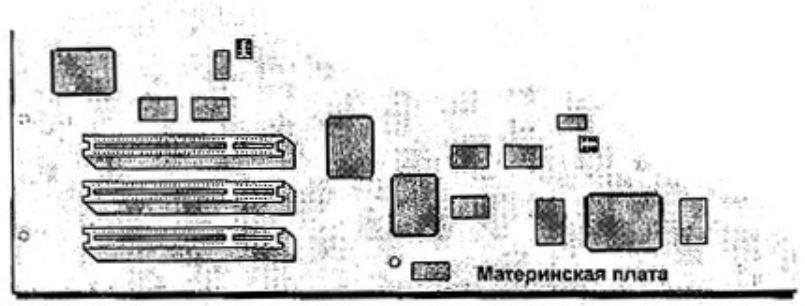


Рис. 7.2. Слоты ISA все еще можно встретить на большинстве материнских плат

Шина PCI (Peripheral Component Interconnect — интерфейс периферийных устройств) имеет архитектуру локальной шины (local-bus architecture). В ней развиты и использованы некоторые полезные идеи, реализованные в стандарте локальных шин VESA (Video Electronics Standard Association — Ассоциация по стандартам в области видеоэлектроники). Однако в архитектуре шины PCI устранены некоторые недостатки, присущие шинам VESA, а именно: отсутствие поддержки средств Plug-and-Play, сложности "в общении" с процессорами Pentium, затруднения в организации высокоскоростного соединения с системной платой при установке более двух слотов VESA. Технология локальных шин допускает работу на тактовой частоте системной шины материнской платы. Иначе говоря, если тактовая частота системной шины материнской платы составляет 33 МГц, то уста-

новленная в этот слот плата может работать с этой же частотой, а не "ползти" на 8 МГц. Слоты PCI показаны на рис. 7.3.



Слоты PCI (обычно белого цвета) используют для установки высокоскоростных плат, которые могут работать с тактовой частотой системной шины материнской платы

Рис. 7.3. Слоты PCI используют для установки высокоскоростных плат, которые могут работать с тактовой частотой системной шины материнской платы

Примечание

Технология локальной шины (local bus technology) первоначально развивалась как средство для повышения производительности при обработке видеоизображений, однако разработчики быстро обнаружили, что она пригодна для установки и остальных периферийных устройств.

Если PCI намного быстрее ISA, то почему же шина ISA все еще используется? Как и 10 лет назад, основная причина - совместимость. Никто не смеет заявить: "Эта плата работает невыносимо медленно. Давайте выбросим её и прекратим использовать платы ISA". Такой человек станет всеобщим посмешищем. Во-вторых, хотя в серверных системах ISA-шина работает несколько медленнее, она прекрасно подходит для клиентных машин. Кроме того, платы ISA дешевле плат PCI. В-третьих, шины PCI отнюдь не столь, универсальны. Так, для обслуживания последовательных и параллельных портов должны использоваться только шины ISA, но не PCI.

Повышение быстродействия шин

В конце 1998 г. PCI-шина была самой быстродействующей из всех имеющихся шин. Однако разработка новых шин продолжается. В 1999 г. ожидается выпуск (фирмой Intel) шин PCI с разрядностью 64 бит и тактовой частотой 66 МГц. Если и этого окажется недостаточно, фирмами Hewlett-Packard, IBM и Compaq разработана расширенная шина PCI, получившая название PCI-X. Новая шина спроектирована для работы с тактовой частотой 133 МГц и может обеспечить передачу данных между процессором и периферийными устройствами со скоростью 1 Гбит/с.

PCI-X – только временный заменитель улучшенной PCI-шины, применяемый до тех пор, пока его не сменит что-либо более совершенное. В 2000 г. ожидается появление соединений между периферийными устройствами и материнской платой, реализованных на базе фабрики (fabric-based connections). Вместо подключения к шине периферийные устройства будут использовать высокоскоростные линии связи для подключения к подсистемам, микросхемам и даже друг с другом. Такой метод подключения уже применяется в мэйнфреймах и суперкомпьютерах, но только сейчас реализован в персональных компьютерах.

Если периферийное устройство поддерживает PCI-шину, рекомендуем и вам использовать эту шину. Она используется достаточно давно, поэтому для нее можно без труда найти любые платы. Однако нередко применение плат ISA в клиентных машинах вызывает меньше затруднений. С другой стороны, для серверов, к быстродействию

ет меньше затруднений. С другой стороны, для серверов, к быстродействию которых предъявляют повышенные требования, необходима более быстродействующая шина. По этим причинам в большинстве современных персональных компьютеров предусмотрены слоты как PCI, так и ISA.

Заброшенный, но не забытые MCA и EISA

Как указывалось выше, шины ISA работают намного медленнее материнских плат. Почему же замена 16-разрядной шины ISA на более совершенную PCI заняла 10 лет? Да просто потому, что шины других типов работали неудовлетворительно.

С появлением 386-х машин фирма IBM выпустила более скоростную шину MCA (MicroChannel Architecture – микроканальная архитектура). Эта шина имела несколько преимуществ перед ISA, разрядность – 32 бита, тактовая частота – 10 МГц, поддержка управления шиной и – особо отметим – поддержка технологии Plug-and-Play. Конечно, MCA имела и недостатки. Во-первых, она не поддерживала платы ISA – фирма IBM создала шину MCA, как уникальное изделие. Такая несовместимость возникла как побочный результат ускорения шины. Возможно, это сыграло меньшую роль, чем несовместимость шин PCI и ISA, однако IBM усугубила ошибку, предложив производителям плат приобретать лицензию на право производства плат MCA (IBM не собиралась отдавать это право даром), а затем платить процент с прибыли.

IBM получила единодушный ответ: «Идите к чёрту». Группа из девяти производителей материнских плат (известная под названием «Банда девяти») начала разрабатывать собственную шину с достоинствами шины MCA, но не создающую проблем с лицензированием. Именно так была создана шина EISA (Extended Industry Standart Architecture – расширенная промышленная стандартная архитектура). В ней предусматривалась 32-битовая шина данных (data path), поддерживалось управление шиной (bus mastering) и технология Plug-and-Play, а с целью обеспечения совместимости с ISA, шина работала на частоте 8 МГц.

Однако обе шины были не слишком хороши. MCA страдала от недостатка плат, создаваемых для работы с ней, а EISA-платы никогда не поступали в широкую продажу, хотя они и получили определённое признание в серверных машинах. Людям было проще найти нужную плату ISA – вполне работоспособную – и работать с тем, что хорошо им известно, ожидая появления чего-нибудь лучшего.

Оперативная память

Общим принципом при выборе размеров оперативной памяти является такой: вы никогда не сможете установить ОЗУ слишком большого размера.

ОЗУ или RAM (Random Access Memory — память с произвольным доступом) — платформа для большинства компьютерных операций. Все коды и данные, используемые в настоящий момент, сохраняются в ОЗУ, которое иногда также называют *основной памятью (main memory)*. Когда объем информации, к которой требуется более-менее быстрый доступ, превышает объем установленной оперативной памяти, наименее полезная информация кэшируется на жестком диске. Если эти данные опять понадобятся запущенной программе, они вновь загружаются в оперативную память. Процесс обмена данными между дисковым буфером и оперативной памятью называют *страничной подкачкой (paging)*.

Разумеется, перемещение данных из дискового кэша занимает время, поэтому следует по возможности уменьшить частоту обращения компьютера к диску. С этой целью следует установить, память большего объема.

Примечание

На практике некоторое количество данных всегда находится на диске. В современных операционных системах предусмотрен именно такой метод работы - это позволяет загружать в память большее количество данных, чем может вместить ОЗУ. Но следует стремиться ограничить использование страничной подкачки, поскольку считывание данных с жесткого диска занимает гораздо больше времени, чем считывание из ОЗУ.

Оперативная память, находящаяся на системной плате, является *динамическим ОЗУ* (Dynamic RAM). Слова "динамическая память" звучат загадочно, однако означают всего лишь, что такая память способна сохранять данные не более 4 мс, после чего их. следует регенерировать — образно говоря, памяти следует "напомнить" ее знания. Динамическое ОЗУ медленнее статического (Static RAM), которое используется в кэше L2, однако оно значительно дешевле.

Совет

Скорость работы ОЗУ зависит от характеристик используемых для его организации микросхем. Чем меньше время доступа, тем лучше. Поэтому при покупке памяти обязательно поинтересуйтесь временем доступа и выберите наиболее быстродействующее ОЗУ.

Основные разновидности динамической памяти

До самого недавнего времени большинство динамических ОЗУ были построены по схеме FPM (Fast Page Mode — быстрый постраничный доступ). Время доступа к памяти FPM составляет либо 70, либо 60 нс. Время доступа 60 нс требуется для обеспечения работы материнских плат Pentium, тактовая частота системной шины которых составляет 66 МГц. В памяти типа FPM можно одновременно получить доступ к одному (сравнительно большому) блоку памяти.

Примечание

Термин "быстрый постраничный доступ" относится к методу организации памяти, который обеспечивает в ОЗУ такого типа доступ к данным. Схемное построение памяти таково, что скорость ее работы максимальна, если следующий требуемый бит данных находится на одной странице с предыдущим битом. В машинах, построенных на основе процессоров семейства x86, размер страницы памяти составляет 4 Кбайта.

В системах-предшественницах Pentium характеристики ОЗУ типа FPM соответствовали характеристикам остальных компонентов компьютера. Однако даже при времени доступа 60 нс максимальная рабочая частота не превышает 30 МГц. Это означает, что даже в моей старенькой 486-й машине процессор с тактовой частотой 33 МГц работает быстрее, чем память. В настоящее время, когда процессоры работают в среднем на частоте 400 МГц, быстродействие ОЗУ типа FPM совершенно неудовлетворительно. Кроме того, поскольку тактовая частота системной шины материнских плат подскочила с 66 МГц до 100 МГц, ситуация стала еще хуже. Скорость работы ОЗУ чрезвычайно важна для обеспечения производительной работы компьютера и должна быть, по крайней мере, не меньше, чем у окружающих его компонентов. Необходимость создания более скоростного ОЗУ привела к созданию двух новых типов памяти.

- EDO (Extended Data Output — расширенный вывод данных) RAM.
- Синхронная динамическая RAM (SDRAM).

Память обоих типов рассматривается в следующих разделах.

Два удовольствия сразу - память типа EDO

EDO-память представляет собой усовершенствованную FPM-память без каких-либо радикальных изменений. Конструкция FPM-памяти задумана как "пожарная цепочка", когда за один раз из ОЗУ можно было извлечь единый фрагмент данных и передать его далее. В конструкции же EDO-памяти в этой цепочке предусмотрен "помощник": пока цепочка данных передается в процессор, он, обрабатывая их в фоновом режиме, отыскивает следующую порцию данных, которые необходимо обработать, и ставит их в очередь.

Повышение эффективности, которое достигается отысканием следующей порции данных за время передачи в процессор первого бита, ускоряет работу EDO-памяти по сравнение с FPM-памятью. Однако тактовая частота памяти при этом достигает всего 40 МГц, что существенно ниже тактовой частоты процессора и даже материнской платы. Поэтому, по мере ускорения работы систем, было предложено множество радикальных решений, позволяющих избежать ситуации, когда процессор сидит без дела, барабаня пальцами и ожидая поступления данных из ОЗУ.

Динамическое ОЗУ с пакетной передачей данных

Чтобы пояснить методы повышения быстродействия ОЗУ, вернемся немного назад и поговорим о том, как же, собственно, работает ОЗУ.

Одно из основных препятствий на пути ускорения работы ОЗУ (RAM) описано в названии памяти. Когда мы говорим, что к памяти предоставлен "произвольный" доступ, это означает одинаковую легкость доступа ко *всей* памяти.

Однако, хотя доступ можно получить одинаково *легко*, это еще не означает одинаково *быстро*. Если процессор может попросить компоненты сделать что-нибудь за единственный цикл, значит вы используете компьютер в режиме работы без периодов ожидания (zero wait state machine). Если операция не может быть выполнена за нужное время, в работе компьютера появляются периоды ожидания (wait states). По существу, период ожидания по длительности равен длительности периода колебаний тактового генератора (clock tick), в течение которого процессор простаивает. А раз так, этого следует избегать.

Примечание

Период колебаний тактового генератора представляет собой величину, обратную тактовой частоте процессора. Генератор процессора с тактовой частотой 300 МГц в одну секунду "выдает" 300000000 периодов колебаний. Чем выше тактовая частота процессора, тем короче период колебаний.

Контроллер памяти (memory controller) для доступа к DRAM разбивает ячейки памяти на четырехбитовые пакеты (four-bit bursts). При этом дольше всего обрабатывается первый бит адреса. Это связано с тем, что данный бит описывает адрес нужной страницы памяти. Итак, когда контроллер памяти считывает данные из FPM DRAM, он затрачивает первые пять тактов, для нахождения страницы, на которой находится первый бит запрошенных данных, а затем еще три такта, чтобы считать каждый дополнительный бит с этой страницы памяти. (Поскольку при каждом обращении считывается только один бит, для

считывания одного байта данных требуется параллельная работа восьми микросхем памяти. — Прим. ред.) Дело несколько ускоряется, если используется EDO-память, поскольку, хотя при работе с ней тоже требуется пять тактов, чтобы найти первую страницу, считывание последующих битов требует только двух тактов на каждый бит. Разумеется, если следующий бит данных находится на другой странице, все оказывается напрасным и для считывания следующего бита снова понадобится пять тактов. Решение этой проблемы облегчают кэши L1 и L2 (входящие в систему памяти процессора), поскольку в них сохраняются последние использовавшиеся данные, с тем, чтобы контроллеру памяти не требовалось постоянно извлекать их из ОЗУ. Однако емкость кэш-памяти невелика.

Чтобы обойти эту проблему применяется *технология пакетной передачи (bursting technology),* предусматривающая считывание не только текущих четырех битов, а сразу *всей* страницы (в системах, построенных на основе процессоров семейства x86, она имеет размер 4 Кбайт). По этой технологии после считывания из памяти всей страницы, *для считывания остальных данных, адреса которых описываются тремя оставшимися битами в каждом четырехбитовом наборе, дополнительные периоды ожидания уже не требуются.* Поскольку биты обнаружены, на их поиск, не затрачивается дополнительное время. Как и прежде, чтобы найти новую страницу, вам опять придется подождать пять тактов, но когда эта страница будет обнаружена, для считывания каждого бита достаточно единственного такта, а периода ожидания не требуется. Память сама "подскажет" контроллеру, как найти остальные биты.

Возможно, вы запутались, тогда попытайтесь вообразить все это примерно так. Представьте себе DRAM-память как ряды темных комнат, причем каждая из них представляет собой одну страницу памяти. Данные хранятся в ящиках (представляющих собой адреса), расставленных в комнатах и расположенных в логическом порядке, т.е. за ящиком 6 стоит ящик 7 и т.д. Единственная тонкость заключается в том, что ящики не соприкасаются, хотя расположены последовательно.

Когда контроллеру памяти необходимо получить данные с определенной страницы DRAM-памяти, он должен сначала найти страницу, на которой хранятся данные, а затем идти получать нужные данные. Итак, когда контроллер памяти приступает к работе, он идет по коридору, в который выходят двери всех комнат.

Если используют обычную DRAM-память, то контроллер памяти должен сначала найти нужную комнату, затем открыть дверь в Нее и, *все еще находясь в темноте,* на ощупь найти данные. Чтобы найти первый ящик потребуется некоторое время, однако если контроллер памяти его найдет, он сможет нащупать и найти следующий, затем еще один. С этого момента контроллер памяти может отправлять данные в процессор.

Насколько же упростится этот процесс, если осветить комнаты! Именно это и достигается применением технологии пакетной передачи данных. Когда контроллер памяти входит в освещенную "комнату", он все еще должен осмотреться, чтобы найти первый адрес, из которого необходимо извлечь данные. Однако после этого он может увидеть следующий ящик, затем еще один, а не нащупывать их по одному в потемках.

Таким образом "произвольная" часть доступа к RAM уже не выглядит столь произвольной — предполагается, что все биты находятся на одной странице. В противном случае производительность процесса поиска упадет.

Теперь, уяснив эти вопросы, рассмотрим современные технологии пакетной передачи данных: пакетную EDO-память и синхронную динамическую RAM-память.

Пакетная EDO-память

EDO-память (BEDO — Burst EDO) является дальнейшим улучшением технологии EDO за счет использования ускоренного упреждающего считывания. Он может работать синхронно с процессором вплоть до частоты 66 МГц.

Результат аппаратного ускорения – SDRAM

Перспективное решение, реализованное в современных микросхемах SDRAM-памяти, которые могут работать синхронно с процессором вплоть до частоты 100 МГц, что соответствует времени доступа 10 нс.

Пакетная передача данных

Как вы уже поняли, в настоящее время теоретический предел тактовой частоты DRAM-микросхем составляет 100 МГц. Конечно, это больше 28 МГц, обеспечиваемых микросхемами FPM DRAM, но никоим образом не сопоставимо с рабочими частотами современных процессоров, достигающими 400 МГц. Как же решить эту проблему?

В настоящее время — никак. Современные микросхемы не могут работать в такой частотой. Есть, правда, пара возможных кандидатов, однако пока что их схемотехника разработана только теоретически — на рынке нет микросхем, созданных на базе этих технологий. В то время, когда писалась эта книга, в основном использовались память EDO или SDRAM и только изредка — BEDO. В наиболее совершенных машинах их применение приводит к появлению периодов ожидания.

Чтобы ускорить работу памяти, можно повысить частоту тактового генератора (clock speed), увеличить разрядность шины данных (data path) либо использовать оба подхода. Проблема создания действительно скоростной памяти (как и вообще чего-нибудь быстродействующего) заключается в том, что чем быстрее работает память, тем важнее становится качество ее работы. Без применения дополнительных средств управления, скорость работы SDRAM-памяти достигает предельного значения. В разработке скоростной памяти основное значение имеет решение проблемы достаточной надежности.

В настоящее время предложены две основные технологии повышения скорости работы памяти.

- Технология SLDRAM (DRAM-память с синхронными связями).
- Технология Rambus DRAM (RDRAM).

Технология SLDRAM развивается консорциумом Synchronous Link Consortium, в который входят 15 фирм, в том числе Hyundai, IBM и Apple. Технология RDRAM разработана фирмой Rambus и поддерживается фирмой Intel. В настоящее время конструкция SLDRAM предусматривает использование модулей памяти на 64 Мбайт, работающих на частоте 400 МГц и передающих данные по двум конвейерам (pipelines) со скоростью 800 Мбит/с — в восемь раз выше скорости SDRAM. Память RDRAM работает на частоте 800 МГц, обеспечивая общую скорость передачи данных 1,6 Тбит/с по двум магистралям (pipelines).

Какая технология завоюет рынок? Пока неясно. Память RDRAM уже используется в некоторых моделях видеоплат (video cards), однако пока что не применяется в качестве оперативной памяти. Конструкция SLDRAM сложна. Некоторые ее экземпляры прошли испытания, но в то время, когда писалась эта книга, в коммерческую продажу память такого типа не поступала. Конечно, внедрению технологии RDRAM немало содействует поддержка фирмой Intel, однако члены консорциума Synchronous Link Consortium тоже весьма влиятельны.

Диски и контроллеры

Еще один ключевой элемент быстрого и надежного сервера — жесткий диск. Независимо от типа сервера — файлового, печатного, связи, приложений — все ваши данные и программы хранятся на диске. Поэтому для повышения производительности следует выбирать самый быстрый диск.

Интерфейс EIDE

Жесткий диск состоит из двух основных частей: собственно диска и платы контроллера. На заре эпохи персональных компьютеров стандартом ESDI (Enhanced Small Disk — улучшенный интерфейс малых устройств) предусматривалось разделение жесткого диска и его контроллера на две части, соединенные плоскими кабелями (рис. 7.4).

Этот интерфейс работоспособен, однако соединительные кабели подвержены тем же FR-помехам, что и сетевые кабели (в компьютере немало источников помех, причем один из них — второй кабель жесткого диска).

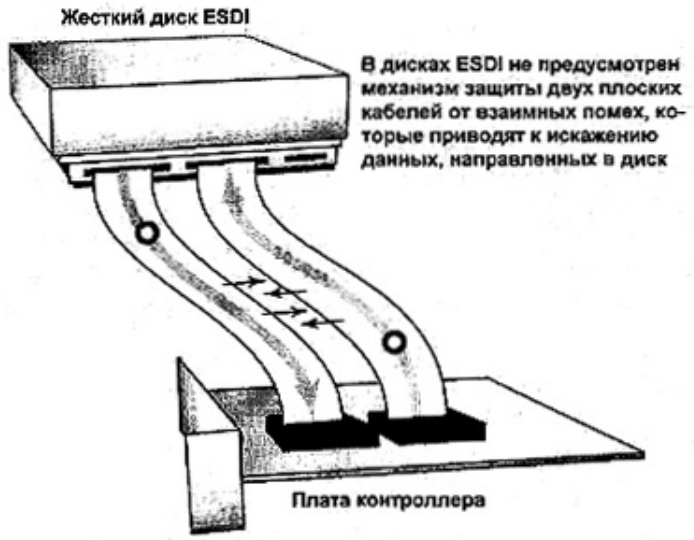


Рис. 7.4. Жесткий диск ESDI и плата контроллера

Что такое интерфейс IDE

В 1998 г. фирмой Western Digital (и другими) разработан стандарт IDE (Integrated Drive Interface — встроенная электроника управления диском). Он предусматривал объединение контроллера и диска в единый блок. Если перевернуть диск IDE, вы увидите контроллер диска (drive controlling mechanism). Кроме того, в систему входит главный (хост) адаптер (host adapter). Однако он нужен только для связи между системной платой и дисковым контроллером и никоим образом не связан с обработкой данных. Хост-адаптер идентифицирует любое подключенное к нему устройство либо как "ведущее" (master), либо "ведомое" (slave), (а в некоторых случаях как "вторичное ведомое устройство" (secondary slave device)).

Технология IDE ограничена. Во-первых, к хост-адаптеру можно подключить только два устройства. Это означает, что для подключения нескольких дисков (или других устройств IDE, например, ленточных накопителей) необходимо множество плат контроллеров, установленных в слоты с разными прерываниями. Во-вторых, вместимость дисков IDE невелика. Максимальная вместимость диска IDE составляет 528 Мбайт — в настоящее время этого едва достаточно для загрузки операционной системы и полного набора офисных приложений, не говоря уже о месте для файлов подкачки и прочих данных. (Следует заметить, что ограничение на емкость диска в 528 Мбайт налагается операционной системой DOS, а не аппаратными
особенностями жесткого диска. — Прим. ред.)

С этими проблемами помог справиться усовершенствованный IDE интерфейс, называемый EIDE (Enhcanced Integrated Drive Interface - усовершенствованный интерфейс малых устройств). Контроллеры EIDE позволяют подключать к материнской плате одновременно до четырех устройств, что намного повышает гибкость системы. Кроме того, в то время, когда писалась эта книга, диски EIDE позволяли хранить до 16 Гбайт данных.

Интерфейс SCSI

Фирма Apple Computer разработала ещё один тип интерфейса для контроллера жесткого диска, который со временем стал использоваться не только в компьютерах Macintosh, но и PC иных типов. Данная технология, называемая SCSI (Small Computer System Interface — интерфейс малых вычислительных систем), сходна с технологией IDE/EIDE в том, что жесткий диск и его контроллер образуют единое устройство, подключенное к системной плате через хост-адаптер. Различие заключается в методе соединения этих устройств. Хост-адаптеры SCSI соединяют любые устройства SCSI в *последовательную* цепь выходящую даже за пределы компьютера, и насчитывающую до семи устройств, не считая хост-адаптера. Хотя каждое устройство соединено напрямую с другим устройством, а не с хост-адаптером, все они сообщаются с главным адаптером.

Как главный адаптер узнает, с каким жестким диском он "разговаривает" или кому он посылает данные? Каждому устройству в цепочке SCSI, включая и сам хост-адаптер, присваивается номер, называемый *идентификатором SCSI ID*. ID 7 резервируется для главного адаптера. Значения ID 0 и 1 предназначены для жестких дисков (причем 0 резервируется для загрузочного диска), а ID 2—6 можно присваивать любому другому устройству в цепочке. Значения ID не обязательно должны следовать порядку расположения устройств в цепочке SCSI. Кроме того, совсем не обязательно использовать *все* значения ID. Иными словами, в цепочку SCSI не обязательно включать все семь устройств. Единственный действительно существенный момент заключается в том, что все зарезервированные ID должны использоваться по назначению, а оба конца цепочки SCSI следует правильно согласовать. Согласование обеспечивается соответствующей установкой перемычек на плате (для точного согласования устройств следует ознакомиться с их техническим описанием. — Прим. ред.), значения же ID устройств SCSI могут устанавливаться аппаратно либо программно в зависимости от типа конкретного устройства.

Совет

Точно так же, как ранее был дан совет записывать значения IRQ и адресов ввода/вывода, имеет смысл записать значения идентификаторов SCSI ID, а также устройств, которыми заканчивается цепочка. Намного проще узнать эти значения из списка, который лежит под рукой, чем переворачивать каждое устройство, чтобы выяснить его установки, особенно, если оно находится внутри компьютера.

Если вам необходимо включить в систему новое устройство SCSI, выключите компьютер, подсоедините устройство к концу цепи и установите терминатор. Это выглядит очень просто.

Конечно, так бы оно и было, если бы существовал единый стандарт SCSI, а все устройства и хост-адаптеры SCSI были совместимы. В табл. 7.1 приведены различные типы SCSI-интерфейсов, используемые в настоящее время.

Таблица 7.1. Типы SCSI-интерфейсов

Тип SCSI	Описание
SCSI-2	Используется 50-штыревой разъём, 8-битовая шина, обеспечивается скорость передачи данных 4 Мбит/с
Wide SCSI	Используется 68-штыревой разъём и 16-битовая шина
Fast SCSI	Аналогичен обычному SCSI-интерфейсу, но в данной версии тактовая частота увеличена в два раза, чем обеспечивается скорость передачи данных 10 Мбит/с
Fast and Wide SCSI	Объединяет в себе 16-битовую шину интерфейса Wide SCSI и тактовую частоту Fast SCSI, обеспечивает скорость передачи данных 20 Мбит/с
Ultra SCSI	Используется 8-битовая шина и обеспечивается скорость передачи данных 20 Мбит/с
Ultra Wide SCSI/SCSI-3	Используется 16-битовая шина и обеспечивается скорость передачи данных 40 Мбит/с
Ultra2 SCSI	Используется 8-битовая шина и обеспечивается скорость передачи данных 40 Мбит/с
Ultra2 SCSI Wide	Используется 16-битовая шина и обеспечивается скорость передачи данных 80 Мбит/с

Примечание

В интерфейсе SCSI-1, предшественнике SCSI, использовался 25-штыревой разъем, и не предусматривалось объединение устройств в цепочку SCSI. В общем случае, если говорит просто SCSI, без уточнений, то имеют в виду SCSI-2, а не SCSI-1.

Одна из замечательных возможностей SCSI-интерфейса заключается в том, что он обеспечивает не только подсоединение цепочки устройств к одному хост-адаптеру, но и передачу данных по этой цепочке. Интерфейсы, перечисленные в табл. 7.1, предназначены не только для подключения единственного жесткого диска, но также и для всех SCSI-устройств в цепочке. Хост-адаптер SCSI может одновременно "разговаривать" с несколькими устройствами, работая с ними в многозадачном режиме. Это важно по двум причинам. Первая: считывающим и записывающим головкам жесткого диска необходимо время, чтобы найти нужное место на диске, а затем прочесть или записать данные. Кроме того, хост-адаптер может "думать" быстрее, чем периферийные устройства, подключенные к нему. Вторая причина: единственному устройству в цепочке SCSI не требуется вся доступная полоса пропускания. Поэтому разделение хост-адаптером времени передачи данных между множеством устройств весьма эффективно.

Различия между интерфейсами SCSI и EIDE

Несмотря на большую стоимость по сравнению с EIDE, SCSI — более совершенная серверная технология (не просто технология, а именно *серверная* технология) по нескольким причинам.

Первая: в отличие от EIDE-устройств, хост-адаптерам SCSI изначально была присуща многозадачность. Когда обработки дожидаются данные, предназначенные для чтения или записи с/в нескольких устройств, хост-адаптер EIDE должен завершить работу с одним диском, прежде чем сможет начать обрабатывать второй запрос. Здесь возможны два варианта. Во-первых, прежде чем контроллер может приступить к чтению или записи с другого устройства, он должен завершить считывание с медленных жестких дисков или CD-ROM (а устройства CD-ROM *намного* медленнее жестких дисков). Во-вторых, для одного устройства резервируется *вся* полоса пропускания между главным адаптером и диском, но диск может и не нуждаться во всей полосе. Поскольку же главный адаптер может одновременно "общаться" только с одним-единственным устройством, остальная часть полосы пропускания простаивает. Следовательно, чем больше устройств установлено в машине EIDE, тем больше бесцельная затрата времени и полосы пропускания.

Вторая: SCSI-интерфейс более "гибок", чем EIDE. Для добавления устройства в SCSI-машину достаточно выключить машину, присвоить устройству идентификатор SCSI ID (чтобы гарантировать отсутствие конфликтов с другими устройствами), а затем правильно согласовать это устройство. Добавление устройств с EIDE-интерфейсом сложнее. В конечном итоге, если учесть экономию времени, такая гибкость окупается.

Что еще важнее, интерфейсами SCSI снабжены многие устройства -сканеры, жесткие диски, CD-ROM, съемные диски, ленточные накопители. В то же время с интерфейсом EIDE выпускаются только жесткие диски и устройства CD-ROM.

Примечание

Одно из SCSI-устройств вам понадобится обязательно - это ленточный накопитель для резервного копирования. Накопители, снабженные другим интерфейсом, не могут работать с контроллером гибких дисков (floppy controller) и, кроме того, слишком медленно обрабатывают данные тех типов, которые обычно архивируются на сервере.

Третья: SCSI-диски вместительнее дисков EIDE, несмотря на то, что в настоящее время диски EIDE могут хранить до 16 Гбайт данных, и требования к емкости "хранилищ" данных продолжают расти. Программное обеспечение и операционные системы постоянно разрастаются, средства становятся более обширными, и нет никаких признаков, что разработчики собираются умерить темп работы, чтобы подождать пока характеристики устройств "дотянутся" до требуемого уровня. Разрослись не только программы, объем данных тоже непрерывно растет по мере распространения мультимедийных файлов и документов с развитым форматированием. Поэтому для сервера вам необходим возможно больший объем дискового пространства.

С клиентной машиной дело обстоит несколько иначе. Во-первых, в среде клиент/сервер оборудование большинства клиентных компьютеров обновляется значительно медленнее, чем оборудование серверов. Как никак, цель создания сети заключается в централизации вашего оборудования именно на сервере и его совместного использования клиентами. Во-вторых, способность SCSI-интерфейса к работе в многозадачном режиме влечет за собой и некоторые издержки, которые не имеют особого значения по сравнению с повышением производительности 5—6 дисковых устройств. Однако когда в системе используется один диск, эти издержки имеют значение. В-третьих, большинство персональных компьютеров обеспечивают поддержку интерфейса EIDE, Добавление поддержки SCSI-интерфейса требует дополнительных затрат, что неприемлемо для большинства клиентов. На клиентной машине обычно установлен один жесткий диск, следова-

тельно, конкуренция за полосу пропускания и доступ к хост-адаптеру не столь важна. А поскольку интерфейс EIDE значительно дешевле, он используется наряду со SCSI.

Монитор для сервера

Рассмотрение мониторов в составе сервера будет достаточно кратким. Поймите, вам нет нужды тратиться на приобретение для сервера высококачественного монитора, поскольку никто не будет проводить за ним много времени. Если вы можете приобрести монитор с приемлемой частотой регенерации (refresh rate) не менее 75 Гц (имеется в виду частота кадровой развертки. — Прим. ред.), то он будет работать вполне удовлетворительно. Вы и без того выкладываете немало средств на поддержку SCSI-интерфейса и дополнительную память, так что не стоит разоряться еще и на 21" монитор, на который мало кто посмотрит вообще. Однако, как указано в гл. 8, у клиента все обстоит совершенно иначе.

Защита от сбоев питания

Защита от сбоев питания для сервера обязательна. Во-первых, снабжение электричеством ни в коей мере нельзя считать надежным — все обстоит как раз наоборот. Одна из проблем электроснабжения — электрические бури (electrical storms). Я живу в Виржинии, и здесь обычным летом вполне могут возникать краткосрочные перебои в подаче электроэнергии — не реже одного раза в неделю. Пару лет назад лето было очень плохим, когда перебои случались два раза в неделю, иногда ненадолго, а иногда и на несколько часов. Как правило, перебои не слишком мешают моей работе, однако без принятия надлежащих мер защиты при каждом отключении электроэнергии данные будут теряться. Если перебои (как нас уверяют) действительно вызваны глобальным потеплением, положение не улучшится никогда; Ожидается, что одним из побочных эффектов глобального потепления станут все более мощные и частые электрические бури, поскольку таяние льда на полюсах насыщает атмосферу влагой.

Причины перебоев возникают не только в природе, но и в работе системы подачи электроэнергии. Некогда она проектировалась для использования меньшим числом людей и *намного* меньшим числом электрических приборов. Со временем системы энергоснабжения оказались в значительной мере перегруженными. В результате перегрузки заметно падает напряжение при подключении слишком большого числа потребителей, поскольку сила тока превышает допустимую величину. Хотя и в меньшей степени, но это же происходит в системе электроснабжения крупных зданий. В современных зданиях проложена силовая электропроводка, рассчитанная на значительную нагрузку. Это в какой-то степени защищает электронные приборы от перегрузок из-за включения мощных моторов, работа которых и так неблагоприятно сказывается на общем состоянии системы энергоснабжения. Однако в старых зданиях электропроводка по-прежнему пригодна всего лишь для освещения и работы электрических пишущих машин.

В идеальном случае следует защищать электропитание всех сетевых компьютеров, а не только сервера. Если вы серьезно относитесь к защите данных, следует защитить сервер, по крайней мере, от внезапных перебоев в электроснабжении, а также падений и всплесков электрического напряжения, которые могут повредить его компоненты.

Подавители всплесков (surge protectors) обеспечивают недостаточно эффективную защиту от повышения напряжения, однако можно воспользоваться удлинителем со встроенным подавителем — это удобный способ подключения множества устройств к одной

штепсельной розетке. Почему же они неэффективны? Во-первых, они бесполезны при отключении электричества, а во-вторых, не обеспечивают должную защиту от всех всплесков электрического напряжения. Всплеск, который не будет подавлен подавителем (например, вследствие его краткости), может, тем не менее, повредить более чувствительное электронное оборудование компьютера. Если вы используете подавитель перенапряжений, то следует предварительно убедиться, что он сможет защитить компьютер от всплесков в вашей сети.

Чтобы реально защитить компьютер, следует использовать источник бесперебойного питания (UPS — Uninterruptable Power Supply). К источникам бесперебойного питания можно отнести любую систему, в которой предусмотрен резервный аккумулятор. Он отдает энергию при пропадании напряжения от штатного источника питания (например, блока питания компьютера). Аккумулятор сможет проработать не слишком долго, но этого времени должно хватить на то, чтобы корректно завершить работу программ, сохранить файлы и выключить машину, что, безусловно, должно привести в восторг операционную систему.

Примечание

Время, *в* течение которого UPS обеспечивает работу компьютера, зависит от емкости его батареи и степени заряженное™ аккумулятора в момент пропадания напряжения, а также количества подключенных к нему устройств. Выбирая UPS, объясните продавцу, что именно вы собираетесь подключать к устройству (например, сервер и монитор), и в течение какого промежутка времени должна обеспечиваться работоспособность компьютера при пропадании электроэнергии. Тогда продавец сумеет вам подсказать, какой емкости аккумулятор следует приобрести.

Выпускают два типа устройств UPS: переключаемые источники электропитания (SPS — Switched Power Supplies) и автономные, которые можно отнести к истинным UPS.

Переключаемые источники электропитания

Как показано на рис. 7.5, в нормальном режиме в переключаемом источнике электропитания напряжение из электрической розетки подается непосредственно на компьютер, а часть энергии расходуется на подзарядку аккумулятора. При отключении сетевого напряжения источником питания становится аккумуляторная батарея.

Обратите внимание на два обстоятельства. Во-первых, SPS не всегда улучшает подаваемое на компьютер напряжение. Иными словами, электроэнергия подается из электрической розетки "как есть", т.е. вместе со всеми падениями и всплесками, которые могут быть в электросети. Чтобы избежать подобных проблем, приобретая SPS, выбирайте тот, где предусмотрена защита от перенапряжений. Во-вторых, в таком устройстве предусмотрен контроль за состоянием напряжения в электросети, при котором SPS отключается от внешней линии электроснабжения и кричит: "Внимание! Напряжение пропало! Переключаюсь на аккумулятор!" ,— и переключает питание на аккумулятор. Иными словами, на некоторый (краткий) период питание компьютера все же отключается.

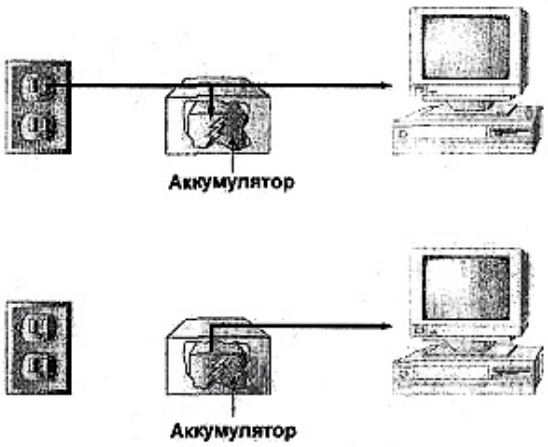


Рис. 7.5. Переключаемый источник питания

Сколько длится этот период? В настоящее время — недолго. SPS сможет переключить питание с внешней линии на аккумулятор примерно за 4 мс. Этого компьютер не заметит. Точно так же, как вы можете жить, ненадолго задержав дыхание, компьютер сможет поработать некоторое время без подачи электроэнергии. Просто не рекомендуется отключать напряжение (как и переставать дышать) на слишком долгое время.

К SPS относится большинство UPS, выставляемых на продажу. Они намного дешевле автономных UPS (рассматриваемых ниже), и превосходно работают во многих случаях, при условии, что подаваемая электроэнергия имеет достаточно высокое качество. Ваше оборудование не повредят повышения напряжения и его скачки.

Автономные источники питания

Если вам необходима более эффективная защита, чем та, которую может обеспечить коммутируемый UPS, следует использовать автономные UPS. Автономный UPS получает напряжение от внешней сети, преобразует его и подает на аккумулятор, а затем повторно преобразует, после чего подает сетевое напряжение на устройства потребителя (рис. 7.6). Возникающие в первичной сети перенапряжения портят аккумулятор, но не сервер. В то же время, пока сетевое напряжение есть, аккумулятор подзаряжается.

Поскольку компьютер всегда питается от аккумулятора, при отключении внешнего напряжения задержки в подаче напряжения даже на 4 мс нет. Однако теперь электрическая энергия уже не поступает в аккумулятор, так что компьютер будет работать только до тех пор, пока аккумулятор не разрядится.

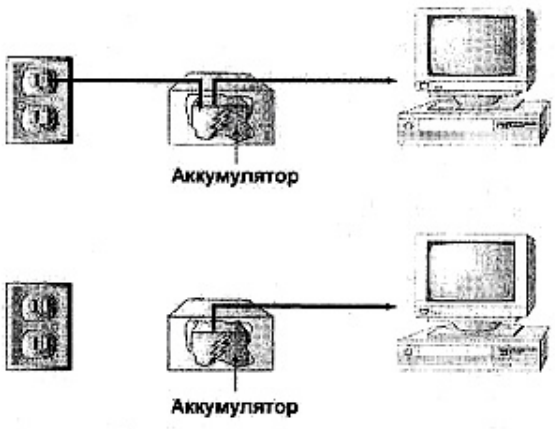


Рис. 7.6. Автономный источник питания

Выбор UPS

Что же выбрать: SPS или UPS? Это зависит от того, что вам нужно. Устройства обоих типов в последнее время значительно подешевели. Но, хотя автономный UPS дороже, желательно все же приобрести именно его, если вы хотите обеспечить своим устройствам комфортные условия. Цена устройства зависит от емкости аккумулятора и мощности. Ориентировочно SPS обойдется вам в несколько сотен долларов, а автономный UPS — несколько тысяч.

Какие устройства следует подключать к такому источнику питания? серверах желательно защитить не только компьютер, но и монитор, поскольку, если вам понадобится корректно завершить работу сервера, без монитора не обойтись. Не стоит защищать *все* устройства, поскольку это ускорит разрядку аккумулятора. *Никогда* не защищайте лазерный принтер, поскольку он потребляет большой ток и практически мгновенно разрядит аккумулятор.

А как быть с клиентными машинами? Еще недавно считалось непрактичным защищать клиентные машины. Однако в последнее время источники бесперебойного питания (как и многое другое) значительно подешевели. Можно приобрести переключаемый источник электропитания всего за 100 $. Возможно, имеет смысл потратить эти деньги, чтобы спасти данные при внезапном отключении электроэнергии.

Выводы

В этой главе рассмотрены основные элементы оборудования, используемого практически во всех серверах. Попутно обсуждались некоторые технологии, которые следует использовать в серверах.

Подводя итог, я рекомендую для построения сервера использовать следующее.

- Быстродействующий процессор со встроенной кэш-памятью большой емкости.
- Материнскую плату с шиной PCI.
- Память SDRAM (объемом *не менее* 64 Мбайт: чем больше компьютеров в сети, тем больше требуется памяти).
- Для подключения внешних устройств установить хост-адаптер SCSI.
- Дешевый монитор с минимальными допустимыми характеристиками.
- Источник бесперебойного питания.

Воспользовавшись этими компонентами, вы создадите сервер, соответствующий запросам большинства клиентов вашей сети. Конечно, к некоторым серверам предъявляются специфические требования, основанные на назначении сервера. В гл. 8 обсуждаются различные типы серверов, с которыми, вероятно, вам придется иметь дело, а также требования к ним.

Упражнение 7

1. Где находится кэш L1 и каково его назначение?
2. Что в современных компьютерах работает быстрее: процессор иди оперативная память? Почему?
3. Платы ISA работают с тактовой частотой ____МГц, в то время как платы PCI работают с тактовой частотой ____МГц.

4. В настоящее время самая быстрая оперативная память, которую можно найти в продаже, называется

   A. EDO.
   B. SDRAM.
   C. FPMRAM.
   D. RDRAM.

5. Заполните пустые места в таблице, взятой из этой главы.

Тип SCSI	**Описание**
SCSI-2	Используется 50-штыревой разъём, __-битовая шина, обеспечивается скорость передачи данных 4 Мбит/с
Wide SCSI	Используется __-штыревой разъём и 16-битовая шина
_____	Аналогичен обычному SCSI-интерфейсу, но в данной версии тактовая частота увеличена в два раза, чем обеспечивается скорость передачи данных 10 Мбит/с
Fast and Wide SCSI	Объединяет в себе 16-битовую шину интерфейса Wide SCSI и тактовую частоту интерфейса _____, обеспечивает скорость передачи данных __ Мбит/с
Ultra Wide SCSI/SCSI-3	Используется 16-битовая шина и обеспечивается скорость передачи данных __ Мбит/с
_____	Использует 8-битовую шину, но поддерживает скорость передачи данных 20 Мбит/с
Ultra2 SCSI Wide	Используется __-битовая шина и обеспечивается скорость передачи данных 40 Мбит/с
_____	Используется 16-битовая шина и обеспечивается скорость передачи данных 80 Мбит/с

6. Поясните различие между автономным UPS и переключаемым UPS.

Глава 8

Серверы и дополнительное оборудование

В гл. 7 приведен список основных компонентов, из которых состоит сервер: процессор, хост-адаптеры, память и т. д. Все это всего лишь "скелет" сервера, поскольку организация сети подразумевает нечто большее, нежели просто централизованное хранение файлов. Далее будут описаны серверы нескольких типов, с которыми вы, вероятно, встретитесь, и рассмотрены специализированные аппаратные средства, которые могут потребоваться для их создания.

Конечно, должна быть обеспечена поддержка таких, подчас весьма специфических средств системными компонентами, описанными в гл. 7. (Никакой пользы от самого быстрого в мире принтера при работе на компьютере с малым объемом памяти не будет.) Я расскажу, как эти основные компоненты сервера обеспечивают поддержку дополнительного оборудования. Кроме того, некоторые серверы должны сочетать в себе возможности серверов двух или более типов (нередко можно встретить отдельный сервер, для хранения файлов и печати).

Хранение данных

Системы для работы с файлами, являются прародителями всех сетевых файловых серверов. Вы можете не нуждаться в услугах сетевой связи или многопользовательских приложений (в некоторых сетях обходятся без серверов печати), но практически всем пользователям сети типа клиент/сервер требуются удобные средства для хранения и архивирования файлов.

Организация дисковой памяти

Перед тем как углубиться в описание систем, работающих с дисками и файлами, кратко рассмотрим, как в компьютере в принципе организована эта работа.

Поверхность диска для хранения данных физически разделена на окружности, называемые *дорожками (track)*, и на секции, в виде радиально расходящихся из центра окружностей клиньев. Дуги окружностей, образованные пересечением таких концентрических окружностей и клиновидных секций, называют *секторами*. В файловых системах FAT (File Allocation Table – таблица размещения файлов) и NTFS (New Technology File System – новая файловая система) эти секторы, в свою очередь, логически группируются в *кластеры*, количество которых на диске зависит от типа используемой системы и размера диска. Отнюдь не во всех файловых системах секторы организуются в кластеры. Например, в спроектированной для OS/2 файловой системе HPFS этого не делается. В последнем случае логической единицей хранения данных является сектор.

Каждый диск форматируется соответствующей утилитой, которая присваивает уникальный (неповторяющийся) номер каждой логической единице хранения данных на диске (например, каждому кластеру). После того как диск будет отформатирован, операционная система получит в своё распоряжение «карту» (таблицу) жёсткого диска, содержащую описание того, какие из кластеров используются для хранения соответствующих данных,

а также какие из них свободны и где они находятся. Каждый раз, когда данные записываются или удаляются с диска, содержимое таблицы обновляется. Хотя далее (для упрощения изложения) все приводимые примеры будут основаны на файловой системе FAT, всё сказанное также применимо и к другим файловым системам. Форматы таблиц и способы их структурирования изменяются при переходе от одной файловой системы к другой, но их функции остаются теми же.

Дисковый сервер

Средства работы с файлами произошли от средств для работы с дисками, предоставляемыми дисковым сервером. *Дисковый сервер* — центральное хранилище файлов и данных, подключенное к сети таким же образом, как и любой узел. Поскольку он фактически является общедоступным жестким диском совместного использования, то каждый клиент сети может задавать у себя соответствующее этому диску имя так; как если бы этот диск был локальным. При чтении или записи на диск операционная система обращается к таблице FAT, которая локализует данные на диске по номерам соответствующих им кластеров.

Рис. 8.1. Клиент открывает файл, хранящийся на дисковом сервере

Вероятно, вы уже заметили потенциальные проблемы такого подхода. В конечном итоге задача сервера состоит в предоставлении всем клиентам сети доступа к жесткому диску, не правда ли? Но поскольку файлы на жестком диске создаются и удаляются, его таблица, поддерживаемая FAT, будет изменяться. Удаление файлов приводит к появлению на диске свободных кластеров, в которых могут быть сохранены вновь создаваемые файлы. В файловой системе FAT запись файла всегда начинается с первого свободного кластера. Таким образом, после достаточно длительной работы нескольких клиентов таблица жесткого диска может совершенно измениться. Таблица, содержимое которой было корректно по состоянию на 8 часов утра, может стать совершенно неточной к 4 часам вечера, что может замедлить и даже полностью приостановить поиск данных.

Для решения этой проблемы диск сервера обычно разделяют на несколько томов (по одному для каждого пользователя), либо в него устанавливают съемные диски, каждый из которых доступен только одному пользователю. Серверы могут применяться также и для других целей. Например, можно использовать дисковый сервер для предоставления доступа к гибкому диску пользователям бездисковой рабочей станции. Однако хотя дисковые серверы и не исчезли совершенно из употребления, они сегодня не используются так широко, как файловые.

Файловые серверы

Вместо организации совместного использования физических дисков, файловый сервер предоставляет клиентам сети совместный доступ к области хранения данных. Как указывалось выше, системы для работы с файлами функционируют так же, как и системы для работы с дисками.

- Файловый сервер предоставляет совместный доступ пользователям всей сети к определенному тому.
- Клиент использует имя диска (или путь Unicode) для доступа к совместно используемому тому.
- Клиент может читать и писать в совместно используемый том.

С точки зрения клиента обращение к совместно используемому тому подобно обращению к локальному жесткому диску, за исключением одного: если сервер, на котором хранится совместно используемый том, будет отключен от сети или приостановит совместное использование данного тома, то клиент не сможет к нему

Как работает файловый сервер

Хотя файловые и дисковые серверы могут показаться клиенту совершенно одинаковыми, это вовсе не так. Разница заключается, в основном, в распределении обязанностей. Отличие между дисковыми и файловыми серверами можно выразить следующим образом, Когда сетевой клиент первый раз после перезагрузки запрашивает у дискового сервера файл, тот просматривает свое содержимое и находит "карту" склада, хранящего данные. После этого дисковый сервер говорит клиенту: "Вперед, малыш, забирай свой файл, но получи себе еще и карту. Я предпочитаю заниматься более интересными вещами, поэтому обеспечивай себя сам с помощью этой карты". Каждый раз, когда клиент получает что-либо со склада или что-либо возвращает в него, порядок на этом складе немного изменяется, но поскольку при этом выполняется автоматическое обновление, то карта, предоставленная дисковым сервером, будет точна. Однако когда клиентный компьютер через некоторое время снова обратится к серверу для поиска файлов с помощью своих старых карт, очень может быть, что склад будет уже организован по-другому, и клиент не сможет ничего найти.

В отличие от дискового, файловый сервер будет искать требуемое сам, не разрешая толпе сетевых клиентов обшаривать свой собственный жесткий диск. Когда рабочая станция запросит у него файл, файловый сервер ответит ему: "Я должен переслать эти данные — уж лучше я сделаю все сам". После этого он передаст запрос драйверу файловой системы, который найдет файл и пошлет информацию о его местонахождении клиентному приложению, после чего оно откроет этот файл. Клиент никогда не получит копию FAT-таблицы диска сервера, Хотя и использует серверные средства обработки такого запроса. Поэтому в файловом сервере существует только одна копия FAT-таблицы, всегда соответствующая текущему моменту времени.

Обслуживание файловых операций является одной из наиболее распространенных функций сетевого сервера, позволяющих решить несколько очень полезных задач. Во-первых, с помощью соответствующих средств обеспечивается централизация хранения данных для облегчения их последующего архивирования. Во-вторых, файловые серверы предоставляют доступ к одному файлу сразу нескольким пользователям. Конечно, во многих случаях клиентный компьютер может предоставить весь свой жесткий диск для совместного использования всей сетью, так что локально хранимые файлы становятся дос-

тупными всей сети (что обычно делается в одноранговой сети). Однако при этом могут возникнуть проблемы, если, например, сразу 40 человек в сети предоставят некоторую часть своих жестких дисков для совместного использования всей остальной сети. Это может привести к тому, что отдельные файлы найти будет чрезвычайно сложно.

Файловые серверы имеют только один недостаток: такой сервер *должен* все время находиться в режиме оперативного доступа, и содержимое его жесткого диска *должно* регулярно архивироваться, в противном случае он становится хуже, чем бесполезным. Если файлы хранятся на клиентных компьютерах, то при отключении одного из них все остальные еще могут продолжать работу. Но если выключится файловый сервер, работа сети будет парализована. Поддержка операций архивирования и необходимость обеспечения надежности функционирования являются критическими требованиями при организации работы хорошего файлового сервера.

Оборудование файлового сервера

Что же требуется для создания хорошего файлового сервера? Емкие и надежные жесткие диски для хранения информации, достаточный объем оперативной памяти, позволяющий эффективно обслуживать запросы на открытие и сохранение файлов, а также надежная система архивации. Все это и рассмотрено в последующих разделах.

Требования к жесткому диску

Диски должны быть быстрыми, с набором соответствующих аппаратных; функций. Возвратившись к описанию жестких дисков (см. гл. 7), вспомним, что наилучшим типом жестких дисков для файлового сервера почти наверняка являются диски с интерфейсом SCSI. Они дороже дисков EIDE, но быстрее обслуживают множественные запросы и удобнее в использовании, поскольку их легко добавлять в SCSI-цепочку.

Примечание

Хорошая сетевая операционная система должна содержать набор средств для расширения томов, т.е. должно быть предусмотрено добавление нового дискового пространства к ранее созданному разделу без изменения структуры логических дисков так, чтобы два и более физических дисков могли рассматриваться в виде одного тома.

Сколько нужно памяти

Требуется достаточный объем оперативной памяти для поддержки всех запросов чтения и записи файлов, поступающих на сервер. Сколько для этого нужно памяти? Ответить на этот вопрос нелегко. При работе сервера приложений (который будет рассмотрен в конце этой главы) можно воспользоваться эмпирическим правилом, в соответствии с которым следует предоставлять каждому пользователю 4—8 Мбайт оперативной памяти. Но файловый сервер работает не так напряженно, как сервер приложений, поскольку работа файлового сервера состоит всего лишь в обработке запросов чтение/запись. После открытия файла память файлового сервера уже не расходуется, в то время как сервер приложений размещает файлы приложения в своей собственной памяти.

Защита файлов

Вам потребуется система архивирования. Основная причина использования файлового сервера в качестве главного хранилища информации — это возможность эффективной защиты данных компании (или ваших личных данных, если сервер — часть домашней сети). Если данные не являются важными, они, вероятно, и не должны находиться в главном хранилище. Методы архивации не обязательно должны быть самыми передовыми, однако вы должны их знать и уметь восстанавливать с их помощью архивированные данные при повреждении жесткого диска.

Архивирование — весьма важная операция для большинства типов серверов, но для файлового сервера она, безусловно, является жизненно важной. Поэтому давайте немного углубимся в описание некоторых носителей архивной информации.

Примечание

Какие носители архивной информации следует использовать, зависит от вашей операционной системы и выбранной утилиты архивирования. Перед ее покупкой выясните, какие потребуются аппаратные средства, поддерживаемые этой утилитой. Например, для записи архивов на компакт-диск вам потребуется программа архивирования, способная работать не только с магнитными лентами.

Накопители на магнитной ленте

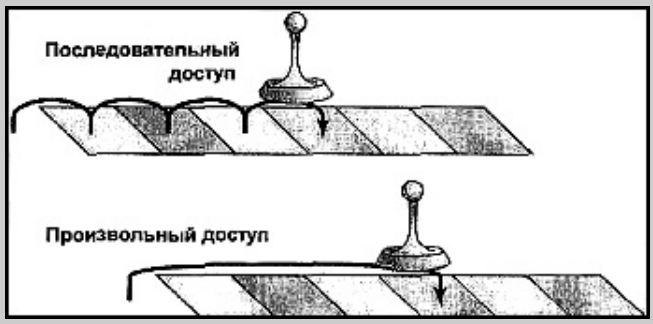
Когда говорят "носители архивной информации", то первое, что подразумевают под этими словами — накопители на магнитной ленте. Имеется множество доводов в их пользу: магнитные ленты сохраняют большой объем данных, они дешевы и, что самое главное, их применение предусмотрено в большинстве утилит архивирования. Однако не во всех программах архивирования предусмотрена поддержка всех типов накопителей на магнитной ленте (далее в этой главе будут описаны некоторые типы). Следует также учесть, что невозможно удовлетворительно решить задачи архивирования, если накопитель медленно записывает и считывает данные. К тому же ленты очень чувствительны к воздействию окружающей среды, например, к высокой температуре. Но их достоинства в большинстве случаев перевешивают недостатки, и сегодня применение магнитных лент является самым популярным способом решения проблемы архивирования.

Если у вас уже есть определенный опыт использования программных средств архивирования, то вы, вероятно, знаете, что архивирование представляет собой двухэтапный процесс: сначала данные объединяются в один каталог, а затем каталог копируется на ленту. Почему же нельзя сделать все это за один этап? Недостатком некоторых технологий архивирования на магнитной ленте, называемых DAT (Digital Audio Tape — цифровая магнитная аудиолента), является невысокая эффективность работы с небольшими файлами, поскольку каждая хранимая на ленте единица данных должна иметь заголовок. Поэтому очень важно скопировать на ленту информацию в виде одного крупного набора данных, вместо целой "охапки" файлов. В противном случае большая часть пространства на ленте будет потеряна. По этой же причине утилиты архивирования создают каталоги данных и далее записывают именно эти каталоги вместо записи данных непосредственно на ленту.

Магнитные ленты могут иметь различные, взаимно несовместимые форматы, для работы с которыми требуются специально спроектированные накопители. Вообще, накопитель на магнитной ленте предназначен для копирования данных с жесткого диска на ленту. Большинство утилит для архивирования на магнитную ленту могут использовать различные алгоритмы сжатия, увеличивающие объем информации, записываемой на ленту, и ускоряющие запись. Единственным недостатком сжатия могут оказаться сложности с поиском содержимого на ленте.

Почему ленточный накопитель работает медленнее, чем жёсткий диск

Одна из самых важных причин, почему вы никогда не увидите ленточный накопитель на месте жёсткого диска, - скорость работы. Данные, для чтения которых с жёсткого диска требуются считанные микросекунды, с магнитной ленты будут считываться значительно дольше. Это различие напрямую связано со способом записи данных на ленту или диск.



Диски являются устройствами с *произвольным доступом*. Это значит, что к данным, расположенным в различных местах, обратиться одинаково легко, и для обращения к ним не требуется придерживаться определённого порядка. Головка диска может перемещаться к позициям A, D, Z, L на диске и не должна обращаться к ним в каком-либо порядке или проходить через B и C на пути к позиции D. Чем ближе позиции друг к другу, тем быстрее диск сможет к ним обратиться, но порядок, в котором эти позиции расположены, не влияет на время доступа.

Накопители же на магнитной ленте, наоборот, являются устройствами с *последовательным доступом*. Они считывают данные в том порядке, в котором те записаны на ленту. Более того, для достижения какой-либо позиции на диске на своём пути они должны пройти через всю последовательность промежуточных позиций.

Предупреждение

Многие производители оборудования указывают емкость магнитной ленты в соответствии с коэффициентом сжатия 2:1, так что лента емкостью в 1 Гбайт для несжатых данных будет рекламироваться как лента емкостью 2 Гбайт. Как вы, вероятно, знаете, степень сжатия, как правило, зависит от типа данных, с которыми вы работаете, поэтому можно получить большую степень сжатия для данных одного типа и нулевую - для других. Ленту следует выбирать, ориентируясь на объем несжатых данных. Следуя этому правилу, вы будете приятно удивлены внезапно увеличившейся емкостью ленты, вместо того чтобы раздражаться из-за невозможности записать на нее так много, как хотелось.

Поскольку емкость жестких дисков возрастает, емкость носителей архивной информации должна возрастать вслед за ними. Дискеты можно использовать для архивирования информации с жесткого диска емкостью 20 Мбайт, но невозможно — с диска емкостью 500 Мбайт. В этом случае лучше воспользоваться магнитной лентой емкостью 40 Мбайт. Емкость ленты можно увеличить тремя способами.

- Увеличить длину ленты.
- Увеличить ширину ленты.
- Увеличить плотность записи.

Рассмотрим некоторые наиболее широко используемые типы лент, чтобы узнать, насколько они соответствуют потребностям пользователей с точки зрения увеличения плотности записи и как это, с другой стороны, влияет на производительность накопителя.

Кассеты QIC (Quarter-Inch Cartridge — 1/4-дюймовая кассета). Применение термина QIC здесь несколько некорректно, поскольку в современных кассетах могут использоваться ленты как шириной 0,25, так и 0,315 дюйма. Основные отличия между различными модификациями кассет QIC заключаются в способе размещения данных на ленте и в траектории движения ленты внутри корпуса кассеты.

В настоящее время имеется три основных типа кассет QIC.

- Travan.
- QIC-Wide.
- QIC-Ex.

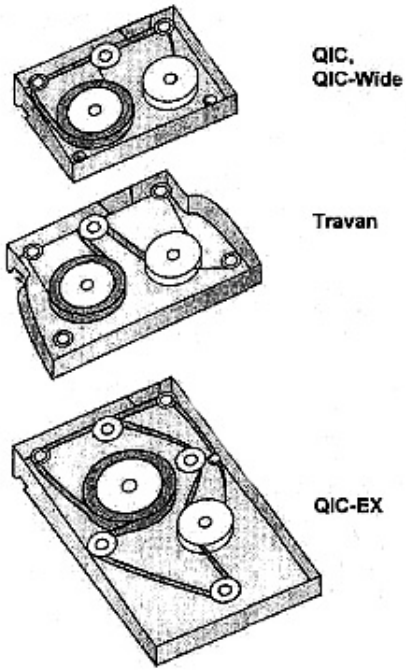


Рис. 8.2. Кассеты QIC различаются траекторией движения ленты, а не только ее шириной

В кассете Travan (базовый формат QIC), разработанной фирмой Imation Enterprises, используют улучшенную ленту шириной 0,315 дюйма, что позволяет варьировать емкость кассеты от 400 Мбайт до 10 Гбайт. В кассетах QIC-Wide используют ленты того же типа, что и в QIC, но большей ширины, что позволяет организовать на ней больше дорожек для записи и тем самым увеличить емкость. В кассетах QIC-Ex также используют ленты QIC, но большей длины. Соответственно, и кассета стала больше. Лента в кассете QIC-Ex может быть шириной как 0,25, так и 0,315 дюйма.

Кассеты QIC, вероятно, являются самыми распространенными. Они имеют различную емкостью (от 40 Мбайт до 20 Гбайт), хотя те кассеты, которые продаются сегодня, в основном имеют емкость не более 4 Гбайт (без учета сжатия). QIC популярны по нескольким причинам. Во-первых, накопители на магнитной ленте работают с ними сравнительно быстро, Во-вторых, в накопителях приняты меры для обеспечения обратной совместимости. Накопитель, созданный в соответствии с последними требованиями, часто может читать и иногда даже записывать на старые кассеты. Накопители Travan, например, могут

работать с лентами шириной 0,315 дюйма в кассетах любого типа. В-третьих, накопители QIC и их кассеты являются наиболее дешевыми из всех имеющихся в продаже устройств (для вновь создаваемых локальных сетей это является основным преимуществом).

Кассеты DLT (Digital Linear Tape — магнитная лента **с цифровой линейной записью).** Кассеты DLT, изображенные на рис. 8.3, первоначально были разработаны фирмой Digital Corporation для компьютеров VAX, но с тех пор стали широко использоваться в компьютерах PC для архивирования. Их емкость весьма велика (до 35 Гбайт) и поскольку в них используется лента шириной до 0,5 дюйма, эта технология обеспечивает высокую скорость переноса данных. DLT-кассеты не так популярны, как например, QIC или DAT, но они подходят для компьютеров крупных локальных сетей.

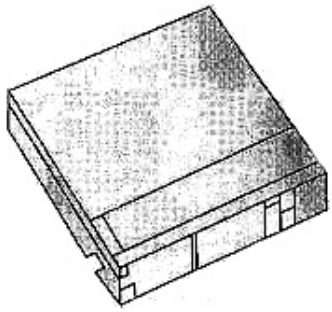


Рис. 8.3. Кассеты DLT

Кассеты DAT (Digital Audio Tape — цифровая магнитная аудиолента). Кассеты DAT не слишком пригодны для архивирования. Они представляют собой кассеты с лентой шириной 4 мм. Запись данных выполняется и соответствии со стандартом DDS (Digital Data Storage — хранение цифровых данных). Емкость кассет зависит от используемого стандарта DDS: стандарт DDS предусматривает запись несжатых данных объемом до 2; DDS-2 — до 4; DDS-3 -до 12 Гбайт. Кассета DAT с лентой шириной 4 мм изображена на рис. 8.4.

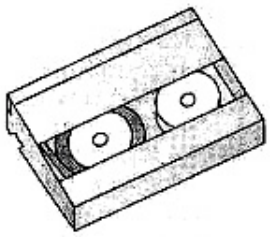


Рис. 8.4. Кассета DAT напоминает обычную аудиокассету

Технология записи DAT до некоторой степени аналогична записи видеоинформации с точки зрения максимального использования пространства для хранения данных на каждой ленте. Вместо использования неподвижных головок, как это делается в QIC-совместимых накопителях, в накопителях DAT используется так называемый *механизм наклонной развертки (helical scan mechanism),* который извлекает ленту из кассеты и перемещает ее относительно записывающей головки под некоторым углом.

Зачем все это делается? В любом случае, при архивировании данные записываются на ленту в виде последовательности полосок (strips) или дорожек. В кассетах QIC и DLT эти полоски образуют параллельные линии вдоль всей длины ленты. Но вспомните, что одно из ограничений, налагаемых на скорость передачи данных кабеля, — ограничение "плотности" передаваемой информации — связано с тем, что между двумя не экранированными близко расположенными параллельными проводниками возникают взаим-

ные помехи, приводящие к повреждению данных. То же самое справедливо для расположенных поблизости цепочек записей данных - они "портят" друг друга, если плотность записи слишком велика.

Для устранения повреждений данных можно либо настолько уменьшить ширину дорожек, чтобы они не воздействовали друг на друга слишком сильно либо с этой же целью их можно соответствующим образом упорядочить. В технологии DAT применяют второй способ. Проблема решается с помощью приема, используемого в кабелях типа "витая пара". Дорожки записей на ленте DAT не параллельны друг другу, и все они расположены под углом к продольной оси ленты. Угол наклона каждой полоски немного отличается от остальных, что снижает вероятность их взаимодействия друг с другом. Для дополнительной защиты данных при записи применяют два набора головок. Один набор записывает данные, а другой, головки которого расположены под углом 90 градусов к записывающим головкам, — читает их сразу же после записи, контролируя корректность операции. Если прочитанные данные не соответствуют записанным, то они могут быть немедленно перезаписаны. Далее процедура записи и проверки повторяется до тех пор, пока не будут правильно считаны записанные данные. Практически это означает, что при записи на ленту DAT данные могут быть упакованы очень плотно, без всякого повреждения. Такой метод отличается высокой емкостью хранения информации.

Однако описанный выше метод записи данных имеет и некоторые недостатки. Во-первых, запись выполняется медленнее, поскольку для ее верификации требуется дополнительное время. Во-вторых, головки накопителей DAT изнашиваются быстрее, чем накопителей других типов, поскольку они вращаются. В-третьих, технология DAT предполагает использование дорогостоящих двигателей (которые не требуются в накопителях с неподвижными головками), а это увеличивает общую стоимость устройства.

Технология Exabyte (8 мм). В технологии Exabyte используется принцип, аналогичный применяемому в DAT для создания носителей с высокой плотностью записи. Запись данных также производится на наклонно расположенные дорожки (треки) на ленте. Главное отличие между этими двумя технологиями заключается в размере ленты (как вы уже догадались, в ней используется лента шириной 8 мм вместо 4 мм, что означает большую ёмкость лент), а также в величине, угла, под которым расположены контролирующие головки - 221 градус вместо 90. Поэтому кассеты Exabyte (рис. 8.5) имеют более высокую емкость по сравнению с кассетами DAT.

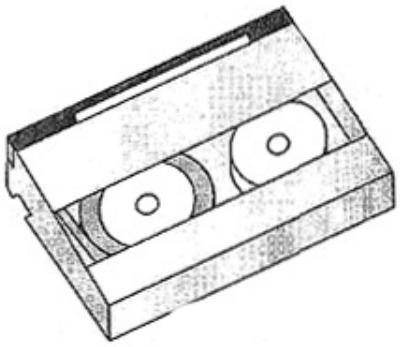


Рис. 8.5. Кассета Exabyte выглядит как увеличенная кассета DAT

Выбор типа ленты. Поскольку кассеты QIC имеют ограниченную ёмкость, но, в то же время, стоят недорого, они прекрасно подходят для использования в локальных сетях небольших и средних размеров или даже для архивирования данных в отдельных компьютерах. Хотя накопители, рассчитанные на использование кассет DAT медленнее накопителей QIC, они обеспечивают удобный и надежный способ архивирования информации в сетях среднего размера. В крупных сетях рекомендуется использовать технологии DLT

или Exabyte. Заметим: фактическая емкость ленты (кассеты) может не соответствовать рекламируемой, что следует учитывать при выборе средств архивирования на магнитной ленте.

Что можно сказать о различных типах накопителей? Накопители на магнитных лентах поставляются с интерфейсами трех типов.

- Параллельный интерфейс (Centronix).
- IDE.
- SCSI.

Для архивирования информации с жестких дисков сервера рекомендуем использовать интерфейс SCSI. Параллельные порты работают медленно, что не позволяет использовать их для архивирования сколько-нибудь "серьезного" объема данных. Интерфейс SCSI предпочтительнее EIDE-интерфейса с точки зрения использования в сервере, поскольку в SCSI-системах используется более эффективный метод управления операциями чтения и записи данных.

Оптические диски

Тем, кто располагает значительными средствами, и (или) тем, кому необходимо распространять архивируемую информацию, использование перезаписываемых компакт-дисков может предоставить еще одну удобную возможность решить проблему архивирования. Записывающее устройство выглядит примерно так же, как и обычное устройство считывания CD-ROM, отличаясь от последних только способностью производить запись на специальный компакт-диск.

Подобно всем другим устройствам CD-ROM, компьютер рассматривает устройство для записи на компакт-диск точно так же, как жесткий или гибкий диски. Вам не нужно специально организовывать (каталогизировать) данные перед их записью на компакт-диск, а достаточно скопировать на него требуемые файлы или каталоги.

Примечание

Описываемые здесь оптические диски не обязательно являются привычными нам компакт-дисками. Обычные компакт-диски не используются вовсе, поскольку они имеют маленькую емкость и слишком медленно работают, чтобы их можно было эффективно использовать в качестве удобных носителей архивируемой информации.

Записываемые компакт-диски имеют два недостатка. Первый: устройства для записи весьма дороги, хотя компакт-диски для них сравнительно дешевы. Второй: наибольшая емкость этих дисков, встречавшаяся автору книги, составляет 5 Гбайт. Это не так мало, но уже сравнимо с емкостью современных жестких дисков, что в ряде случаев может оказаться недостаточным.

Съемные диски

Съемные диски — еще один носитель архивируемой информации, который можно использовать для сохранения и распространения файлов. Они не обладают такими возможностями, как оптические. В наши дни почти каждый современный компьютер имеет устройство для считывания дисков CD-ROM, но далеко не каждый — устройства для работы с дисками Zip, Jaz или что-нибудь подобное. Однако такие устройства дешевы и удобны.

На рынке доминируют два основных типа устройств со съемными дисками: Zip фирмы Iomega и Jaz. Во-первых, используются диски объёмом до 250 Мбайт, что совершенно недостаточно для архивирования информации с жестких дисков сервера. Во-вторых, применяются диски емкостью от 1 до 2 Гбайт (в зависимости от используемой кассеты). Они несколько лучше подходят для работы, особенно при ежедневном архивировании. Их, впрочем, не следует использовать в больших локальных сетях, в которых лучше воспользоваться ленточными накопителями Exabyte или DLT, или оптическими накопителями, но они вполне пригодны для небольших локальных сетей или для архивирования информации клиентных компьютеров.

Серверы печати

Другим типом сервера, который можно обнаружить почти во всех локальных сетях, является сервер, предоставляющий услуги печати. Суть его применения очень проста: вы подключаете принтер к определенному серверу, устанавливаете соответствующие драйверы и используете принтер совместно со всей сетью. Все те, кто хочет использовать этот принтер, должны установить на своих рабочих станциях соответствующие средства поддержки принтера. Состав набора этих средств зависит от операционной системы. Например, в компьютерах, работающих под управлением Windows 3.1 для связи с сервером печати необходимо загрузить все драйверы на локальных машинах. А вот в компьютерах, работающих под управлением Windows NT, для связи с сервером печати этого делать не следует — все требуемые драйверы будут загружены автоматически.

Если сервер печати будет использоваться только как сервер печати, то всё, что для него требуется, — это хороший принтер. Размер дискового пространства не так важен, поскольку на диске должно храниться: операционная система, соответствующие драйверы и буферные файлы. В большинстве локальных сетей для управления всеми задачами печати на сервере достаточно иметь единственный диск IDE емкостью примерно 500 Мбайт. Поскольку сервер печати может использовать собственную память для расширения памяти принтера, то следует предусмотреть некоторое количество оперативной памяти, но ее требуется не так много, как, например, для сервера приложений. Даже скорость работы процессора не является жизненно важной для работы хорошего сервера печати, поэтому все те, кто не смог продать или не отдал даром детали от компьютера с 486 процессором, смогут сделать себе хороший сервер печати.

Как подсоединить принтер к сети

Итак, у вас есть принтер и сеть. Как же подсоединить их друг к другу? Это можно сделать тремя способами.

- Подключить принтер к уже имеющемуся обычному компьютеру.
- Присоединить принтер к серверу печати.
- Использовать сетевой принтер, который можно подсоединить к сети напрямую.

Приступим к описанию этих способов.

Печать с компьютера

Данная конфигурация используется весьма широко, особенно в небольших (или только что созданных) локальных сетях. Сегодня очень легко приобрести недорогой ПК,

а, как вы помните, серверам печати и не требуется больших вычислительных ресурсов, чтобы они могли хорошо выполнять свою работу. Наиболее узким местом при печати является кабель параллельного интерфейса (более подробно об этом будет сказано чуть ниже, при рассмотрении сетевых принтеров), поэтому даже компьютеры с процессором Intel 386 смогут надежно выполнять эту работу, так что вы можете использовать даже один из таких устаревших компьютеров (рис. 8.6). До тех пор пока ПК исправно функционирует и в состоянии общаться с сетью, он может работать в качестве сервера печати.

Старый 486-й компьютер можно использовать как сервер печати

Рис. 8.6. Возьмите 486 компьютер и используйте его в качестве сервера печати

Если же вы отказываетесь от такого варианта, то *не следует* подсоединять принтер к сетевому клиентному компьютеру. Конечно, отдельные задания на печать не смогут нормально загрузить процессор или потребовать больших объемов памяти, но задания на печать от всей сети — смогут. Тщательно оцените количество ожидаемых заданий на печать и примерный объем работы, который придется выполнять на таком ПК, перед тем как делать его сетевым сервером печати.

Печать с сервера печати

Отнюдь не все серверы печати — вышедшие из употребления ПК. Среди них имеются устройства, представляющие собой настоящие сетевые серверы печати, которые можно подключить к сети и использовать как одно устройство для предоставления сетевого доступа к нескольким принтерам (рис. 8.7). Управление таким устройством осуществляется с сетевого компьютера.

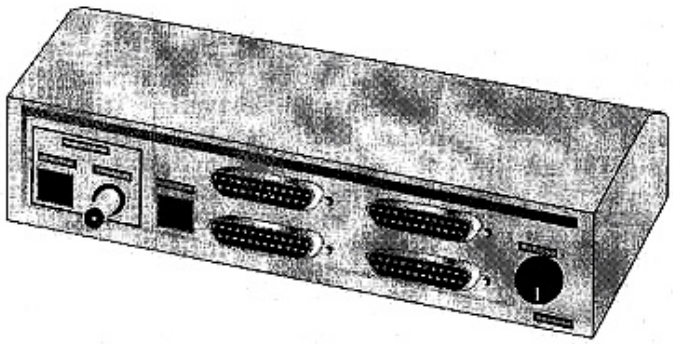


Рис. 8.7. Серверы печати могут обеспечить удобный способ подключения нескольких принтеров к одному компьютеру

Зачем же нужно использовать сервер печати вместо компьютера с подсоединенным принтером? Одним из соображений в пользу такого варианта является гибкость в работе. Такие устройства позволяют подсоединять два, три и даже пять принтеров к сети в одном отдельном месте вместо одного или двух — при использовании обычного ПК. Другим соображением является стоимость. Даже приняв во внимание падение цен на ПК, приобре-

тение сервера печати обойдется намного дешевле того, во что вам обойдется покупка нового ПК, особенно если у вас в данный момент отсутствуют доступные для использования резервные ПК.

Сетевые принтеры

Ранее уже указывалось, что узким местом при выполнении заданий печати оказывается вовсе не сеть, поставляющая задания на печать, или что-либо другое, связанное с принтером или соединенным с ним компьютером - в действительности им является кабель параллельного интерфейса (parallel cable). (Или, что еще хуже, кабель последовательного интерфейса (serial cable). Надеюсь, вам не приходилось печатать через сеть на принтере с последовательным интерфейсом.) Применение сетевого принтера позволяет обойти эту проблему, поскольку в нем вообще нет таких портов (и кабелей). Сетевой принтер напрямую подключается к сети с помощью соединения со скоростью 100 Мбит/с, которого вполне достаточно для решения всех задач (рис. 8.8).

Рис. 8.8. Подключение принтера непосредственно к сети устраняет задержку, возникающую из-за медленного параллельного интерфейса

Такое техническое решение имеет несколько последствий, которые следует принять во внимание. Во-первых, не все принтеры допускают прямое подключение к сети. Вам потребуется принтер, имеющий разъем для подключения сетевой платы. Во-вторых, для печати на сетевом принтере необходим специальный транспортный протокол (например, DLC) для связи с сетью. Альтернативой специальному протоколу печати является система, посылающая задания на печать с помощью протокола TCP/IP или аналогичного ему. Наконец, поскольку сетевые принтеры не используют ПК или сервер печати, к которым можно было бы обратиться "за помощью", задания на печать не могут поддерживаться памятью (дисковой или оперативной) и передаваться на принтер для обработки. В сетевом принтере требуется такая память, объема которой будет достаточно для полной обработки поступающих заданий на печать. Рекомендуем установить в каждом сетевом принтере память объемом минимум 16 Мбайт.

Требования к принтеру, установленному в локальной сети

Используете ли вы сервер печати (построенный на базе ПК) или какой-либо другой "черный ящик", производительность его в основном будет зависеть от возможностей присоединенного к нему принтера. В таком случае, что же делает хороший принтер хорошим? Хороший принтер локальной сети должен быть:

- быстрым;
- с гибкими возможностями;
- надежным.

Давайте посмотрим, что все это значит на практике.

Требования к скорости печати

Скорость для принтеров в основном выражается в количестве страниц, печатаемых за минуту (ppm — page per minute). Она зависит не от объема памяти принтера, а от того, как он устроен — как быстро он может переносить изображение на бумагу и прокручивать эту бумагу через себя. В настоящее время приличный принтер позволяет печатать черно-белые копии со скоростью не менее 10 стр./мин и не более 24 стр./мин.

Если не считать по-настоящему высококлассных принтеров, стоящих тысячи долларов, то цветная печать требует значительных затрат времени, поскольку черно-белая копия печатается за один проход, в то время как цветная — три прохода. Однако вы сможете купить цветной и недорогой принтер, который сможет выполнять цветную печать со скоростью 3—4 стр./мин.

Примечание

Скорость работы принтеров растет прямо на глазах, так что не удивляйтесь, если за то время, пока вы читаете эту книгу, появятся более скоростные. Перед покупкой принтера всегда следует поискать что-нибудь получше.

Всё для всех

Вероятно, в своей практической деятельности вам придется встретиться с набором претензий, предъявляемых к печати клиентами сети. Дизайнеры хотят распечатывать цветные изображения на прозрачных пленках; для печати административных документов необходим только черно-белый принтер; сотрудники отдела маркетинга иногда нуждаются в цветной печати на бумаге, а иногда им достаточно черно-белой — для пробной печати черновика документа перед медленным и дорогостоящим выводом его цветной копии.

Что можно тут сделать? Во-первых, вы должны иметь хотя бы один принтер, печатающий как цветные, так и черно-белые документы (например, струйный). Если вас не беспокоит необходимость периодического переключения картриджей, такое решение вполне приемлемо. Для тех же, кто работает в серьезных сетях, наличие более одного принтера может быть источником сложных проблем.

Если вы делаете все работы, применяя одни и те же цвета, но на разной бумаге (в зависимости от требований к качеству продукции), подумайте о приобретении принтера, имеющего несколько лотков подачи бумаги. В зависимости от конфигурации можно использовать одни лотки для дешевой бумаги (черновики), другие - для более дорогой (официальные документы), а также выделить отдельный лоток для пленок или этикеток. Конечно, при этом должна быть предусмотрена возможность программного переключения на различные лотки с бумагой в соответствии с тем, что требуется в каждом отдельном случае. Как бы то ни было, в крупных сетях, в которых клиенту нелегко получить доступ к принтеру для смены бумаги, использование нескольких лотков для нее поможет сохранить много времени.

Несколько практических советов

В наши дни широко используют лазерные принтеры, являющиеся наилучшими устройствами для печати с точки зрения надежности. Они имеют очень небольшое число

движущихся частей, так что если вы предпримете меры предосторожности, то все будет в порядке.

Во-первых, предохраняйте бумагу от скручивания (коробления) во время хранения. Храните ящики с бумагой плотно закрытыми и в сухом месте, чтобы бумага не сморщилась. Неровная бумага заедает в принтере, что является простой, но весьма досадной проблемой, для решения которой приходится извлекать из механизма транспортировки застрявший там обрывок бумаги.

Подумайте о выборе места подключения принтера. Чтобы не мешать работе ПК, не подключайте принтер и компьютер к одной розетке (если это возможно), поскольку лазерный принтер генерирует мощные электромагнитные помехи, ухудшающие качество электроэнергии. Кроме того, для нормальной работы самого принтера (и сохранения нервной системы всех тех, кто посылает ему задания на печать из удаленного места в здании) не подключайте его к коммутируемой линии электропитания, которая может быть обесточена, если кто-либо выключит свет в комнате.

Используйте для принтера короткие кабели (не длиннее 6 футов (2 метра)), поскольку длинные кабели будут хорошим приемником помех. Если вы будете покупать только стандартные кабели, это будет нетрудно сделать.

Наконец, старайтесь приобретать для принтера двунаправленные кабели (с полным комплектом проводников), поскольку тогда при возникновении каких-либо проблем в работе принтера вы сможете получить о них более достоверные и полные сообщения. Простые кабели для принтера передают ограниченное количество сообщений (например, о заедании бумаги), но при этом нет информации о причине (пребывание принтера в автономном режиме, отсутствие бумаги или какие-либо другие проблемы).

Память принтера

Объём памяти, установленной на принтере, не влияет напрямую на скорость или надёжность работы. Однако наличие памяти достаточного размера экономит много времени, которое может быть потрачено на перепечатку документов и ограничений, налагаемых на объём файлов подкачки. Память достаточного объёма – крайне необходимое условие, приобретающее большое значение по мере усложнения документов. Безусловно, при печати некоторых документов на принтере, подключенном к ПК, можно задействовать некоторую часть его оперативную память. Но рано или поздно при выполнении какого-либо задания возникает необходимость сохранить одну или две страницы в памяти принтера. (Если вы используете принтер, напрямую подсоединённый к сети или к серверу печати, то потребуется установить память, достаточную для управления любым заданием.)

Когда какое-либо задание на печать или его часть сохраняется в памяти принтера, то все данные, необходимые для выполнения этого задания, также должны быть записаны в эту же память. Это значит, что описание каждого шрифта (начертание и размер), рисунки, линии и другие компоненты страницы должны быть сохранены в памяти. И они не стираются из памяти по завершении печати этой страницы, т.е. происходит накопление информации. Чем выше требования к печатаемому документу в каждом отдельном задании на печать, тем больше памяти для них необходимо. В противном случае придётся затратить много времени и бумаги на перепечатку документов, подготовленных настольной издательской системой, которые будут печататься с использованием шрифта Courier размером 12 пунктов и с большими буквами X в тех местах, где должны появиться рисунки. Имеется несколько способов обойти эту проблему, но наилучшим решением будет всё-таки установка памяти достаточного размера.

Работа с принтером

Когда вы начинаете работать с принтером, учтите, что вовсе необязательно работать с одним принтером, пользоваться одним общим именем и одним набором разрешений доступа. В. зависимости от используемой операционной системы (или в некоторых случаях – от свойств самого принтера) вы можете сделать так, что один принтер будет выглядеть для пользователя как два разных. Можете полностью скрыть некоторые принтеры от всех пользователей сети, но при этом оставить их доступными для избранных клиентов. Можете объединить несколько принтеров вместе, создав один (логический) принтер.

Создание набора индивидуальных пользовательских характеристик (профилей) для принтера

Вы можете организовать совместный доступ к одному принтеру в виде нескольких отдельных принтеров, создавая несколько экземпляров объекта (принтера) и устанавливая для них различные разрешения доступа. Например, из соображений безопасности, можно так сконфигурировать принтер, что он будет доступен только несколько часов в течение дня (возможно, нежелательно, если кто-то хочет напечатать документ после 6 часов вечера). Если же какой-либо клиент заслуживает такого "доверия", то ему будет разрешен доступ к принтеру в сверхурочное время, что можно сделать, не идя на компромисс при установке разрешений доступа для всех остальных клиентов. Достаточно предоставить совместный доступ к принтеру, но под другим именем (и с другими установками системы защиты, предотвращающими несанкционированный доступ) и с иными ограничениями на время доступа к данному ресурсу.

Маскирование совместно используемых принтеров

Любая "уважающая себя" операционная система содержит некоторый набор "защитных средств", позволяющих задавать пароль или устанавливать разрешения на доступ пользователей к совместно используемым устройствам или файлам. Принтеры - не исключение. При совместном использовании принтера со "скрытым" именем (в сетях Microsoft, например, вы можете присвоить принтеру такое сетевое имя, в котором самым последним символом будет знак доллара ($)) он не будет отображаться ни в одном из списков просмотра.

Комбинированные наборы принтеров

Если к какому-либо принтеру поступает слишком много заданий, можно избежать перегрузки, перенаправив их избыток на другой подобный принтер. Для этого требуется всего лишь приобрести второй принтер. Заданные же для старого принтера значения параметров желательно не изменять (если это возможно), поскольку всякие изменения могут только запутать пользователей.

Одним из способов реализации такого метода является создание *пула принтеров (printer pooling):* два одинаково сконфигурированных принтера объединяются под одним именем. Когда пользователь отправляет задание на печать какому-либо принтеру (например, с логическим именем LaserJet), это задание может быть выполнено на одном из двух (и более) принтеров в зависимости от того, который из них был менее занят в момент по-

ступлении запроса. Этот процесс "прозрачен" для пользователя, за исключением, может быть, сведений о времени завершения работы. Если вы будете держать принтеры одного пула рядом друг с другом и сообщите пользователям, что их работа может быть выполнена на одном из них, то сможете избежать большинства конфликтов, возникающих при печати.

Коммуникационные серверы

Потребность в организации связей офиса с внешним миром возникла не сегодня. Для передачи документов вот уже около десяти лет применяется факс. Соответствующие средства существовали и ранее (например, телетайп), но только десять лет назад люди перестали спрашивать, есть ли у вас телекс, и стали спрашивать: "Какой у вас номер факса?". Точно так же и электронная почта из эпизодически используемой превратилась в важнейшее средство корпоративной связи. Фактически в некоторых областях она стала более популярным средством, чем передача факсов.

Отдельные пользователи могут получать оперативный доступ к сети с помощью специальных средств коммутируемого доступа. Однако такие средства непрактично предоставлять для больших групп людей (которым для работы требуется факс или электронная почта), находящихся в одном месте.

- Экономически невыгодно покупать модем для каждого ПК и подводить соответствующую линию связи к каждому пользователю.
- Расточительно распределять выделенные средства связи поровну между всеми пользователями. Некоторым из них факс необходим 20 раз и день, а другим достаточно обращаться к электронной почте раз в неделю.
- Наличие незащищенной линии связи с Internet подвергает риску всю офисную систему защиты сети. Кроме того, чем больше открытых клиентных связей, тем больше лазеек, которые необходимо закрыть, чтобы они не были использованы непорядочными людьми.

Как решить эти проблемы? Необходимо организовать пул совместно используемых модемов, к которому смогут подключаться пользователи сети, или (в качестве альтернативы) установить прокси-сервер, который обеспечит доступ к локальной сети через единственное модемное соединение.

Модемный пул

Одним из способов решения задачи обеспечения всех сетевых пользователей средствами коммутируемого доступа является совместное использование установленного на сервере модема. При этом в случае, если пользователю потребуется проверить свою электронную почту или произвести поиск в Web, он должен подсоединиться к совместно используемому модему и набрать внешний номер, что несколько напоминает совместное использование принтера или жесткого диска. Для небольших сетей с незначительным трафиком этот метод может быть пригоден, но для крупных сетей, или таких, в которых сосуществуют несколько серьезных пользователей Internet, борющихся за использование модемного времени, следует ожидать возникновения конфликтов.

Но не возникнут ли подобные проблемы при одновременном подключении нескольких пользователей к нескольким модемам на сервере? Нет, поскольку в данном случае ра-

бота модемов отличается от совместного использования принтеров. При работе с совместно используемыми принтерами можно установить в очередь задание на печать докладной записки одного пользователя и в то же время продолжать печатать черновик ежегодного отчета. В отличие от них, если модем занят, то он занят. Здесь необходим метод, который будет обеспечивать доступ к нескольким (возможно не ко всем) модемам, но запрос на установление соединения всегда будет направляться к тому из них, кто в данный момент свободен. Это метод используется при создании *модемного пула (modem pooling).*

В модемном пуле применяется метод совместного использования нескольких модемов всей сетью, при котором они представляются пользователям как бы единым устройством. Когда пользователь сети подключается к модему в пуле, то для установления текущего соединения будет выбран любой из свободных модемов. При каждом последующем подключении состав используемых модемов будет зависеть от того, какие модемы в данный момент времени заняты. Однако внешне вся эта деятельность для пользователя незаметна - все, что он знает, это то, что он установил удаленное подсоединение. И прекрасно, потому что это все, что ему *нужно* знать.

В большинстве компьютеров есть один или два порта связи, и один из них, скорее всего, уже использован для подключения мыши. Поэтому подсоединить эти модемы к компьютеру Так, как подключают один модем (через свободный последовательный порт) нельзя. Для коммуникационных серверов с модемным пулом предпочтительно использовать плату расширения, содержащую несколько COM-портов. Пример такого подключения показан на рис. 8.9.

Поскольку скорость работы сети значительно выше скорости любого из модемов (56 Кбайт/с по сравнению с 100 Мбайт/с), связывающиеся через сеть клиенты не почувствуют никакой задержки, которую они замечали при подсоединении через коммуникационный сервер.

Единственный недостаток модемного пула заключается в том, что каждый модем в пуле должен быть идентичен остальным - иметь одинаковые скорость работы, драйвер и т. д. Иначе могут возникнуть проблемы, поскольку клиентный компьютер не будет знать, как ему связываться с модемом. Если к мультипортовой плате подключены разнотипные модемы, то объедините модемы каждого типа в отдельный пул.

Какие аппаратные ресурсы необходимы для работы нескольких модемов? Конечно память. Неплохо также иметь достаточное количество линий связи. Необязательно, чтобы каждый модем имел одну линию связи, но их должно быть столько, чтобы каждый клиент, нашедший свободный модем, мог установить нужное ему удаленное соединение. Поскольку каждый модем подключен к своей собственной линии связи, то скорость работы модема зависит от характеристик соединения, а не от числа одновременно подключившихся пользователей: они работают без совместного использования полосы пропускания.

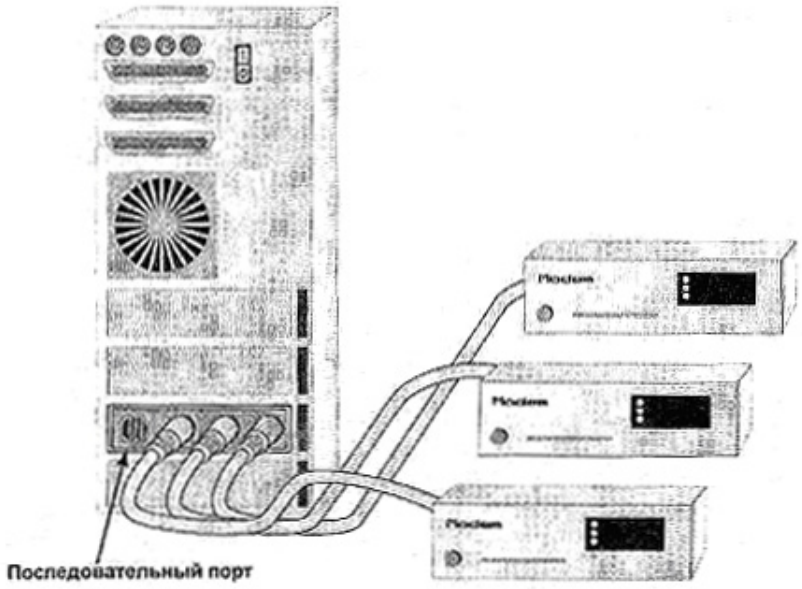


Рис. 8.9. Подключение нескольких модемов к одному компьютеру

Что касается программного обеспечения, то на сервере должны быть установлены некоторые совместно используемые программные средства (система Windows, например, не содержит этих средств в стандартной конфигурации). Каждому клиенту требуется разрешение на клиентный доступ к совместно используемым модемам. Какие протоколы должны использовать клиенты - зависит от протоколов, применяемых в сети, с которой они устанавливают удаленное соединение. Если модемы предназначены для доступа к Internet, то клиентам потребуется установить протокол TCP/IP и настроить его точно так же, как если бы он предназначался для прямого подключения к сети.

Прокси-серверы

Прокси-сервером называется компьютер, содержащий программное обеспечение, позволяющее ему работать в качестве портала (portal) между сетевыми клиентами и сетью типа Internet. Имеющееся программное обеспечение для прокси-серверов различных типов предоставляет множество возможностей, например таких, как установка системы защиты и настройка кэш-памяти серверов. Однако главный принцип остается неизменным, независимым от этих возможностей.

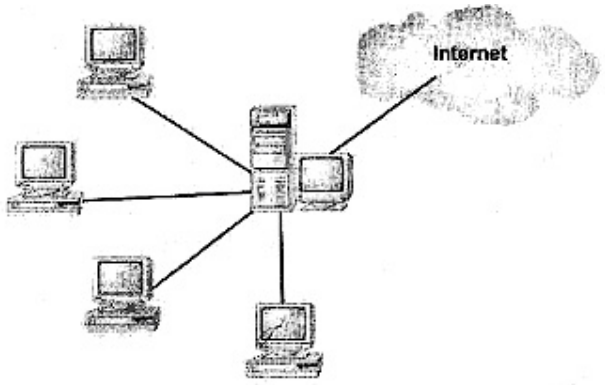


Рис. 8.10. Использование прокси-сервера для обеспечения доступа к другим сетям через центральный узел

Прокси-сервер — это не просто сервер с установленными на нем модемами. Во-первых, поскольку все сетевые клиенты совместно используют единственное соединение, он должен быть в состоянии обеспечить пропускную способность, достаточную для обслуживания работы сетевых пользователей. Во-вторых, кэширование, необходимое при работе с Internet, выполняется на прокси-сервере, поэтому ему требуется жесткий диск и файловая система, ориентированные на работу с большим числом маленьких файлов. Как и любой сервер, он должен иметь достаточный объем памяти.

Тип протокола, используемого в сети с прокси-сервером, зависит от программного обеспечения прокси-сервера. Иногда достаточно, чтобы общий протокол имели клиент и прокси-сервер, а также прокси-сервер и связанная с ним сеть (внешняя). При этом не обязательно, чтобы протокол взаимодействия клиента с сервером был такой же, как протокол взаимодействия сервера с данной сетью. Другими словами, клиент может использовать совместимый с IPX/SPX протокол, в Internet — TCP/IP, но прокси-сервер должен поддерживать TCP/IP и совместимый с IPX/SPX протокол.

Аппаратные средства связи

При выборе типа сети и оборудования для построения своей собственной сети вам потребуется определить одну комбинацию оборудования и программных средств из нескольких доступных. Главным образом имеется в виду способ соединения с внешними сетями: с помощью обычного модема по стандартной телефонной линии, ISDN-соединения или средств, обеспечивающих ретрансляцию кадров. Последние описаны в гл. *6,* так что в этом разделе мы остановимся на двух первых.

Модемы 56 Кбайт/с

Слово модем — аббревиатура словосочетания МОдулятор/ДЕМодулятор. Этим словом обозначают любое устройство для преобразования в компьютере цифровых сигналов в аналоговые, передаваемые по телефонным линиям. И точно так же, как сетевая плата представляет собой устройство, которое делает пригодной для использования компьютерную сеть, модем является устройством, которое делает обычную телефонную линию пригодной для. использования компьютерами в качестве сети.

Путем улучшения алгоритмов сжатия и вследствие возросшего качества телефонных линий скорость работы модемов в последние годы значительно возросла — с 2,4 Кбит/с (80-е гг.) до 56 Кбит/с (90-е гг.).

Как это всегда происходит при появлении новых более скоростных модемов, должно пройти некоторое время, необходимое для внедрения стандартов работы модемов со скоростью 56 Кбит/с. Окончательная версия стандарта V.90 (предусматривающая скорость передачи данных 56 Кбит/с) была не согласована вплоть до февраля 1998 г. Окончательно ее утвердили в сентябре 1998 г. Тем не менее, на момент утверждения было продано множество модемов 56 Кбит/с, и в настоящее время существуют две конкурирующие и взаимно несовместимые технологии: K56Flex (Rockwell/Lucent Technologies) и X2 (US Robotics и частично фирмы 3Com). Поэтому для организации соединения с Internet со скоростью 56 Кбит/с на сервере провайдера должен быть установлен модем на 56 Кбит/с, причем совместимый с вашим модемом.

Что случится с этими технологиями сейчас, после утверждения стандарта V.90? Не следует выбрасывать свой модем, поскольку большинство производителей создали фирменные программные средства обновления, расположенные на соответствующих Web-

узлах. Перед обновлением модема до стандарта,V.90 убедитесь, что ваш провайдер Internet также выполнил обновление к данному стандарту.

Хотя модемы 56 Кбит/с в настоящее время и в самом деле являются самыми быстрыми, из существующих модемов, их название выглядит немного некорректно. Во-первых, скорость передачи данных неодинакова в обоих направлениях: стандарт X2 определяет методы, поддерживающие перенос данных со скоростью до 31,2 Кбит/с при выгрузке (передаче) данных (uploading) и скорость до 56 Кбит/с при их загрузке (приеме) (downloading). Во-вторых, по различным причинам, например, из-за шумов в линии связи, фактически никогда не удается достигнуть скорости 56 Кбит/с в обоих направлениях — скорость передачи данных не превысит 40 Кбит/с.

Примечание

Вследствие ограничений, налагаемых FCC (Federal Communication Commission - Федеральная комиссия связи (США)) на переносимую по линиям связи мощность, модемы 56 Кбит/с не могут переносить данные со скоростью, превышающей 53 Кбит/с. Сейчас идут дискуссии, о возможности обхода данного ограничения, но пока это только дискуссии.

Теперь осталось только сказать, что модем 56 Кбит/с является недорогим средством для быстрой связи с Internet. Ведущаяся "Война Стандартов" способствует понижению цен на оборудование (по крайней мере, так было в течение 1998 г., но после утверждения стандарта V.90 цены могут стабилизироваться). Стоимость соединения со скоростью 56 Кбит/с с Internet (там, где это возможно) обходится не дороже связи со скоростью 28,8 Кбит/с. Однако с точки зрения скорости это соединение не такое уж быстрое, по сравнению с возможностями других средств, как имеющихся сейчас, так и только-только появившихся на горизонте. Пригодны ли модемы 56 Кбит/с для использования в локальных сетях? Для тех, кто в качестве основного средства корпоративной связи использует модемный пул, модемы 56 Кбит/с — подходящее средство. Тем же, кто желает использовать прокси-сервер и намеревается организовать совместное использование полосы пропускания линии связи, может потребоваться нечто более быстрое, и именно для этого может пригодиться описываемая далее технология.

Цифровая связь с интеграцией услуг (ISDN)

Что может служить альтернативой модемам? Крупные компании со значительными финансовыми ресурсами уже давно пользуются арендованными каналами (высокоскоростными линиями связи, выделенными им для монопольного использования). Такие технические решения работают прекрасно, но имеют один большой недостаток: они весьма дороги.

В середине 90-х гг. возникла и начала развиваться (вначале только в отдельных регионах США) новая технология связи. Ее применение сделало возможной такую связь, при которой, хотя и не предоставлялась выделенная полоса пропускания шириной 1,5 Мбит/с, но *стали* достижимыми скорости свыше 14,4 Кбит/с. Эта технология была более доступной, по крайней мере, для некоторых областей. Речь идет о цифровой связи с интеграцией услуг (ISDN - Integrated Services Digital Network).

Самая простая, магистральная версия ISDN, известная как ISDN с номинальной скоростью (BRI — Basic Rate ISDN), реализуется с помощью трех каналов: двух каналов данных (D — Data) и одного — несущей (B — Bearer), предназначенного для передачи информации о соединении. Два канала D могут использоваться как независимо, для дуплексного (двунаправленного) доступа со скоростью передачи 64 Кбит/с, так и в едином логическом канале со скоростью передачи 128 Кбит/с. За дополнительную плату можно приобрести несколько каналов, получив при этом скорости передачи в 256 Кбит/с или да-

же в 512 Кбит/с. Некоторые устройства ISDN поддерживают сжатие данных, что увеличивает реально достижимую пропускную способность.

Каков путь развития ISDN? Первая реализация ISDN была весьма впечатляющей. Во-первых, такая система обеспечивала весьма быстродействующее соединение (по сравнению с тогдашними модемами). Во-вторых, она предоставляла удобный способ организации связей между удаленными офисами, расположенными хотя и рядом друг с другом, но недостаточно близко для создания обычной локальной сети. Там, где возможно применение ISDN, она обойдется не так дешево, как доступ к Internet, но будет значительно дешевле арендованных линий.

В наши дни технология ISDN еще жива, но ее преимущества стали менее очевидными, чем это было ранее. Во-первых, цена. Телефонные компании более не предоставляют неограниченное по времени соединение. (Ранее это также не всегда было возможно, но иногда такая услуга предоставлялась, если два города, соединенные линией ISDN, были расположены близко друг к другу.) Например, компания Bell Atlantic предоставляла три различные схемы работы, в соответствии с которыми нужно было уплатить за определенное количество часов времени связи, а дополнительное время оплачивалось по повышенному тарифу. Для тех, кто намеревается организовать работающие в течение всего дня связи между офисами или соединения с Internet, это будет достаточно дорого. Это тем более справедливо, если учесть, что при расчете стоимости оплаты сюда относят *все* время работы ISDN, включая телефонные услуги (если вы используете для этого цифровые линии). Вдобавок, помимо оплаты услуг связи, для организации соединения ISDN требуются некоторые дорогостоящие аппаратные средства: адаптер терминала (подобие сетевой платы), который должен входить в состав коммуникационного сервера, а также моста или маршрутизатора для подсоединения к цифровой сети.

Во-вторых, появились и другие средства передачи данных, которые заняли место в промежутке между тем, что может сделать ISDN**,** и тем, что могут предложить средства оперативного доступа. В их число входят кабельные модемы, получающие все более широкое распространение. Многообещающими выглядят также средства ADSL, которые в течение 1999 г. должны стать доступными не только в качестве экспериментальных устройств (ADSL описаны в одном из последующих разделов этой главы). Тем не менее, там, где новые возможности пока еще не стали доступными, средства ISDN вполне жизнеспособны.

Кабельные модемы

Начиная с 1997 г., в отдельных регионах США стала развиваться новая разновидность оперативной связи: кабельные модемы. Возможности высокоскоростных сетей такого типа могут далеко превзойти параметры модемов 56 Кбит/с и даже ISDN. Кабельные модемы - это не совсем то же самое, что классические, они (в зависимости от типа) являются модемами только наполовину. Соединения, реализуемые с помощью кабельных модемов, бывают двух разновидностей: односторонние и двусторонние. Двусторонние модемы фактически вообще не являются модемами, а представляют собой устройства для подсоединения к очень крупной сети Ethernet.

Для создания соединения на основе кабельного модема следует установить в компьютер сетевую плату и проложить кабельный отвод от компьютера к главному магистральному кабелю. При создании однонаправленного соединения, эта сетевая плата и кабель соединяются с помощью обычного модема и телефонной линии связи, а обращение выполняется средствами удаленного доступа. Информация, следующая "вверх по течению" (от ПК к сети), передается со скоростью, задаваемой модемом. Информация, движущаяся "вниз по течению" (от сети к ПК), проходит через магистральный кабель и поэтому здесь достигается скорость передачи, совпадающая со скоростью обмена провайдера с Internet.

При двусторонних соединениях, информация, проходящая в обоих направлениях, передается по кабелю. На рис. 8.11 показаны два типа соединений, реализуемых с помощью кабельного модема:

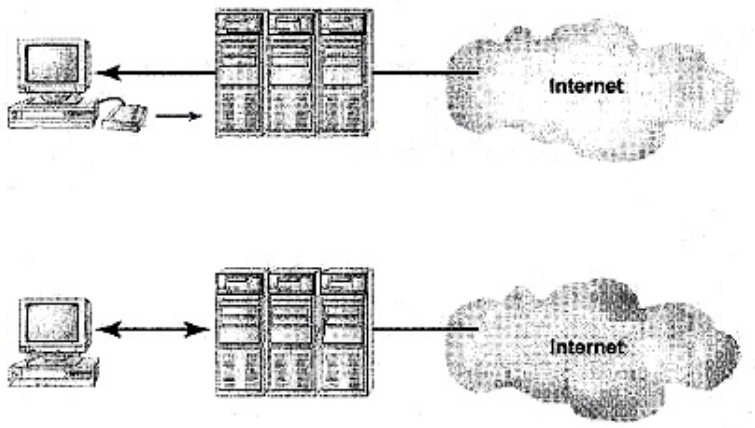


Рис. 8.11. Однонаправленный и двунаправленный кабельные модемы

Хотя однонаправленные кабельные модемы не позволяют достичь быстродействия двунаправленных при передаче данных "вверх по течению", для большинства пользователей это не существенно. Как часто вы выгружаете столько же информации, сколько загружаете? Как правило, средний объем одного письма, пересылаемого по электронной почте, не превышает 1 Мбайт и его легко передать с помощью модема на скорости 36,6 Мбит/с, А вот соединение с Internet по большей части используется для загрузки просматриваемых Web-страниц или для получения электронной почты. Поэтому если вы планируете передавать большой объем информации, то вам потребуется или двустороннее соединение, реализованное с помощью кабельного модема, или же какое-либо другое средство, работающее одинаково быстро в обоих направлениях (ISDN).

Примечание

Если в вашем городе предлагаются услуги компьютерной связи, реализованной на базе кабельных модемов, узнайте в компании, является ли это соединение двусторонним или же односторонним. Как правило, вам предложат выбрать между односторонним и двусторонним соединением.

Насколько быстро работают кабельные модемы? Если порасспросить разных абонентов, использующих: кабельные модемы с одной и той же полосой пропускания, то ответы на вопросы будут зависеть от того, какую магистраль использует провайдер для связи с Internet и какое число подписчиков в данный момент эксплуатируют данное соединение. Обычно скорость загрузки колеблется возле значения 6.0 Кбит/с, с возникающими время от времени пиками до 130 Кбит/с, Такие скорости вполне достаточны для передачи насыщенных графикой страниц — их можно загрузить в течение считанных секунд. Однако поскольку кабельные модемы все еще развиваются и только-только становятся доступными в густо населенных регионах, трудно точно сказать, как они поведут себя в условиях напряженной работы.

По прошествии всего одного года после того, как кабельные модемы появились в продаже, еще рано решать, как они покажут себя при повсеместном внедрении, особенно в локальных сетях. Хотя кабельные модемы больше подходят для установки в прокси-серверы, а не для работы в качестве отдельного модема, они необязательно будут иметь, полосу пропускания, необходимую для обслуживания, всей локальной сети (особенно, если клиенты сети ожидают от нее молниеносной скорости работы соединения). Для корпоративных сетей более эффективными решениями могут оказаться технологии ADSL или

DSL Lite. Однако домашние сети, вероятно, смогут успешно работать, используя средства доступа, предоставляемые кабельными модемами.

Асимметричная цифровая абонентская линия (ADSL)

Любопытно, а что это такое?

Технология ADSL (Asymmetric Digital Subscriber Line— асимметричная цифровая абонентская линия) специально разработана для высокоскоростного обмена данными (64—200 Кбит/с на передачу и до 8 Мбит/с на прием, направление отсчитывается "от абонента") по существующим телефонным линиям связи. В данное время она представлена экспериментальными образцами, работающими в различных регионах США. Ее предоставляют такие компании, как PacBell, Ameritech, BellSourth и другие. Технология DSL обеспечивает совместное использование одной и той же линии связи для передачи голосовых сигналов и цифровых данных, поэтому она позволяет обходиться без двух отдельных линий для обслуживания этих потоков.

Однако то, что сейчас предлагают различные провайдеры, не является ADSL в полном смысле этого слова, а представляет собой нечто, что можно назвать DSL Lite (частичной DSL). В чем же состоит их различие? Технология ADSL предусматривает передачу данных по линиям телефонной связи, но изначально предполагаемая легкость инсталляции устройств все еще остается проблематичной — особенно в части разделения линии для передачи голосовых сообщений и цифровых данных на высоких скоростях. Подстегиваемые давлением со стороны кабельных модемов, ставших весьма популярными в тех регионах, где они начали широко применяться, производители разработали упрощенную версию технологии ADSL, называемую DSL Lite. В этой новой версии еще поддерживается высокоскоростной доступ (компания PacBell предлагает соединения, работающие на скорости от 384 Кбит/с до 1,5 Мбит/с), но это отнюдь не та головокружительная скорость, которая должна быть доступна с настоящей ADSL.

Итак, кабельные модемы или ADSL? На момент написания книги на этот вопрос не легко ответить, поскольку эти технологии настолько новы, что в большинстве регионов США они доступны только порознь. Полоса Пропускания в DSL более соответствует запросам локальных сетей, поэтому такая система может оказаться наилучшим выбором для тех, кому требуются средства для совместного использования одной полосы пропускания несколькими клиентами. Единственным ее недостатком является стоимость. В такой системе стоимость доступа больше чем у системы, построенной с помощью кабельных модемов, которая сама по себе уже дороже обычных систем удаленного доступа. А высокая стоимость, скорее всего, ограничит использование этой технологии отдельным классом пользователей с толстыми кошельками, а также корпорациями.

Серверы приложений

В прошлом было много дискуссий о наилучших способах уменьшения стоимости использования и администрирования ПК. По мере падения цен на ПК стало ясно, что наибольших затрат требуют не сами ПК, а их сопровождение.

Одной из дорогостоящих составляющих стоимости использования ПК является поддержка приложений в надлежащем состоянии. Как гарантировать, что все сетевые клиенты используют одни и те же приложения, установленные со всеми требуемыми исправлениями и другими обновлениями? Чтобы упростить решение этой задачи, можно загрузить все офисные приложения на сервер приложений, централизованно хранящий, соответ-

ствующие файлы для того, чтобы все клиенты использовали одинаковые версии приложения.

Вы не понимаете, почему здесь вообще возникли какие-то проблемы? Представьте себе ошибки, возникающие при использовании коллективом сотрудников несовместимых приложений. В оригинальной версии Office 97, не предусмотрено сохранение файлов типа .doc в формате, совместимом с Word 95 или Word 6.0. Для обеспечения совместимости с этими программами приходится устранять информацию о форматировании документа, открывая файл в старой операционной системе. Предположим, Word 95 является стандартным сетевым приложением, тогда, если кто-то войдет в сеть со своей домашней копией Word 97 и выполнит обновление файла, возникнут проблемы совместимости. Кроме того, возникнут проблемы и с лицензированием, но эти вопросы рассмотрены в гл. 11.

Другая проблема сетевых администраторов может быть проиллюстрирована примером поддержки средств языка Visual Basic (VB). Когда кто-либо из разработчиков обновляет самую последнюю версию VB, он приобретает доступ к библиотечным объектам, которых нет в предыдущей версии, и поэтому может реализовывать с помощью своего программного обеспечения то, что другим разработчикам недоступно. С одной стороны, это хорошо, поскольку позволяет ему создавать более мощное программное обеспечение, а с другой — плохо, поскольку это значит, что другие разработчики, которым может понадобиться поработать с приложениями, созданными с помощью этих новых объектов, сделать это не смогут.

Частично решить эти проблемы можно с помощью одного простого правила администрирования, которое гласит: "Никогда не устанавливай на своем компьютере нелицензионное программное обеспечение". Это хорошее правило для всех случаев как с точки зрения лицензирования и производства, так и защиты сети от вирусов типа "Троянский конь" (вирусов, упакованных в безвредное программное обеспечение). Но если кто-либо будет загружать такие приложения локально, проконтролировать ситуацию будет сложнее. А вот если приложение будет храниться на сервере, то вероятность того, что клиенты при работе *с* ним будут испытывать неприятности, значительно уменьшиться, и это положительно повлияет на работу всей сети.

Следует также учесть стоимость ручного обновления программного обеспечения в сети, в которой все приложения хранятся локально. Установка и настройка программ в местах размещения Компьютеров может выполняться относительно легко с помощью каких-либо программных средств, работы с дисками, но их обновление будет затруднено если только не использовать сервер SMS (System Management Server — сервер управления системами) или какое-то другое инструментальное средство для централизованного администрирования. В этом случае централизованное хранение приложений на единственном сервере значительно облегчает жизнь.

Сконцентрировать приложения в одном месте можно двумя различными способами. Во-первых, просто установить все приложения на центральном сервере и обеспечить связи с загрузочными файлами, необходимыми для исполнения приложения клиентами. (Для многих приложений это вполне работоспособный вариант, хотя некоторые приложения могут запускаться только локально. В последнем случае вы возвращаетесь туда, откуда начали.) Во-вторых, установить специализированное сетевое приложение, если для этого имеются соответствующие возможности. В-третьих, запустить приложение в памяти сервера, выделив клиентам только интерфейс приложения.

Примечание

Какой бы метод вы не выбрали, вам всегда следует зарегистрировать приложения. В гл. 11, приведены более подробные сведения о лицензировании и регистрации.

Хранение приложений на сервере

Для работы с приложением, хранящимся на центральном сервере, требуется установить файлы приложения на жесткий диск сервера и сделать его доступным для всей сети. Сетевые клиенты смогут запускать приложение после того, как будет установлено соответствие между логическими и физическими томами.

Средства Windows 2000 предоставляют альтернативный способ, заключающийся в хранении на сервере процедур инсталляции приложения и предоставления доступа к ним клиентам сети. Для этого существуют два метода. Первый: приложение можно сделать доступным с помощью сервера, и тогда оно появится в списке аплета **Установка и удаление программ (Add/Remove Program)** на **Панели управления** Windows у клиента. Второй метод заключается в организации доступа к приложению с помощью ярлыка на **Рабочем столе** компьютера клиента. После щелчка пользователя на соответствующем ярлыке приложение автоматически загружается на клиентный компьютер, инсталлируется и запускается. Чтобы сделать это, требуется приобрести приложение, поддерживающее такую удаленную установку, но Windows 2000 содержит инструментальные средства для упаковки приложений, изначально не предназначенных для работы в таком окружении. Любое приложение, которое отмечено логотипом "Designed for Windows 2000" (спроектировано для Windows 2000) будет поддерживать описанную выше процедуру "удаленной" инсталляции.

Использование терминального сервера

Другой подход к проблеме централизованного хранения приложений в сети состоит в их установке на сервере, работающем под управлением многопользовательской операционной системы типа Unix, WinFrame фирмы Citrix или Windows Terminal Server фирмы Microsoft, При этом клиенты запускают приложения на сервере, а результаты отображаются на их рабочих станциях. Такой сервер называют *терминальным сервером,* а машины пользователей — терминалами. Вне зависимости от того, какой мощности средства установлены на клиентом компьютере, никакой реальной обработки он не выполняет, за исключением той, которая требуется для отображения интерфейса приложения. Сеть с такой структурой называют также *тонкой клиентной сетью,* поскольку концентрация всех ресурсов на сервере "утолщает" его, а клиенты становятся "тоньше".

Работа сети терминальных серверов и клиентных терминалов сложна и сама по себе заслуживает отдельной книги. В этой и последующих главах рассмотрены лишь ключевые моменты ее функционирования, но не более того.

Как работает тонкая клиентная сеть

Функционирование терминального сервера существенно отличается от работы сервера приложений, соединенного с обычными клиентными компьютерами. В сервере приложений сетевые клиенты используют свои собственные локальные ресурсы, требуемые для работы приложения, Единственным ресурсом общего пользования является дисковое пространство, необходимое для хранения каталогов приложения, и (в общем случае) дисковое пространство для хранения файлов. А на терминальном сервере почти все ресурсы принадлежат серверу: дисковое пространство, память, процессорное время и другие.

Как же он работает? Вы не смелеете создать терминальный сервер из обычного, работающего под управлением однопользовательской операционной системы. Каждый тонкий клиент, подключившийся к серверу для работы, ничего не знает о других клиентах. В течение сеанса он может запускать любое приложение, которое ему доступно.

Примечание

Некоторые многопользовательские операционные системы позволяют клиентам всего лишь запускать отдельные приложения, в то время как другие предоставляют доступ к виртуальным рабочим столам.

Реально же происходит следующее: приложение выполняется на сервере, а клиент наблюдает и управляет им. Для этого клиенту, проводящему данный сеанс, передаются изображения, генерируемые серверным приложением, а щелчки мыши или нажатия командных клавиш клиента передаются серверу для последующей обработки (рис. 8.12).

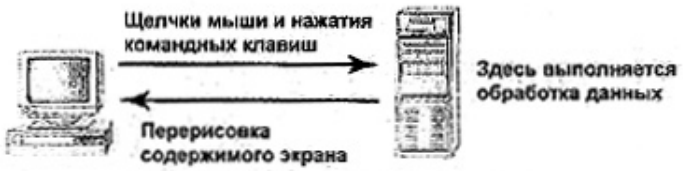


Рис. 8.12. Работа тонкой клиентной сети

Многопользовательская операционная система сортирует вводимые клиентами данные, и затем выполняет запросы клиентов.

Какие ресурсы требуются для тонкой клиентной сети

Помните, что тонкая клиентная сеть требует мощного сервера, оснащенного быстрыми процессорами, и большой объем памяти. Учтите также, что этот сервер должен поддерживать не только себя самого, но также и запросы каждого клиента во время сеанса работы. Эти сеансы "конкурируют" Друг с другом за использование процессорного времени и памяти, а также за пространство на жестком диске. Поэтому с точки зрения наличия ресурсов терминальные серверы имеют склонность превращаться в настоящих монстров, выставляющих напоказ сотни мегабайт памяти, множество процессоров и жесткие диски огромной емкости. По умеренным оценкам на них требуется установить, по крайней мере, 4—8 Мбайт памяти для каждого клиента, имеющего доступ к терминальному серверу, не считая затрат самой операционной системы. Терминальные серверы, которые автору приходилось встречать на практике, обычно представляют собой, как минимум, компьютеры с двухпроцессорной симметричной обработкой (SMP).

Примечание

С помощью Windows 2000 станет возможным уменьшить нагрузку на серверные средства за счет кэширования клиентных приложений.

Потенциальной проблемой терминальных серверов в Windows NT является хроническая нехватка виртуальной памяти. Операционная система Windows NT 4.0 и более ранних версий может адресовать виртуальную память объемом до 4 Гбайт. Допустим, 30 клиентов вошли в терминальный сервер, и каждый использует 100 Мбайт адресного пространства памяти (что не так уж и много, учитывая размер некоторых современных приложений и файлов). После этого работа с памятью будет затруднена, если принять во внимание еще и потребности самой операционной системы. Что же случится, если процессор сервера попытается выйти за пределы адресного пространства? Это, вероятно, не

произойдет в управляемой ситуации, но если и случится, то дело, скорее всего, окончится полным отказом системы. А полный отказ терминального сервера весьма нежелателен, поскольку тогда разрушится каждое используемое в данный момент приложение, причем без всякого шанса на сохранение результатов.

Примечание

Операционная система Windows 2000 будет способна адресовать виртуальную память объемом до 64 Гбайт, но только при использовании поддерживающего оборудования.

Итак, количество тонких клиентов, которые могут одновременно использовать терминальный сервер, ограничено не только возможностями операционной системы, но и доступной виртуальной памятью. Компьютер может использовать лишь столько виртуальной памяти, сколько ему доступно.

Выводы

В этой главе рассмотрены вопросы, относящиеся к специализированным серверам, которые могут устанавливаться в создаваемой сети, и необходимое для них оборудование. Почти всем без исключения серверам требуются высокопроизводительные средства, описанные в гл. 7, но, кроме того, для отдельных типов серверов может потребоваться некоторая дополнительная настройка.

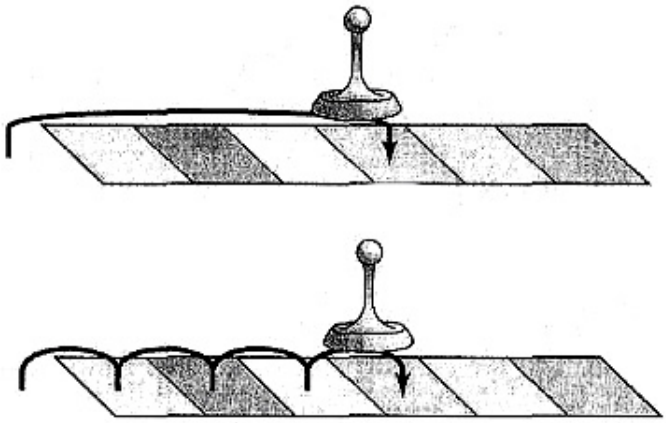
Каждый тип сервера, описанный в этой главе, рассмотрен отдельно от других, что подразумевает использование в сети только специализированных серверов: сервер печати только печатает, файловый сервер — хранит файлы и так далее. Вообще, нельзя заранее считать, что так будет на самом деле, Особенно это касается маленьких сетей, в которых приходится комбинировать возможности серверов, что означает необходимость дублирования существующих ресурсов сервера.

В двух предыдущих главах содержится развернутое описание серверов, впрочем, без акцентированного углубления в такие технологии будущего дня, которые фактически не оказывают большого воздействия на серверы и их компоненты. В гл. 9 будут рассмотрены технологии, которые смогут осчастливить ваших клиентов.

Упражнение 8

1. Наиболее часто совместно используются данные, хранимые на серверах, называемых _____.

2. На каком, из двух рисунков показан процесс поиска данных на ленте? В чем заключается отличие?



3. Вы хотите архивировать данные с жестких дисков сервера общим объемом 30 Гбайт. Если вам доступны все перечисленные ниже типы кассет, то какую из них предпочтительнее использовать?

A. DLT.
B. DAT.
C. QIC.
D. Ни одна из указанных выше.

4. Какие компоненты предпочтительнее использовать в сетевом принтере по сравнению с принтером, подключенным к серверу печати? Почему?

5. Какие устройства могут рассматриваться сетевым клиентом, как единичный элемент оборудования компонента аппаратных средств, в то время как в действительности это может быть несколько физических устройств, представленных одним логическим устройством.

6. С какой скоростью модем на 56 Кбит/с обычно передает данные?

7. В чем отличие между технологиями ADSL и DSL Lite?

A. В ADSL данные передаются в направлении к пользователю быстрее, чем в обратном направлении, в то время как DSL Lite предусматривает передачу данных с одинаковой скоростью в обоих направлениях.
B. В DSL Lite данные передаются медленнее в обоих направлениях.
C. В DSL Lite данные передаются в полудуплексном режиме, в то время как в ADSL — в дуплексном.
D. В ADSL данные передаются от пользователя быстрее, чем к пользователю, в то время как в DSL Lite - с одинаковой скоростью в обоих направлениях.

8. В полудуплексном режиме в сети ISDN данные передаются со скоростью до _____.

9. Где находится карта структуры каталогов, хранимых на дисковом сервере? На файловом сервере?

Глава 9

Клиентные рабочие станции

В предыдущих двух главах были описаны средства, необходимые для создания сервера. А что нужно клиентам? В зависимости от того, чем занимаются пользователи сети, список средств, используемых ими, может оказаться даже более обширным, поскольку зачастую именно здесь попадается весьма пестрое собрание электронного оборудования. Например, зачем серверу высококачественная видеосистема? Она более полезна для рабочей станции, за которой сидят люди и днями напролет смотрят на экран.

В этой главе рассматриваются два основных класса клиентных машин: обычные рабочие станции и устройства тонких клиентов (thin client devices). Разумеется, вы не обязаны устанавливать все описываемое здесь оборудование в свой клиентный компьютер. Более того, здесь и не приводится полный перечень всего оборудования, которое вы можете использовать. Вместо этого перечислен "разумный" набор оборудования, которое можно встретить в клиентных компьютерах, а также даны некоторые рекомендации по его конфигурированию.

Оборудование сетевых клиентов

Одно из назначений сети - облегчение загрузки централизованных ресурсов сетевыми клиентами. Если все клиенты сети смогут получить доступ к оборудованию, расположенному на сервере, их собственные запросы на его установку, безусловно, уменьшатся.

Основные компоненты компьютера были описаны в гл. 7. Здесь эта тема развивается дальше, но в данном случае обсуждаются, в основном, клиентные (пользовательские) компьютеры и технологии, относящиеся к сетевым клиентам и фактически не имеющие ничего общего с серверами.

Примечание

Приведенные ниже рекомендации по выбору оборудования для клиентных компьютеров адресованы, главным образом, покупателям нового оборудования, а не всем пользователям (покупателям) вообще. Иными словами, если у вас уже установлены клиентные машины, конфигурация которых не полностью соответствует этим рекомендациям, не отчаивайтесь. Для решения большинства задач сетевых клиентов вполне пригодны устаревшие машины. Разумеется, не стоит использовать ПК с 486 процессором для создания чертежей, однако он прекрасно подойдет для работы с текстом.

Процессор

Поскольку на клиентной машине работает единственный пользователь, быстродействие процессора в данном случае не имеет принципиального значения. Однако во всем остальном то, что важно для сервера, будет важно и для клиента. Если вам придется выбирать между объемом кэш-памяти и тактовой частотой, предпочтите кэш-память. Таким образом, вы получите процессор, который сможет достаточно быстро обрабатывать больший объем последних использованных данных, а не тратить время на загрузку данных из основной памяти, а затем очень быстро их обрабатывать. Если же вы начали задумываться о быстродействующих процессорах, появившихся за последние два года, то учтите, что разница в тактовой частоте даже в 100 МГц в данном случае не столь существенна.

Стоит ли приобретать системную плату, на которой тактовая частота системной шины составляет 100 МГц, или достаточно 66 МГц? Это зависит от области применения, однако для большинства клиентных компьютеров, как правило, загруженных относительно мало, дополнительные расходы не окупятся. Такие платы имеет смысл устанавливать в компьютерах отдельных пользователей (power-users), выполняющих сложные расчеты. Однако тем, кто в ос-

новном работает с текстовыми процессорами, приобретать быстродействующие системные платы не имеет смысла.

А какие процессоры предпочтительнее использовать в клиентных машинах: CISC или RISC? Как и в серверах, ответ зависит от программного обеспечения и, в основном, от типа используемой операционной системы. В мире персональных компьютеров нелегко найти клиентную операционную систему, работающую с RISC-процессором. Например, среди операционных систем семейства Windows к ним относится только Windows NT Workstation. Клиентные версии операционных систем UNIX работают на RISC-платформах, а операционные системы компьютеров Mac — на RISC-платформах Apple.

Тенденции развития процессоров

В конце 1998 г. самую высокую тактовую скорость — 450 МГц — обеспечивал процессор Xeon. В настоящее время его устанавливают в серверных машинах. Однако точно так же процессор 486DX66 ранее использовался в некоторых сетях в качестве серверной платформы, поэтому следует ожидать, что и Xeon скоро станет клиентным процессором. Конечно, тут же понадобится и более скоростной процессор для сервера, чтобы он соответствовал производительности процессора клиентной машины. Перспективы развития процессоров x86 на последующие пять лет представляются примерно такими:

Q199. Ожидается выпуск процессора Katmai - MMX-процессора следующего поколения с дополнительным набором команд (Katmai New Instructions (KNI) — Новая система команд Katmai). В нем предусмотрены улучшенные средства поддержки обработки трехмерных графических изображений (3D rendering) и операций с плавающей запятой. Процессоры Katmai должны работать на частоте 450 500 МГц на материнских платах с тактовой частотой системной шины 100 МГц. Ожидается, что процессор будет иметь больший кэш L1, нежели нынешние MMX-процессоры и кэш L2 на 512 Кбайт. Чуть позже должен появиться процессор Tanner, представляющий собой тот же Xeon, но частотой 500 МГц. В него будет встроен кэш L2 емкостью до 2 Мбайт. Ожидается, что последующие модификации смогут работать на материнских платах с тактовой частотой системной шины 133 МГц.

Q299. Следующее поколение процессоров Katmai сможет работать па материнской плате с частотой 133 МГц. Внутренняя частота процессора должна составлять 533 МГц.

Q399. Coppermine — процессор, поддерживающий расширенный набор команд KNI, сможет работать на материнской плате на 133 МГц. Внутренняя частота должна составлять 530—600 МГц.

Q499. Cascades — разновидность Xeon, работающего с тактовой частотой 600—667 МГц. Должен быть предусмотрен встроенный кэш L2.

Q200. Merced - первый 64-битовый процессор в семействе x86 Процессоры этого типа будут в большей мере зависеть от программною обеспечения по сравнению с их 32-битовыми предшественниками, поскольку для ускорения работы некоторые команды логических операций будут удалены из процессора и их выполнение возложено на операционную систему. Ожидается, что Merced будет иметь трехуровневую кэш-память, полученную путем добавления кэша L0. Планируют, что тактовая частота процессора возрастет до 600—1000 МГц, и он сможет одновременно обрабатывать до восьми потоков команд, причем почти втрое быстрее, чем Tanner. Merced предназначен для работы с материнской платой на частоте 200 МГц. В это "дитя" фирм Intel и Hewlett-Packard будут встроены средства поддержки SMP, обеспечивающие совместную работу четырех процессоров, а также поддерживающие 8-, 16- и даже 32-процессорные компьютеры других производителей,

Q400—Q401. Фирма Intel выпустит процессоры Willamette (клиентые платформы) и Foster (серверные платформы), в которых вместо архитектуры Процессора P6 будет исполь зована архитектура нового типа, что позволит обеим микросхемам работать с внутренней тактовой частотой 1 ГГц. Кроме того, в обе микросхемы будет встроен кэш L2 на 1 Мбайт.

Q401. В рабочих станциях процессор Merced заменит процессор McKinley. Как и Merced, McKinley будет работать на частоте 1 ГГц. Ожидается, что ко времени его выпуска разработчики фирмы Intel приобретут опыт работы с 64-битовой архитектурой и McKinley станет серьёзным конкурентом (или даже вытеснит) своих соперников от Hewlett-Packard и Digital.

Sometime in 03. Deerfield - недорогая пользовательская версия McKinley, в которой будут учтены усовершенствования, накопившиеся к 2002 году.

Совет

Параллельно с повышением быстродействия микросхем следует ожидать снижения цен. Вы можете сэкономить деньги, покупая микросхемы предпоследнего поколения. Это не слишком скажется на производительности клиентных машин - обычно требования, предъявляемые к ним, значительно скромнее.

Память

Характеристики памяти исключительно важны с точки зрения производительности клиентной машины, поскольку именно в ней сохраняется вся информация, ожидающая обработки. Чем больше объем памяти, установленной на клиентной машине, тем выше ее производительность. Если вам приходится выбирать между более быстрым процессором и памятью большего объема, рекомендую выбрать память.

Возможно, вы помните (см. гл. 7), что оперативной памяти присущ единственный недостаток: скорость работы процессоров растет намного быстрее, чем ее быстродействие. В то время как внутренняя тактовая частота современного процессора измеряется сотнями МГц, частота сигналов обращения к наиболее широко распространенной оперативной памяти — динамической — измеряется десятками МГц. Это означает, что большую часть времени процессор ожидает, пока будут получены данные из памяти. Конечно, в многозадачных операционных системах во время ожидания получения данных процессор может выполнять другие задачи. Однако чем меньше времени процессор тратит на ожидание данных от других компонентов компьютера, тем лучше.

Как можно сократить эти паузы? Установив более быструю память. Как правило, в современных персональных компьютерах используют оперативную память двух типов: EDO и SDRAM. Рекомендую выбрать память типа SDRAM. Память типа EDO работает быстрее стандартной FPM DRAM, однако предельная рабочая частота EDO-памяти составляет 40 МГц. С другой стороны, память SDRAM, реализованная средствами современной технологии, способна работать на частоте до 100 МГц. С точки зрения долговременной эффективности затрат предпочтительнее приобрести память SDRAM. Память EDO DRAM рекомендуется использовать только при модернизации устаревших машин, поскольку они могут вообще не работать с памятью SDRAM.

Тип шины

Точно так же, как и при выборе плат для серверов, вам придется выбирать платы для клиентных машин: ISA или PCI. ISA общедоступны, дешевы, но работают медленно. В то же время PCI не менее доступ им (хотя есть устройства, рассчитанные только для работы с

ISA-шиной), пот несколько дороже, но намного быстрее ISA.

Примечание

Если в качестве сетевых клиентных машин пользуются портативные компьютеры(laptops), то для установки плат расширения можно использовать слоты PC-Card. Фактически, в данном случае выбора нет - в портативных компьютерах можно использовать только устройства PC-Card и никакие другие. Поэтому вы не сможете устанавливать в них платы ISA.

При покупке новых машин рекомендуем приобретать компьютеры платами расширения PCI. Для плат адаптеров определенных типов (особенно видео- и сетевых плат) повышенная тактовая частота шины приводит к значительному росту производительности. Кроме того, это обеспечит возможность маневра в будущем по мере постепенного вытеснения плат ISA. Это не значит, что если в вашем компьютере используется шина ISA, его надо отдавать на слом. Многие пользователи просто не заметят существенного различия в производительности плат PCI и ISA, тому выбирайте оборудование с шинами PCI, особенно если покупаете новый компьютер или модернизируете компьютеры, выполняющие специализированные задачи. Однако пользователям, работающим с обычными офисными пакетами, можно не заменять уже установленные машины.

Жесткие диски

В гл. 7 при сравнительном рассмотрении интерфейсов EIDE и SCSI рекомендовалось использовать в сервере устройства с интерфейсом SCSI. Однако в большинстве клиентных машин предпочтительнее интерфейс EIDE.

Во-первых, клиентным машинам не нужны столь гибкие средства для работы с дисками. В большинстве клиентных машин установлен один жесткий диск и, возможно, устройство CD-ROM. Поэтому одновременное подключение множества устройств не играет заметной роли.

Во-вторых, хост-адаптер EIDE управляет работой всего лишь пары устройств. Ему не часто приходится управлять локальным доступом (т.е. доступом к файлам, хранящимся на файловом сервере). Следовательно, задержка ожидания ответа (продолжительность запаздывания (lag time)), обусловленная методом, с помощью которого хост-адаптер EIDE ставит в очередь запросы чтения/записи к одному устройству, не столь важна . и в сервере с несколькими устройствами. Помните, что хост-адаптер SCSI может обрабатывать сразу несколько запросов чтения/записи, адресованных личным устройствам: сначала прочитать данные с устройства CD ROM, затем начать запись на диск B, пока CD-ROM обращается искомой дорожке диска. Таким образом, считывание с медленного, устройства CD ROM не задерживает запись на диск. В интерфейсе EIDE не предусмотрена такая возможность, поэтому считывание с медленного устройства CD-ROM замедляет доступ и к жесткому диску. Однако если на доступ к диску претендует единственный пользователь, то маловероятно, что такая ситуация будет возникать настолько часто, чтобы вызывать особые проблемы. Серверные системы должны уметь справляться одновременно с несколькими, возможно, взаимно противоречивыми запросами множества пользователей, клиентная же система должна справляться с запросами всего лишь одного пользователя. Фактически, SCSI-интерфейс может даже замедлить работу систем, в которых к хост-адаптеру подключено единственное устройство, поскольку при этом система обрабатывает избыточную информацию.

В-третьих, хотя по мере увеличения объемов программного обеспечения клиентных машин возрастает и потребность в пространстве для его хранения, устройство EIDE все еще способно удовлетворить запросы многих клиентов. В настоящее время можно приобрести EIDE-диск емкостью до 8 Гбайт — немыслимая величина даже для сервера еще несколько лет назад. Но есть ли реальная необходимость установки на клиентной машине диска емкостью более 8 Гбайт? Если для клиентной машины нужен диск такой огромной емкости, есть смысл

подумать об установке SCSI-диска. Однако в большинстве случаев пользовательские данные хранятся именно на файловом сервере, а не клиентном компьютере.

Четвертое и, фактически, главное соображение заключается в том, что диски SCSI намного дороже дисков EIDE такой же емкости. Итак, если применение SCSI-интерфейса не приводит к значительному росту производительности, то использовать устройства SCSI не имеет смысла.

Пользовательские видеосистемы

По сути, предшествующие страницы были заполнены призывами не разбрасывать деньги понапрасну, поскольку большинство клиентов просто не заметят разницы — ведь одна из задач сервера как раз и заключается в том, чтобы расширить возможности оборудования клиентного компьютера. Тем не менее, есть одна область применения, где они обязательно заметят разницу — видеосистема.

Экран монитора — основная часть компьютера, на которую смотрят все пользователи. Можете не сомневаться: новый монитор не повысит быстродействие медленной машины. Однако даже мощная машина с монитором, имеющим низкую частоту развертки и воспроизводящим 16 цветов, покажется медлительной и убогой. Средства обработки видеоизображений не важны для сервера, но пользователи клиентных машин проводят за мониторами немало времени, и желательно, чтобы это доставляло им удовольствие. Разумеется, это вовсе не означает применения всяческих "украшений", поскольку во многих офисных приложениях они совершенно бесполезны. Однако изображение должно быть качественным и обновляться достаточно быстро.

Примечание

Современные видеотехнологии, такие как AGP и 3D (3D acceleration), наиболее эффективны в компьютерных играх. Однако они полезны и при работе с программами анимации (rendering software).

Видеоплаты

Как и оперативная память, видеопамять является "пристанищем" для обрабатываемых данных и команд, которые должны быть переданы на монитор для визуализации. Чем больше число цветов, отображаемых монитором, чем выше разрешение и частота регенерации (чем выше частота регенерации, тем устойчивее изображение), тем больше памяти необходимо для хранения этих данных. Чем выше скорость считывания и записи данных в эту память, тем быстрее изображение "реагирует" на действия пользователя.

На что следует обратить внимание при выборе видеоплаты? В основном, на три параметра.

- Объем видеопамяти.
- Быстродействие шины.
- Тип памяти.

Совет

Вам не нужно приобретать дополнительную плату видеоакселератора (video acceleration). Все современные видеоплаты, как правило, снабжены соответствующими средствами, даже если это и не оговорено отдельно в спецификации видеоплаты.

Поскольку быстродействие шины и видеопамять уже рассмотрены, можно обойтись без дополнительных пояснений. Третий параметр — тип используемой памяти — возможно, требует дополнительных пояснений из-за разнообразия типов схем памяти, предложенных для ускорения работы (в отличие от оперативной памяти). От типа используемой памяти в зна-

чительной степени зависит производительность видеоплаты и ее цена (остальные два фактора тоже имеют большое значение).

Обычная (FPM) видеопамять. Как вы, возможно, помните (см. гл. 7), FPM-память — самая старая и медленная из используемых до сих пор типов. Как правило, время доступа к ней составляет 60—70 нс. Она способна одновременно выполнять только одну операцию: или чтение или запись. Ее преимущество заключается в дешевизне. Эта память чаще всего применяется в дешевых видеоплатах, обеспечивающих воспроизведение не более 256 цветов.

Примечание

Все микросхемы видеопамяти представляют различные модификации микросхем динамической памяти (DRAM). Если в спецификации на конкретную видеоплату в обозначении типа памяти присутствует аббревиатура "DRAM", то, вероятно, в плате используется память типа FPM (Fast Page Mode - быстрый постраничный доступ).

В некоторых видеоплатах используют EDO-память. Подобно сноси "родственнице", используемой в оперативной памяти, EDO-видеопамять быстрее FPM-видеопамяти, поскольку может выполнять следующую операцию считывания еще по время завершения предыдущей. Однако она ненамного быстрее, чем FPM-память.

Чтобы работать с чем-то более сложным, чем 256-цветное изображение с низким разрешением, вам понадобится память другого типа, оптимизированная для вывода видеоинформации. С этой целью в память добавляют вторую шину данных (память типа VRAM) либо повышают тактовую частоту (память SGRAM и MDRAM), либо используют оба метода совместно (WDRAM). Память всех этих типов стоит дороже, чем FPM/EDO-память, однако они (каждая по-своему) обеспечивают большую производительность.

VRAM (Video RAM — Видео ОЗУ). Правда ли, что любую память, расположенную на видеоплате, можно назвать VRAM-памятью (видео ОЗУ)? Не совсем так. VRAM-память - это память, специально разработанная для работы с видеоизображениями. Ее секрет заключается в наличии двух шин данных. В то время как в FPM-памяти одновременно можно выполнять только одну операцию (т.е. только считывать или только записывать), в памяти VRAM предусмотрены две шины: одна — для чтения, другая — для записи.

Синхронная графическая память (SGRAM). В отличие от VRAM память типа SGRAM однопортовая, однако по своей производительности она находится на уровне VRAM, а не FPM или EDO. Это достигается за счет скорости — она так же может делать только что-либо одно, но зато очень быстро. Память типа SGRAM получила широкое распространение, поскольку обеспечивает высокую производительность в системах со средним разрешением (medium-resolution systems). Она не может работать с графическими изображениями, требующими высокого разрешения (что, например, может делать память WDRAM, рассматриваемая ниже), однако и так работает с весьма высокой скоростью, и платы с памятью такого типа приобрести достаточно легко.

Память Windows DRAM (WDRAM). Те, кто недоволен успехами фирмы Microsoft в мире программного обеспечения, будут счастливы узнать, что имя видеопамяти этого типа не имеет ничего общего с популярной операционной системой, а относится к типу изображения, при работе с которым используется память. Подобно VRAM-памяти, память WDRAM — двухпортовая, однако кроме этого она обладает и более высоким быстродействием. Во-первых, полоса пропускания у WDRAM шире, чем у VRAM, что позволяет ей быстрее связываться с процессором. Во-вторых, в системе управления памятью WDRAM предусмотрены некоторые команды, обычно необходимые для обработки изображений в окнах, включая те, что применяют для вывода текста (text rendering) и рисования цветовых блоков больших размеров. Вероятно, WDRAM можно считать самой быстрой видеопамятью, известной в настоящее время. Кроме того, поскольку она позволяет воспроизводить большое количество цветов (complex color depth) с высоким разрешением, то стоит очень дорого.

Multibank DRAM (Многоблочная DRAM). Как правило, видеопамяит (и обычная память, если на то пошло) логически разделена на блоки объемом не менее 1 Мбайт. Одновременно можно получить доступ только к одному блоку памяти, независимо от скорости доступа и количества шин, ведущих к этому блоку. Такой доступ имеет два недостатка. Первый: доступ к памяти не столь гибок, поскольку одновременно можно выполнять только одну операцию чтения или записи (во всем блоке объемом 1 Мбайт). Второй: вы обязаны наращивать память блоками размером не менее 1 Мбайт, даже если вам и не надо так много памяти.

Чтобы обойти эти проблемы, в MDRAM-системе предусмотрено "расщепление" памяти на логические блоки размером 32 Кбайт. Это повышает гибкость системы, поскольку операции чтения и записи могут чередоваться, но уже между секциями памяти размером 32 Кбайт. Почему это важно? Главным образом потому, что позволяет избежать снижения производительности видеоплат с памятью малого объема. Посудите сами: если самый малый логический блок памяти, к которому можно адресоваться, имеет размер 1 Мбайт, то каждая очередь на выполнение операций чтения и записи все равно будет адресована к блоку объемом не менее 1 Мбайт. Если же для ускорения вывода вы захотите использовать большее число очередей, то вам следует добавлять память, причем блоками размером не менее 1 Мбайт. Иными словами, в большинстве систем плата с видеопамятью 2 Мбайт всегда будет работать быстрее платы с видеопамятью 1 Мбайт. И так будет даже в том случае, если для вывода необходимой видеоинформации буфер объемом в 2 Мбайт не требуется только потому, что в плате с памятью 2 Мбайт используются две шины. В памяти WDRAM это не так. Конечно, если нужно дополнительное пространство для хранения видеоизображения, вам тоже придется наращивать память. Но если нужна только дополнительная магистраль, проблема решается без труда.

Еще одно преимущество памяти MDRAM заключается в том, что теоретически применение такой памяти позволяет создавать платы с размерами буферов, соответствующими минимальному выводу, который они должны поддерживать. Однако, как правило, вы найдете в продаже видеоплаты WDRAM с теми же размерами памяти, что и у остальных плат: 2 Мбайт, 4 Мбайт и т.д.

Как выбрать монитор?

Еще один немаловажный аспект, который следует учитывать при выборе видеосистемы, — тип монитора. В целом, видеоплаты имеют достаточную мощность, а значит не должны отставать и мониторы. Вы не ощутите никаких преимуществ от установки видеоплаты PCI с памятью WDRAM объемом 8 Мбайт, если ваш монитор не соответствует ее возможностям.

Как и прочее оборудование, мониторы стали более совершенными и значительно подешевели. Как правило, в новых пользовательских компьютерах применяют 15-дюймовые мониторы. В более дорогостоящих системах устанавливают 17-дюймовые и даже 21-дюймовые мониторы неслыханные размеры для обычных рабочих станций еще несколько лет назад. Однако независимо от размеров монитора каждому пользователю необходимо как можно больше свободного места на рабочем столе Windows.

Совет

В некоторых операционных системах, таких как Windows 98 и UNIX, поддерживается одновременная работа нескольких мониторов. Поэтому вы можете объединять видимые области с двух небольших мониторов в один рабочий стол. Ожидается, что и в Windows 2000 будет предусмотрена поддержка нескольких мониторов.

Для оценки характеристик мониторов полезно знать принцип их работы. На видеоплате имеется микросхема, называемая RAMDAC (RAM digital-to-analog converter — цифро-аналоговый преобразователь RAM), которая преобразует цифровую информацию, хранящуюся в видеопамяти, в аналоговую, отображаемую дисплеем. Фактически, RAMDAC состоит из четырех частей: собственно цифро-аналогового преобразователя и нескольких каналов об-

работки преобразованного сигнала — по одному на каждый луч основного цвета (красный, зеленый и синий). Из этих трех цветов можно создать любой другой цвет. Электронные лучи, создаваемые в трубке монитора, перемещаются по экрану, облучая люминофор, покрывающий его внутреннюю сторону. При попадании потока электронов на люминофор последний начинает светиться. В результате на экране образуется видимое изображение.

Таков общий принцип действия монитора, но как работает конкретный монитор? Ответ зависит от нескольких факторов. Во-первых, с какой частотой электронный луч освещает люминофор? (Люминофор светится только тогда, когда на него попадает электронный луч. Но даже после того, как луч перестал освещать люминофор, он в течение некоторого времени продолжает светиться.) Чем чаще лучи попадают на люминофор, тем устойчивее видимое изображение. Если ваш глаз в состоянии заметить снижение яркости экрана, значит вы будете видеть мерцающее изображение. Эта проблема особенно существенна для больших экранов, поскольку светочувствительные палочки на периферии сетчатки глаза лучше воспринимают движение, чем колбочки в центре сетчатки. Итак, вам необходим монитор, который "перерисовывает" изображение достаточно регулярно. Чистота, с которой это происходит, называется частотой регенерации (refresh rate). Чем выше частота регенерации, тем лучше.

Примечание

С целью удешевления в некоторых устаревших мониторах использовалась чересстрочная (interlaced) развертка. Слово "чересстрочная" означает, что при каждом проходе луча по экрану освещаются не соседние строки, а расположенные через один ряд. Таким образом, частота регенерации повышается, однако мерцание изображения снижается незначительно. В настоящее время трудно найти монитор с чересстрочной разверткой, но даже если вам это удастся, избегайте такой покупки. Если вы заставите людей целыми днями смотреть на экран такого монитора, они вас возненавидят.

Во-вторых, что такое степень детализации (granularity) изображения? Чем больше точек на экране, тем отчетливее изображение. Однако чем больше размеры экрана, тем больше точек, поэтому требуется иной показатель качества. Таким показателем является размер точки люминофорного покрытия, который называется зернистостью (dot pitch) и измеряется в миллиметрах. Обычно в современных мониторах зернистость находится в пределах 0,26—0,39 мм, а в среднем у большинства мониторов составляет 0,28 мм. Чем больше размер экрана монитора, тем больше зернистость (и это будет незаметно для глаз), однако чем она меньше, тем отчетливее изображение.

В-третьих, какое разрешение должен поддерживать монитор? Разрешение определяется количеством точек, видимых как по вертикали, так и по горизонтали. Поскольку экран монитора имеет прямоугольную форму, разрешение зависит от обеих величин. Так, наименьшее разрешение современных мониторов составляет 640 точек по горизонтали и 480 по вертикали экрана: 640x480. Однако времена, когда разрешение 640x480 в большинстве случаев было вполне приемлемым, давно ушли. Сегодня большинство пользователей работают при разрешении 800x600, а на 17-дюймовых и более крупных мониторах желательно иметь разрешение 1024x768. Некоторые мониторы поддерживают разрешение 1600x1200. Современные мониторы могут поддерживать различные разрешения, поэтому его величина, указанная в документации, соответствует наивысшему значению, поддерживаемому монитором, а не всем разрешениям, которые он может поддерживать. Вообще, чем крупнее монитор, тем большее разрешение следует использовать.

Совет

При выборе монитора обращайте внимание не только на размер экрана монитора (который измеряется по диагонали, как у телевизора), но и на размер видимой области. Так, видимая область у монитора с 17-дюймовой трубкой не превышает 16 дюймов, а у более дешевых моделей - и того меньше.

Что же самое важное в мониторе: частота регенерации, зернистость, разрешение или насыщенность цвета? Все важно. Поэтому следует выбрать компромиссные значения насы-

щенности отображаемого цвета, разрешения монитора и частоты регенерации. При этом придется поступаться скоростью регенерации по мере усложнения изображений. Конечно, есть мониторы, которые могут поддерживать на высоком уровне одновременно все четыре характеристики, однако чем лучше это делается, тем, вероятнее, дороже обойдется монитор. Но даже в самых дорогих мониторах при реализации всех ресурсов требуется идти на компромисс. Если вам необходимо отобразить на экране большое количество цветов, придется понизить разрешение, а если вам необходима высокая частота регенерации, придется пожертвовать насыщенностью цвета.

К счастью, в последнее время нетрудно найти монитор, имеющий частоту регенерации (кадровую частоту) 85 Гц (или около того) и в то же время отображающий 16 миллионов цветов при разрешении 1024x768. 85 Гц — минимальная частота, при которой пользователю удобно работать, хотя некоторые люди могут без всяких проблем (для собственного зрения) использовать мониторы с частотой регенерации 75 Гц и даже 60 Гц.

Плоские дисплеи

Размеры мониторов становятся все больше, и хотя подставки для них стали удобнее, больший монитор потребляет больше электроэнергии и занимает больше места на столе. Один из способов избежать повышенного расхода электроэнергии и приобретения нового стола (хотя это пока что слишком дорого для большинства из нас) — использовать жидкокристаллические дисплеи. Несмотря на меньшие геометрические размеры по сравнению с мониторами, в которых используется широко распространенная электронно-лучевая трубка (ЭЛТ, cathode ray tube (CRT)), у них полезная площадь экрана (viewing area) используется более эффективно, так что полезная площадь 14-дюймового плоского дисплея точно такая же, как у 17-дюймовой ЭЛТ.

Такие дисплеи давно уже используют в портативных компьютерах. Причин тому две. Во-первых, вы не можете тащить за собой монитор с CRT, когда спешите к выходу из аэропорта. Во-вторых, плоские дисплеи потребляют значительно меньше электроэнергии, чем ЭЛТ. Вы не сможете долго работать с обычным монитором от UPS со встроенным аккумулятром, не говоря уж об аккумуляторе портативного компьютера. (Среднестатистический 14-дюймовый дисплей потребляет примерно 70 Вт. Типичная емкость аккумуляторной батареи UPS (12 В) составляет 6 Ахчас. Несложные расчеты показывают, что монитор сможет работать от полностью заряженной батареи в течение 20—30 мин. Системный блок с процессором 486 DX2-80, жестким диском 500—800 Мбайт и 3,5-дюймовым дисководом потребляет 25—35 Вт. Компьютер в такой конфигурации сможет проработать от упомянутого выше аккумулятора 15—20 мин. Обратите внимание, что монитор является основным потребителем электроэнергии. — Прим. ред.). В современных жидкокристаллических дисплеях используется активно-матричная технология (active matrix technology), обеспечивающая превосходную насыщенность цвета и устойчивое изображение, легко воспринимаемое глазом.

Размеры экранов портативных компьютеров постоянно растут. Два года назад для портативного компьютера экран в 12,1 дюйма считался огромным по стандартам портативных компьютеров. Но по сравнению с современными 15-дюймовыми экранами он выглядит карликом. Однако размеры экранов портативных компьютеров не могут быть сделаны сколь угодно большими. Большие экраны все так же потребляют больше электроэнергии, хотя коэффициент полезного действия у активно-матричного дисплея выше, чем у электронно-лучевой трубки. Кроме того, вес портативных компьютеров не должен превышать определенного значения (дополнительный вес компьютерщика ухудшает его эксплуатационные характеристики).

Однако в мире настольных компьютеров эти проблемы несущественны. Электроэнергия подается из электросети, а не из батарей, а переносить настольный компьютер приходится не слишком часто. Поэтому размер плоского дисплея в данном случае допустимо увеличить. Некоторые экраны можно даже вешать на стену, так что вы сможете использовать всю поверхность, письменного стола. Это прекрасная новость дня для тех, кто вынужден использовать

для работы Г-образный стол. (На токам столе выступающая часть используется для установки монитора. - Прим. ред.)

Что же препятствует покупке и использованию плоского дисплея? Цена. В настоящее время при равных размерах видимой области плоские дисплеи вдвое дороже обычных мониторов. Однако по мере снижения цен следует ожидать, что пользователи будут заменять устаревшие ЭЛТ на плоские дисплеи.

Клиентные компьютеры, отличающиеся от типа IBM PC

До сих пор мы рассматривали клиентные компьютеры с типичной "начинкой": мониторы, встроенные диски, клавиатуры и т.п. Компьютеры с такой архитектурой могут выполнять практически все, если установить соответствующее программное обеспечение. Но если от клиентных компьютеров не требуется уметь делать практически все, что может потребоваться? Если клиентный компьютер предназначен для решения конкретной задачи или группы задач, имеет смысл поддерживать только необходимые приложения. Кроме того, специализированные клиентные компьютеры могут иметь меньший размер, а иногда и цену, чем их полнофункциональные собратья. На таких компьютерах проще обучать неопытных пользователей. Пользователь, который чувствует себя неуверенно, сидя перед монитором, процессором и клавиатурой, будет счастлив поработать с сенсорным экраном кассового аппарата.

Операционные системы и приложения, доступные таким "не компьютерным" сетевым клиентам, зависят от их модели и задач, которые должен решать такой компьютер. В этих устройствах могут использоваться как уникальные операционные системы, разработанные специально для данного оборудования, так и более общие, скажем, Microsoft Windows CE -упрощенная версия набора функций API Windows NT, разработанная фирмой Microsoft для использования в малых компьютерных устройствах.

Примечание

Между прочим, "уникальное" отнюдь не означает "плохое". Мне больше нравится устройство Palm Pilot фирмы 3Com с уникальной операционной системой, чем Cassiopeia фирмы Casio, в котором используется Windows CE. Пользоваться первым компьютером намного проще.

Что касается приложений, то фирмой Microsoft разработаны несколько упрощенных версий наиболее популярных приложений, таких как Microsoft Word и Outlook. Другими примерами таких приложений могут служить, броузеры Web, позволяющие получать доступ к Web-приложениям. Кроме того, сюда могут входить дополнительные приложения, например, приложения для составления инвентарных описей или обслуживания кассовых аппаратов.

По состоянию на конец 1998 г. "упрощенные" сетевые клиенты редко использовались вне складов и ресторанов — пока что в деловых сетях чаще можно встретить обычные клиентные ПК типов PC и Macintosh. В настоящее время такие "низкоуровневые" клиентные машины используют скорее как дополнение, а не как альтернативу обычным компьютерам. Тем не менее, их используют, и, возможно, именно благодаря своей простоте такие узкоспециализированные машины начинают применять все большее число пользователей, занимающихся узкими деловыми задачами, а также мобильные пользователи.

Одним из примеров упрощенной клиентной машины может служить персональный цифровой ассистент (PDA — personal data assistant). PDA являются небольшими компьютерными устройствами с упрощенными версиями популярных операционных систем (например, Windows CE) и приложений. Как правило, в таких устройствах установлен небольшой жидкокристаллический монохромный дисплей. Габариты PDA таковы, что позволяют переносить их в большом кармане.

Какие же задачи можно решать с помощью PDA? Многие используют PDA для работы с электронной почтой, деловыми записями, составления ежедневных расписаний либо (если стало скучно) раскладывания пасьянса, но они непригодны для выполнения сколько-нибудь серьезной работы. Как правило, чтобы создать законченный продукт, содержимое PDA необходимо перегрузить в обычный компьютер. В более специализированных PDA предусмотрена поддержка речевого ввода (dictation) и таймера (beeper). В системах PDA используются разнообразные устройства ввода. В некоторых предусмотрены небольшие клавиатуры (которые вполне удовлетворяют пользователей, но, вероятно, они слишком неудобны для ввода большого количества данных). Другие воспринимают символы, вводимые с помощью светового пера (stylus), в соответствии с правилами правописания, которые вы, безусловно, должны знать. Вместо клавиш управления (control keys) клавиатуры используют навигационные кнопки.

Оборудование тонких клиентных сетей

Компьютерные средства "тонких" клиентных сетей (thin client computing) частично рассмотрены в гл. 8. Подробнее они будут описаны в гл. 12. Возможно, вы припомните, что основная идея создания компьютерных средств для таких клиентов заключается в том, что большая часть обработки выполняется центральным сервером. Клиентная машина отвечает только за отображение на экране графики, выводимой приложением, а также за прием информации при нажатии клавиш и щелчках мыши, которые интерпретируются сервером. В таком случае в тонкой клиентной машине нет надобности устанавливать средства обычных клиентных компьютеров. Компьютерные средства таких тонких клиентов содержат ресурсы, делающие пользовательский компьютер высокоэффективной специализированной графической станцией (graphic engine).

Если (оставить в стороне такие устройства, как PDA и интеллектуальное телевидение (smart television), и качестве тонких клиентных машин могут работать три типа компьютеров.

- Любой компьютер, на котором установлено программное обеспечение, превращающее его в тонкий клиентный компьютер.
- Сетевые компьютеры.
- Терминалы Windows.

Разумеется, вы знаете, что такое компьютер. Сетевым компьютером (NC — network computer) называют устройство, которое позволяет либо отображать приложения, исполняемые сервером, либо загружать их с сервера и исполнять локально. Широко известный пример таких программ — апплеты Java.

Строго говоря, терминалы Windows локально не исполняют никаких программ (вся обработка выполняется сервером), а только отображают результаты. На рис. 9.1 показан один из терминалов Windows (Windows terminal device) с отсоединенными монитором и клавиатурой. В этом корпусе помещается все, что необходимо для вычислений. Единственными внешними устройствами являются монитор и устройства ввода.

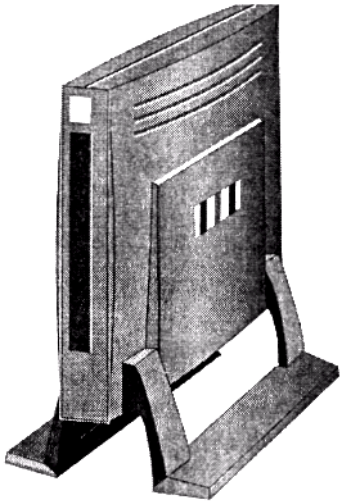


Рис. 9.1. Терминал Windows может иметь весьма небольшие размеры

Примечание

Стоимость сетевых и обычных компьютеров не слишком различается. Однако (и это может привести к путанице) в некоторых устройствах, которые продаются как терминалы Windows, предусмотрены отдельные средства, характерные для сетевых компьютеров. Так, на них можно запускать апплеты Java с помощью локальных аппаратных ресурсов, а в некоторые модели могут быть встроены даже небольшие жесткие диски.

Обратите внимание: степень "тонкости" клиента определяется отнюдь не оборудованием, которое установлено (или, наоборот, не установлено) в по компьютере. Тонкий клиентный компьютер может Пить укомплектован всего лишь процессором, сетевым соединением и оперативной памятью, но им же может быть полностью укомплектованный персональный компьютер "мощного" пользователя (power user). Отличить тонкую клиентную машину от всех других можно по месту, где выполняется основная часть обработки информации. Если клиентная машина в основном (или полностью) выполняет функции дисплея, она является тонкой клиентной машиной независимо от ее комплектации. Единственным требованием, которому должны удовлетворять все тонкие клиенты, является наличие сетевой поддержки (network support). По определению, тонкий клиент должен быть связан по сети с сервером, исполняющим приложения.

Поскольку тонкие клиентные устройства предназначены только для графического вывода, им не требуются такие же средства, как компьютерам, выполняющим локальную обработку. Так, терминал Windows обычно состоит из следующих компонентов.

- Процессор (с тактовой частотой 100 МГц или менее).
- Оперативная память (RAM), достаточная для поддержки вывода видеоинформации, скажем, для начала, 8—16 Мбайт.
- Видеоплата и монитор.
- Сетевая плата.
- Устройство ввода — клавиатура, мышь и т.п.
- Последовательный или параллельный порт.

За исключением мыши и клавиатуры, все компоненты встроены в терминал Windows или сетевой компьютер. Кроме того, в состав тонкого клиентного компьютера может входить дополнительное оборудование, например, звуковые колонки, слоты PC-Card для подключения модемов или небольших жестких дисков и т.п. (выше перечислены только основные типы устройств).

Тонкий клиент — он и есть тонкий (thin). Даже при выполнении программы, требующей значительных ресурсов, процессор тонкого клиентного устройства может работать медленно,

обходиться ограниченной памятью и не слишком мощной видеоплатой. (Из-за ограниченных аппаратных ресурсов монитор тонкой клиентной машины может отображать не более 256 цветов.) Устройства, подобные терминалам Windows и сетевым компьютерам, созданы для быстрого и эффективного отображения графической информации, но сама по себе выводимая информация всегда невыразительна. Кроме того, хотя скорость работы тонких клиентных устройств зависит от скорости работы сети, сетевое соединение не обязательно должно быть скоростным, поскольку объем входящей и исходящей информации невелик.

ПК, работающие как тонкие клиентные компьютеры, могут выступать и в качестве обычных сетевых машин. В таком случае им необходимы соответствующие ресурсы для локального исполнения приложений. К счастью, для работы в такой двойной роли не требуются дополнительные ресурсы (по сравнению с обычными сетевыми машинами). "К счастью" потому, что возможности оборудования тонких клиентных машин ограничены. Перерисовка же изображения на экране остаётся перерисовкой независимо от того, генерируется изображение локально или передаётся по сети.

Теперь вы получили представление о тонких клиентных сетях с точки зрения пользователя. Подробнее об этом см. гл. 12.

Выводы

Как видите, клиентные компьютеры не обязательно имеют такие же мощные средства, которыми снабжен сервер. Требования к ним проще, а рабочие нагрузки - полегче, так что даже самые загруженные клиентные компьютеры выполняют меньшую работу, чем серверы, обеспечивающие ресурсами множество клиентов сети.

Когда потребности клиента совсем невелики, даже персональные компьютеры с традиционной конфигурацией могут оказаться избыточными. Для многих практических применений пригодны упрощенные вычислительные устройства вроде PDA либо другие специализированные компьютеры. Чтобы ощутимо снизить требования к аппаратному обеспечению клиентов, можно заменить клиентные компьютеры тонкими клиентными устройствами: сетевыми компьютерами или терминалами Windows, которые могут отображать графику, создаваемую исполняемым на сервере приложением. Тем не менее, в большинстве случаев все еще применяют традиционные персональные компьютеры.

В трех предыдущих главах обсуждались требования к оборудованию серверных и клиентных компьютеров. В гл. 10 "Сетевые операционные системы" рассматриваются операционные системы, используемые на этом оборудовании, а также поддерживаемые ими приложения.

Упражнение 9

1. Какие клиентные операционные системы на базе Windows поддерживают работу с процессорами на микросхемах RISC?

2. Так же, как и WDRAM-память, память SGRAM является двухпортовой? Ответьте, "да" или "нет".

3. В тонких клиентных машинах обычно предъявляются меньшие требования к памяти и процессору, чем в обычных клиентных машинах. Однако в устройствах для тонких клиентов по определению всегда предусмотрена_____поддержка. Почему?

4. Какой тип контроллера жесткого диска предпочтительно использовать в большинстве клиентных сетевых компьютеров?

A. SCSI.
B. EIDE.
C. IDE.
D. ESDI.

5. Первый 64-битовый процессор семейства x86 фирмы Intel имеет кодовое обозначение ___.

6. Ваш клиентный компьютер предназначен для загрузки приложений Java с сервера, но исполняет их локально. Такой компьютер называется:

A. Терминал Windows.
B. Персональный цифровой ассистент (PDA).
C. Специализированная рабочая станция.
D. Сетевой компьютер.

7. Как правило, требования к оборудованию клиентного компьютера ниже, чем к серверу, кроме случая, когда оно предназначено для_____.

Глава 10

Сетевые операционные системы

Итак, у нас есть сеть, состоящая из компьютеров, соединенных проводами между собой. Теперь нам необходима сетевая операционная система (NOS — network operational system), которая обеспечит функционирование сетевого оборудования, поддержку сетевых протоколов, совместное использование файлов и принтеров и т.п. В этой главе рассматриваются некоторые NOS. Рассказывается о том, чего можно ожидать от сетевой операционной системы и чем они различаются. Мы не будем подробно обсуждать все представленные на рынке сетевые операционные системы, а просто приведем некоторые основные сведения о них.

Как уже упоминалось в предыдущих главах, с точки зрения предоставляемых услуг большинство сетевых операционных систем во многом похожи. Чтобы быть достойным своего имени, любая NOS должна обеспечивать некоторый стандартный набор сетевых функциональных средств, позволяющих клиентным компьютерам совместно использовать сетевые ресурсы. Благодаря конкуренции, как только в одной из NOS появляется какое-либо новое средство, прочие сетевые операционные системы тут же "обзаводятся" аналогичным. Диапазоны возможностей этих функциональных средств могут быть различными. В одних NOS они более мощные, в других — менее (в зависимости от способов их реализации на компьютерном уровне). Так, производительность конкретной операции, например при обработке видеоинформации, в значительной степени зависит от принципов организации этой NOS.

Одно из основных различий между сетевыми операционными системами заключается в типе сетей, для которых они спроектированы: клиент/сервер или одноранговая. NOS сетей клиент/сервер спроектированы для обслуживания только сетевых запросов. С другой стороны, NOS одноранговых сетей спроектированы для обслуживания как сетевых, так и локальных запросов. Другими словами, NOS одноранговых сетей спроектированы для поддержки работы сетевых компьютеров путем предоставления сетевых ресурсов, а NOS сетей клиент/сервер — по-другому. Конечно, в некоторых случаях можно запускать пользовательские приложения на компьютере, работающем под управлением NOS клиент/сервер, однако операционные системы создаются для других целей. При прочих равных условиях приложения будут выполняться лучше, если операционная система создана именно для этой цели. Точно так же, отклики на сетевые запросы ускоряются, если использовать NOS клиент/сервер. Различие в типах сетей не обязательно связано с конструкцией сети или с выделением серверных компьютеров с тем, чтобы компьютеры не пытались выполнять двойную
работу, исполняя два набора запросов. Скорее, это относится к факторам, определяющим конструкцию NOS, а также ее назначение. Различие главным образом заключается в назначении приоритетов исполнения сетевых запросов по сравнению с теми запросами, которые генерируются локально. Как известно, современные операционные системы разделяют время, которое затрачивает процессор на выполнение работы, на потоки, а каждому потоку назначают приоритет. Приоритет потока определяет, насколько быстро ему будет выделено процессорное время на обработку потока. Чем выше приоритет, тем скорее будет предоставлено процессорное время. (Это не означает, что потоки с низкими приоритетами должны всегда ожидать, пока процессор завершит работу с более высоким приоритетом, а только то, что потоки с низшими приоритетами должны ожидать большее время.) Сказанное важно потому, что структура операционной системы и метод ее конфигурирования определяют метод назначения приоритетов потокам, сгенерированным сетью и потокам сгенерированным локально. NOS клиент/сервер спроектированы так, что назначают более высокий приоритет потокам, инициированным сетью. В то же время одноранговые NOS спроектированы так, что более высокие приоритеты назначаются локальным потокам.

Разница между планировщиками (scheduler) серверной и клиентной операционных систем приводит к интересной дилемме в случае, когда они применяются для терминальных

серверов, которые выполняют пользовательские приложения. Таким образом, к их преимуществам можно отнести метод постановки задач в очередь, который свойственен рабочей станции, но не серверу. По этой причине в Windows 2000 можно переключать планировщик в зависимости от того, работает NOS как терминальный сервер либо как сервер иного типа. Это не единственное различие между операционными системами сетей клиент/сервер и одноранговыми. Первые, помимо всего, оптимизированы для работы в сети, поскольку обеспечивают:

- лучшую защиту;
- более эффективную организацию данных (для ускорения поиска);
- более совершенные методы хранения файлов;
- лучшую поддержку совместного использования оборудования.

В целом, операционные системы типа клиент/сервер мощнее одноранговых, которые пригодны для эффективной реализации совместного использования ресурсов только небольших сетей.

Операционные системы одноранговых сетей

Если ваша сеть невелика, а потребности пользователей скромны, одноранговая сеть может оказаться самым подходящим решением. Соответствующие операционные системы не предоставляют таких широких возможностей, как операционные системы клиент/сервер, но имеют два преимущества.

- Они дешевле, чем NOS клиент/сервер.
- Не требуют для управления постоянного вмешательства сетевого администратора.

Вы можете рассчитывать, что одноранговая сеть будет поддерживать совместное использование файлов и принтеров и, возможно, некоторые (хотя и ограниченные) инструменты удаленного администрирования. Как правило, одноранговые сети не содержат развитых средств защиты и удаленного администрирования. Однако, если вас устраивают их скромные средства защиты и организации совместного использования ресурсов, эти операционные системы прекрасно подойдут для небольших и непритязательных сетей.

Примечание

Здесь мы остановимся на операционных системах Windows, поскольку они в наибольшей степени пригодны для создания одноранговых сетей. Фирма Novell прекратила поддерживать свой сервер одноранговой сети (peer network server product), а Warp фактически умирает (так же, как умерла OS/2). В настоящее время одноранговые сети поддерживаются только в Windows.

История древнего мира

Операционные системы Windows уже давно были способны работать в сетях, и вплоть до начала 90-х г. для этого использовалась надстройка DOS, называемая MS-NET. (Кроме того, эта же надстройка использовалась для выхода в сеть клиентов MS-DOS. Однако мы и так достаточно углубились в операционные системы Microsoft.) В конце 1992 г. фирма Microsoft выпустила первую одноранговую NOS, называемую Windows for Workgroup (WfWg). Она не слишком отличалась от Windows 3.x, за исключением наличия диспетчера файлов (File Manager), который поддерживал отображения буквенных обозначений дисков общих каталогов и совместное их использование в сети. К тому же, сетевая поддержка предусматривалась и для

диспетчера печати (Print Manager) — старинного инструмента Windows для управления печатью и конфигурирования принтеров.

По мере развития сетевых операционных систем, Windows for Workgroup перестала соответствовать современным стандартам. С самою начала в ней поддерживался только протокол NetBEUI, поэтому она позволяла устанавливать связь только с другими сетями Microsoft, состоящими из компьютеров Windows for Workgroup и DOS (с сетевыми надстройками). (Поддержка протокола TCP/IP была доступна только как надстройка, поэтому компьютеры не имели встроенной поддержки Internet.) Тем не менее, эта NOS допускала совместное использование файлов и принтеров, поддерживала функции голосовой связи и офисной электронной почты. Буфер обмена (Clipboard) работал с сетевыми данными и позволял с помощью операций вырезки и вставки переносить данные между локальными и сетевыми приложениями. При этом использовался графический интерфейс, который значительно облегчал администрирование сетью но сравнению с интерфейсом командной строки. Это соответствовало требованиям, предъявляемым ктогдашним NOS. Тем не менее, Windows for Workgroup не получила широкого признания на рынке NOS, хотя для своего времени была неплохой операционной системой небольших сетей.

Windows 95

Операционная система Windows for Workgroup была достаточно хорошей, однако не содержала обширного набора функциональных средств и большинство пользователей Windows стремились обновлять текущую версию операционной системы. Работу в сети допускала и Windows 3.x — просто для этого требовалась соответствующая надстройка от Microsoft или Novell. Переход же на сетевую версию обычной операционной системы не был популярным у пользователей.

Первое серьезное достижение в сетях Windows появилось три года спустя, в конце 1995 г., когда фирма Microsoft выпустила операционную систему Windows 95. Возможно, вы припомните шумную рекламу, которая сопровождала ее появление. И хотя реклама все несколько преувеличивала, новая NOS действительно отличалась от предыдущей.

Она была действительно операционной системой, а не графической средой для DOS. Кроме того, в Windows 95, кроме 16-битовых, входили и 32-битовые компоненты. В большинстве случаев они работали в защищенном режиме, вместо использования обычной памяти в реальном режиме. Поэтому управление памятью намного упростилось. Новая 32-битовая файловая система VFAT (Virtual File Allocation Table - виртуальная таблица размещения файлов) допускала использование длинных имен файлов — разумеется, если ваши приложения тоже были 32-битовыми и допускали использование длинных имен.

Примечание

По существу, файловая система VFAT - это система FAT, дополненная средствами работы с длинными именами файлов.

В Windows 95 была встроена поддержка протокола TCP/IP и IPX/SPX-сов-мсстимого протокола. Поэтому она могла связываться с сетями NetWare или Internet без отслеживания текущих и установки новых сетевых протоколов. Кроме того, она продавалась в комплекте со средствами создания 32-битовых клиентных сетей как NetWare, так и Microsoft.

Как можно оценить эффективность применения Windows 95 в качестве NOS? Для одноранговых сетей — весьма положительно. Например, интерфейсы для совместного использования файлов и принтеров весьма просты. Однако Windows 95 недоставало того же, чего и всем одноранговым NOS - средств защиты и эффективного совместного использования аппаратных средств (за исключением дисков и устройств CD-ROM). Тем не менее, эта операционная система получила широчайшее признание на рынке, в связи с чем стало возможным создавать сети, работающие под управлением Windows 95. Эта операционная система более пригодна для операционной системы клиентной машины, а не сервера сети, однако для небольших

сетей, которым не требуется особое распределение функций, она была и остается вполне пригодной.

Windows 98

В конце 1998 г. Windows 98 еще не успела вытеснить Windows 95. Эта операционная система не так глубоко отличается от Windows 95, как Windows 95 от WfWg, однако в ней предусмотрены дополнительные средства, благодаря которым она лучше приспособлена к работе в сети, чем Windows 95.

В Windows 98 предусмотрено большее число средств для взаимодействия с сетью. В этом отношении Windows 95 имела недостатки: она поддерживала только устаревшие сети NetWare. Клиенты Microsoft Windows не могли получить доступ к службам каталогов новейших версий NetWare. Кроме того, не поддерживался протокол IP сетей NetWare. В качестве транспортного протокола для связи с сетями NetWare можно было использовать только протокол IPX/SPX (и совместимые с ним). В Windows 98 включено большее число средств NetWare, в том числе функция, позволяющая компьютеру, оснащенному Windows 98, связываться с серверами NetWare с помощью системы NDS (NetWare Directory Services — служба каталога NetWare). Компьютер, работающий под управлением Windows 95, вынужден использовать базу регистрационных данных (bindery), которая входила в состав NetWare 3.x и старших версий и уже несколько лет не применяется.

Несмотря на то, что система Windows 98 проектировалась, в основном, для работы в качестве клиентной (а не серверной) операционной системы, она может работать также и в качестве серверной системы. Надстройка Peer Web Server (одноранговый Web-сервер) позволяет создавать Web-узлы в офисах только с одноранговыми сетями. Более того, компонент Remote Access Dial-Up Server (удаленный сервер с коммутируемым доступом) позволяет пользователям входить в сеть или в сервер с удаленным доступом Windows 98, поскольку сервер предоставляет только локальный доступ, а не доступ ко всей сети. Очень полезна и поддержка FAT32 — файловой системы, способной работать с жесткими дисками емкостью до 2 Тбайт. Именно благодаря поддержке жестких дисков емкостью более 2 Гбайт Windows 98 предпочтительнее Windows 95 при хранении большого числа файлов малых размеров.

Возможности Windows 98 ограничены и даже более того — несопоставимы со средствами NOS клиент/сервер, таких как Windows NT. Тем не менее, Windows 98 - вполне приемлемая серверная платформа для небольших и непритязательных сетей.

Windows 98 - конец эпохи

Windows 98 — последняя персональная операционная система Microsoft. По псех дальнейших версиях будет использоваться технология Windows NT, т.е. создаваться унифицированное семейство операционных систем. Эта линия получила название Windows 2000. В неё включены версии Windows, разработанные как для клиентных компьютеров, так и для серверов. Последние, как предполагает Microsoft, должны конкурировать с мэйнфреймами.

Хорошо ли это? Если рассматривать Windows как одноранговую NOS, это, пожалуй, неплохо. В Windows 98 все еще сохранились некоторые нежелательные остатки DOS, а операционные системы, разработанные на основе Windows NT, свободны от них и стабильнее в работе как по сравнению с Windows 98, так и с любой другой персональной операционной системой Windows. Клиентная версия Windows, основанная на Windows NT, выпуск которой ожидается в 1999г., спроектирована для поддержки множества средств, уже несколько лет составляющих основу персональных операционных систем Windows. Окончание разработки исключительно персональных операционных систем Windows отнюдь не ограничивает возможности функциональных средств всех вновь разрабатываемых операционных систем.

С точки же зрения клиентных или автономных операционных систем, эта новость не слишком приятна. Несмотря на то, что персональные операционные системы предъявляют все

большие требования к оборудованию, Windows 98 кажется ягненком по сравнению с теми требованиями к оборудованию, которые предъявляют системы, построенные на базе Windows NT. Кроме того, Windows NT весьма "придирчиво" относится к установленному оборудованию, что значительно усложнит жизнь тем, кому достаточно просто приобрести операционную систему, которую они в состоянии поддерживать в более-менее работоспособном состоянии, а там будь что будет. (На основании личного опыта работы с Windows 98 автор сомневается в ее полной пригодности для одновременной работы с одной сетевой интерфейсной платой и CD-ROM на своем компьютере. Однако большая часть оборудования все еще работает с Windows 98.) Вероятно, фирме Microsoft придется выслушать множество разгневанных потребителей, когда их новые купленные компьютеры после Рождества 1999 г. перестанут работать со старыми сканерами или другим оборудованием.

Еще одна проблема, возникающая у тех, кто присматривает себе новую операционную систему для сервера, заключается в изменениях ядра Windows 2000, сделанных для того, чтобы она стала удобнее для пользователей персональных компьютеров и сетевых клиентов. Windows NT всегда предоставляла средства защиты, которые и не снились Windows 9x. Найти же компромисс между средствами защиты Windows NT и относительной простотой и открытостью Windows 9x не так-то легко.

Все эти проблемы того же порядка, что и недостаток новых 16-битовых приложений Windows — их вполне можно разрешить. Однако вы должны знать, об этом. Отныне и впредь потребителям продукции Microsoft предстоит жить, фактически в "мире NT".

Windows NT Workstation

Опреционная система Windows NT не поддерживает режим Plug-and-Play ("включил-и-работай"). Поддержка сю приложений DOS неравноправна - одни приложения работают, другие - нет. Она пожирает массу оборудования, да еще и с "перебором". Список можно продолжить. Почему же такая NOS лучше, чем Windows 98? По трем причинам.

- Она поддерживает файловую систему NTFS.
- В ней предусмотрена превосходная система защиты.
- Она устойчиво работает.

Если вам нужна внешняя мишура, пользуйтесь Windows 98, но если вам необходим устойчивый и надежный одноранговый файловый и печатный сервер, переходите на Windows NT Workstation 4. Ее интерфейс подобен интерфейсу Windows 95, однако внутреннее содержание иное, как с точки зрения архитектуры, так и средств управления общими ресурсами.

Файловая система NTFS

Как и Windows NT Server, версия Windows NT Workstation поддерживает работу с файловой системой новой технологии (NTFS — New Technology File System). Это — первая файловая система, спроектированная Microsoft, поддерживающая длинные имена файлов, имеющая встроенные средства сжатия (уплотнения) (native compression) и работающая с жесткими дисками большой емкости. Файловая система FAT32 имеет аналогичные возможности, но не имеет таких средств защиты как NTFS — регистрации транзакций (transaction logging), предотвращающих повреждение томов; защиты на уровне файлов и более согласованной их организации.

Несмотря на то, что файловая система NTFS поддерживается только в Windows NT, доступ к ней может получить любой клиент сети. Поэтому ее преимущества доступны поль-

зователям всех операционных систем. До появления FAT32 в составе Windows 95 OSR2 система NTFS была единственной файловой системой Microsoft, которая поддерживала тома (устройства) размером свыше 2 Гбайт. И до сих пор это единственная файловая система Microsoft, которая предоставляет защиту на уровне файлов и обеспечивает ведение протокола защиты (security logging).

Средства защиты

Одноранговые сети, средства защиты входа в систему (logon security), предусмотренные в Windows 9x, оставляют желать лучшего. Если вы пытаетесь войти в систему под правильным именем пользователя, но вводите неверный пароль, процедура входа прерывается. Стоит, однако, ввести новое имя пользователя — и вы в системе. Если вас не беспокоит сетевая поддержка, вы можете нажать на <Escape> при появлении входной заставки "Добро пожаловать в сеть" (Microsoft Welcome to Microsoft Networking) и тоже войти в систему. Конечно, вы не получите доступ к зафиксированным общим сетевым ресурсам (persistent network shares) другого пользователя Чтобы создать какие-нибудь новые ресурсы, вы должны присвоить им соответствующие пароли. Однако если вам нужно только получить доступ к компьютеру, это можно сделать одним щелчком.

В одноранговых NOS такое положение имеет неприятные последствия Во-первых, лицо, использующее компьютер, может просматривать всю информацию, которая хранится в нем. В одноранговой сети это будут все рабочие данные штатного оператора, включая и файлы с конфиденциальной информацией. Во-вторых, это лицо может изменять сетевые ресурсы, назначая им новые пароли, удаляя или создавая новые ресурсы, что весьма нежелательно.

В Windows NT Workstation такой проблемы нет: в ней требуется явный вход в систему (explicit login). Если у вас нет учетной записи на данном компьютере, вы не сможете использовать его ни локально, ни удаленно. Предусмотрена, правда, гостевая учетная запись (guest account), однако ее можно блокировать, либо изменять ее пароль, либо установить настолько ограниченные параметры разрешения входа, что лицо, вошедшее по этой учетной записи, не будет представлять никакой угрозы целостности однорангового сервера.
Windows NT может обеспечить все это потому, что в ней предусмотрен инструмент, отсутствующий в Windows 98 и его предшественницах: Диспетчер пользователей (User Manager). Он не столь могущественен, как диспетчер пользователей домена (User Manager for Domains), входящий в состав Windows NT Server. И, тем не менее, диспетчер пользователей можно использовать для создания базы данных учетных записей, устанавливающей не только список лиц, имеющих доступ к компьютеру, но и тип доступа.

В NT суть доступа скрыта в правах и разрешениях. Учетным записям пользователей и групп назначают права, которые определяют, что они могут делать, работая на компьютере или в сети, а файлам и сетевым ресурсам — разрешения. В одноранговой сети вы не можете получить доступ к общему ресурсу компьютера Windows NT Workstation, если у вас нет на нем учетной записи, даже если вы уже вошли в сеть.

В Windows NT Workstation имеется несколько встроенных групп с предопределенными правами. Названия групп отражают их функциональное назначение (табл. 10.1).

Таблица 10.1. Встроенные группы Windows NT Workstation и их функции

Группа	Описание
Administrators (Администраторы)	Мошут администрировать локальный компьютер. Это наиболее могущественная группа
Backup Operators (Операторы резервного копирования)	Могут обходить защиту файлов с целью архивирования файлов так, что даже не имея доступа к файлам, могут выполнять архивирования для сохранения файлов

Guests (Гости)	Гости рабочей группы или домена
Power Users (Квалифицированные пользователи)	Могут открывать общи йдоступ к файлам и принтерам
Users (Пользователи)	Обычные пользователи, без каких либо особых прав

Обратите внимание: обычные пользователи не могут устанавливать общий доступ к файлам Windows NT Workstation. Это могут сделать только члены группы Power Users. Каждая учетная запись входит в одну из групп: однако вы не обязаны пользоваться только перечисленными группами. Вы можете делать следующее.

- Создавать собственные группы с особыми наборами прав.
- Изменять права, предоставленные каждой группе.
- Добавлять или удалять права отдельных пользователей.
- Сделать учетную запись члена сразу нескольких групп. В таком случае права представляют собой сочетание прав объединенных групп.

Примечание

В Windows NT права пользователя "кумулятивные" (накопительные). Иными словами, при анализе учетной записи используются только наименее ограничивающие наборы прав, за одним исключением: право, абсолютно запрещающее доступ, всегда отменяет остальные права, с которыми оно конфликтует.

Если разделы данных сформатированы в NTFS, то в систему можно включить дополнительный уровень защиты. В то время как FAT и FAT32 поддерживают разрешения только на совместно используемые тома (shared volumes) и только на уровне папок, NTFS поддерживает разрешения M.I уровне файлов, как для сетевых, так и локальных ресурсов.

Примечание

По умолчанию каждый, кто получает доступ к компьютеру, имеет полный контроль над файлами. Поэтому если вы используете Windows NT Workstation как одно-ранговую NOS, рекомендуем установить разрешения на использование файлов.

Повышенная устойчивость

Если вам приходилось достаточно долго работать с любой персональной ОС Microsoft Windows, вам нередко приходилось перезагружать ПК после того, как какое-либо приложение или иная программа сбивалась и разрушала операционную систему. Разумеется, сбой Windows NT тоже возможен, однако это происходит значительно реже, чем в персональных операционных системах Windows. Для сетевых операционных систем это очень важно Разрушение ресурсов сервера вам совершенно ни к чему.

Будущее Windows NT Workstation

Если вас интересует будущее, то у Windows NT Workstation его нет • в конце 1998 г. Microsoft переименовала пятую версию этого продукта в Windows 2000 Professional. (Такое, достойное порицания, решение вызвано маркетинговыми соображениями. Оно необходимо, чтобы присвоить торговую марку, которая в настоящее время отождествляется со стабильностью и надежностью, продукту, ассоциирующемуся с показным блеском и ненадежностью.) Это объясняется тем, что Microsoft опасается потери доверия к торговой марке Windows.

Каковы же новые средства Windows 2000? Эта книга не посвящена целиком Windows

NT, но с точки зрения NOS, в Windows 2000 будет обеспечена лучшая защита с помощью системы Kerberos (подробнее см. гл. 14) и внесены некоторые изменения в файловую систему NTFS, повышающие ее гибкость. Windows 2000 поддерживает режим Plug-and-Play, который был в системах Windows 9x. Кроме того, предусмотрено большее число инструментальных средств управления системой, новая версия броузера Microsoft и пр. Большинство изменений, в основном, применимы к версии клиент/сервер. Поэтому они подробнее рассматриваются далее, в разделе "Microsoft Windows NT".

Сетевые операционные системы клиент/сервер

С точки зрения пользователя, важнейшей частью сети, безусловно, являются клиенты, а не серверы. Как следует из самого слова "сервер" (обслуживающее устройство), сам смысл существования сервера заключается в обслуживании клиентов. Ну, а раз так, что же необходимо клиенту?

- Быстрый и простой доступ к данным и пространству для их хранения.
- Гарантия целостности данных.
- Надежная защита данных.

Чтобы добиться выполнения этих требований, в сетевых операционных системах используют разные подходы. Но между различными NOS есть и значительное сходство, поскольку производители видят, чем занимаются конкуренты и стараются перенять их достижения. В этой главе рассматриваются три широко известные операционные системы клиент/сервер: NetWare, Windows NT и UNIX.

Прежде всего, мы обсудим общие черты операционных систем, затем перейдем к некоторым различиям в характеристиках каждой системы. Конечно, это не будет исчерпывающим руководством по всем трем NOS, однако, прочитав эту главу, вы ознакомитесь с их основными средствами и получите представление о работе с ними.

Общие средства

Чем больше изменений, тем больше и сходства. По мере развития сетевых операционных систем, между ними появляется все больше сходств. В самом деле, производители смотрят друг на друга и думают: "Черт побери! Это хорошая идея. Наверно, она понравится людям. Следует использовать ее и в нашей NOS". Из-за таких решений получили широкое распространение графический пользовательский интерфейс (GUI — graphical user interface), заменивший интерфейс командной строки (command-line interface); поддержка средств работы с каталогами; улучшенная система защиты (защита паролями, шифрованием данных); службы архивирования и т.п. Конечно, не все перечисленные средства входят в любую операционную систему, однако они либо разрабатываются, либо доступны как часть пакетов надстроек (add-on pack), таких как Microsoft BackOffice.

Совет

Многие средства NOS нередко предоставляются и независимыми поставщиками, предлагающими средства, отсутствующие в NOS. Так, в качестве программных средств независимых разработчиков поставляются программы архивирования, поддержка RAID и средств работы с каталогами.

Быстрый и простой доступ

Если вы спросите кого-нибудь, чья работа зависит от сети, что бы он хотел от NOS в первую очередь, чаще всего вам ответят: "Что-нибудь с хорошим откликом и надежное". Ниже перечислены средства NOS, которые спроектированы с учетом этого пожелания.

Унифицированный вход в систему. Основная цель разработки сети заключается в том, чтобы проблема доступа к общим ресурсам стала для сетевых клиентов настолько незаметной, насколько это возможно. Это означает, что совместное использование ресурсов должно осуществляться на базе сети (или части сети), а не на базе отдельных серверов. Что же это значит? Как показано на рис. 10.1, если доступ к общим ресурсам предоставляется на базе сети, клиенту достаточно один раз войти в сеть, чтобы получить доступ ко всем сетевым ресурсам. Если же доступ можно получить только на базе отдельных серверов, клиенты вынуждены связываться отдельно с каждым сервером, начиная с сетевого сервера входной регистрации (network login server), а затем переходить от него к ресурсам, разбросанным по всей сети.

Рис. 10.1. В идеальном случае ресурсы совместно используются группой пользователей, а не отдельным компьютером

Совместный доступ на базе сети не всегда означает, что вход в сеть сразу же предоставит немедленный доступ ко всем общим ресурсам. Для большинства пользователей это скорее будет источником лишних хлопот, чем подспорьем, по мере того как они будут сортировать ненужные ресурсы. Но в то же время это позволяет, войдя в сеть один раз, получить доступ сразу ко всем ее ресурсам.

Средства обслуживания каталогов. Ключ к облегчению использования ресурсов — оптимальная структурная организация объектов и хорошие инструменты поиска. Три сетевые операционные системы, описываемые в этом разделе, поддерживают средства обслуживания каталога как современных (NetWare и UNIX), так и грядущих версий операционных систем. В последнем случае имеется в виду Windows NT. В настоящее время в ней отсутствуют соответствующие средства обслуживания каталогов, однако это предусмотрено в ее новой версии, выпуск которой ожидается в 1999 г.

Примечание

Первой из средств обслуживания каталогов (StreetTalk) была система VINES фирмы Banyan.

Средства обслуживания каталогов - это средства для построения в иерархической структуре объектов сети, причем одни из них могут включать в себя подчиненные объекты, а

другие — нет. Иерархическая структура каталога выглядит примерно так, как показано на рис. 10.2.

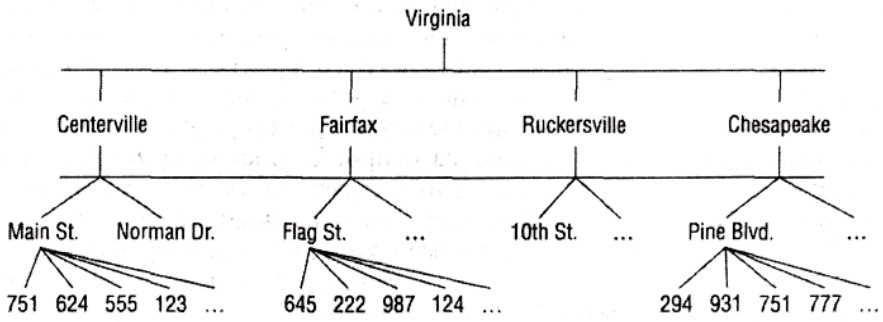


Рис. 10.2. Структура каталога

На рис. 10.2 в качестве примера построения иерархической структуры объектов (не обязательно каталогов) использованы адреса улиц городов штата Вирджиния. Корнем служит название штата "Вирджиния". Ниже расположены названия городов, под ними — названия улиц, а еще ниже — номера домов.

Если применить схему присвоения имен, используемую средствами обслуживания каталогов, то каждому дому будет присвоен примерно такой идентификатор.

```
751.Main Street.Centervilie.Virginia
```

Если пользователь применит средства обслуживания каталогов и запросит доступ к данному объекту, то он (объект) будет найден мгновенно. Во-первых, инструмент поиска (использующий такой протокол как LDAP (Light Data Access Protocol) — упрощенный протокол доступа к каталогам) локализует Virginia как корень, находящийся в конце имени.

Обратите внимание: в данной иерархической структуре каталогов, разные объекты могут иметь одинаковое "первое" имя. Весьма вероятно, что дом № 751 по Main Street (Главная улица) в г. Чесапик (Chesapeake) существует и в г. Сентервилле (Centerville), причем на той же улице. Однако это не приведет к путанице, поскольку два дома с одинаковым номером расположены на разных ветвях структуры (рис. 10.3).

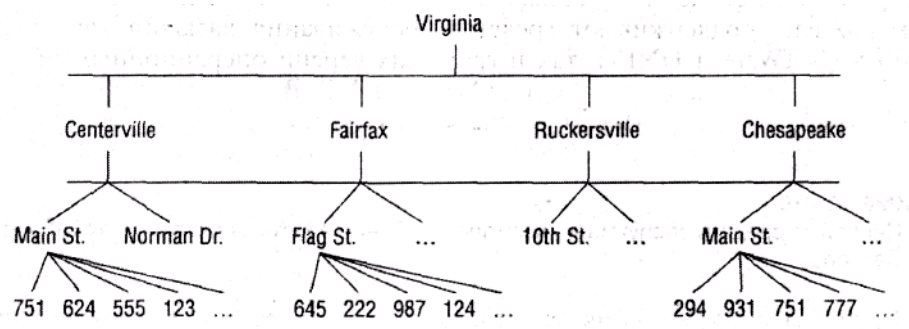


Рис. 10.3. Объекты могут иметь одинаковое "первое" имя, но в то же время находиться на разных ветвях структуры

Безусловно, это зависит от иерархической структуры. Если бы в средствах обслуживания каталога использовались неструктурированные группы (flat groups), объекты идентифицировались бы только по своим "первым" именам — в таком случае использование общих имен стало бы невозможным.

Обнаружить объекты в иерархической структуре несложно, однако организовать их иногда бывает весьма непросто, поскольку место объекта в структуре каталогов определяет, кто сможет получить к нему доступ. Планирование структуры сетевых ресурсов — сложная

задача, поскольку вам необходимо определить места их расположения, гарантирующие доступ тем людям, кому они нужны. Для систем обслуживания каталогов сложность усугубляется ее размерностью.

Расширенная поддержка аппаратных средств. Быстрый и легкий доступ означает не только совместное использование в сети дискового пространства, но также требует от NOS поддержки большого ОЗУ и мощного процессора. Пять лет назад компьютер с процессором 486DX представлял собой вполне приемлемый сервер для (некоторых) приложений. Однако по мере роста требований к серверу, возрастали и требования к поддержке соответствующего оборудования. Сегодня это означает поддержку многопроцессорных систем и процессоров с улучшенной архитектурой. Все три NOS, упомянутые в начале главы, поддерживают (по крайней мере, теоретически) работу системы, содержащей до 32 процессоров. Это, так сказать, теория, далекая от практики. Например, текущая версия Windows NT Server поддерживает работу только четырех внешних процессоров. Для большего числа процессоров можно использовать иную версию HAL (hardware accessibility layer — уровень доступности аппаратных средств) — ту часть NOS, которая обеспечивает ее связь с оборудованием, но реально может работать не более чем с восемью процессорами.

Одна из характеристик расширенной поддержки оборудования — типы поддерживаемых процессоров. В гл. 9 рассмотрены предполагаемые варианты схем процессоров серии x86 в течение 1999 — 2003 гг. Одно из ожидаемых улучшений заключается в применении 64-битовых схем, в отличие от 32-битовых, используемых в настоящее время. В частности, 64-битовые процессоры, начиная от Merced и вплоть до McKinley, будут работать быстрее 32-битовых процессоров вследствие отсутствия в них блоков, ответственных за выполнение некоторых логических функций. Однако поскольку эти логические функции все же необходимы, они будут выполняться операционной системой. В Windows 2000, как и во все новейшие операционные системы, будут встроены средства, поддерживающие 64-битовую архитектуру процессоров.

Поддержка Web-серверов. Поскольку Web жизненно важна для многих фирм (причем как для внутреннего, так и внешнего применения), рассматриваемые NOS могут работать в качестве Web-серверов. С этой точки зрения особую популярность приобрели Windows NT и UNIX. Операционная система Linux (бесплатно распространяемая версия UNIX) также стала популярным продуктом для Web-серверов.

Терминальные серверы. Многопользовательские серверы издавна используются в UNIX, однако для двух других NOS, рассматриваемых нами, это нечто совершенно новое. Как вы узнаете в гл. 12, многопользовательские операционные системы позволяют запускать приложения на сервере с помощью весьма упрощенного сетевого компьютера. Клиентный компьютер отвечает только за вывод изображений, сгенерированных приложением, а не за выполнение сколько-нибудь существенной обработки. Это влечет за собой следующее. Во-первых, клиентные компьютеры могут быть (хотя и не обязательно) крайне упрощенными и, следовательно, дешевыми. Во-вторых, их можно соединить с сервером по медленной линии связи, поскольку между клиентом и сервером передается относительно небольшой объем данных. Кроме того, такой подход повышает эффективность использования ресурсов сетевого оборудования. Это происходит потому, что каждый сетевой клиент, использующий, например, только процессор, загружает его работой лишь в течение небольшого промежутка времени. Многопользовательские системы могут распределять ресурсы процессора в соответствии с потребностями сети, с тем чтобы одно и то же оборудование могло выполнить больший объем работы.

Операционная система UNIX с самого начала проектировалась как многопользовательская. Первоначальную технологию многопользовательских систем Windows NT и NetWare разработала фирма Citrix Corporation, а затем лицензировала ее и для других разработчиков. В настоящее время Microsoft предлагает надстройку для Windows NT, называемую Windows Terminal Server (Терминальный сервер Windows — WTS), однако эта надстройка войдет со-

ставной (но необязательной) частью в ядро следующей версии операционной системы Windows NT.

Инструментальные отладки и оптимизации. Эти инструменты не предназначены для пользователей. Они только помогают улучшить обслуживание сетью нужд пользователей.

- Утилита управления печатью.
- Утилита управления файлами, предназначенная для сжатия, установки разрешений на доступ к файлам и т.п.
- Инструментальные средства удаленного администрирования для конфигурирования клиентных компьютеров и автоматизации установки на них программного обеспечения.
- Инструментальные средства мониторинга сети для отслеживания сетевого трафика и обнаружения "узких" мест.
- Инструментальные средства мониторинга производительности сервера для отслеживания системы показателей, например, процента загрузки процессора, памяти, свободного дискового пространства, пакетов, отсылаемых по сети с помощью какого-нибудь протокола и т.п.
- Ведение журнала регистрации событий (event logging) с записями ошибок, доступа к объектам, входов пользователей, запуска средств обслуживания и т.д.

Использование этих инструментов облегчает управление ресурсами и устранение сбоев.

Средства обслуживания протокола TCP/IP

Благодаря широкому распространению Internet сегодня протокол TCP/IP принят в качестве стандартного сетевого протокола. Однако его использование несколько усложняет сетевое администрирование.

Выделение IP-адресов. Как уже было указано в гл. 4, для идентификации каждого узла в сети TCP/IP необходимо выделить IP-адрес. Как правило, размеры сетей TCP/IP огромны. Этот протокол и его конфигурирование слишком сложны, чтобы поддерживать в небольших сетях (за исключением интрасетей), если они не имеют прямого выхода в Internet. Соответственно процесс назначения индивидуальных IP-адресов каждому сетевому компьютеру вручную слишком трудоемкий. Поэтому в NOS используется средство обслуживания DHCP (Dynamic Host Configuration Protocol — протокол динамического конфигурирования компьютера). Оно поддерживает пул достоверных IP-адресов и выделяет их сетевым компьютерам на заданный период времени. Статический адрес нужен всего нескольким компьютерам (например, основному шлюзу или серверу DHCP), поэтому администрирование сети значительно упрощается.

Определение имен. Хотя компьютерам сети TCP/IP нужны IP-адреса, большинству людей удобнее называть компьютер, скажем, SERPENT (змея), нежели 24.48.12.161. Поэтому, кроме IP-адреса каждому компьютеру следует назначить имя в соответствии с системой NetBIOS, содержащее до 16 символов, либо полностью определенное доменное имя (fully qualified domain name) в формате ftpserver.mycompany.com, а иногда — и оба имени сразу.

Такие имена могут использовать люди, но не сети. Поэтому следует предусмотреть какой-либо метод преобразования имен, удобочитаемых для человека, в имена, с которыми может работать сеть. Вначале наиболее широкое распространение получил метод преобразования имен в IP-адреса с помощью статического списка, называемого файлом HOSTS (если в IP-адреса преобразуются полностью определенные доменные имена), либо LMHOSTS (если преобразуются имена NetBIOS). В принципе, метод работает, однако преобразование занимает слишком много времени, а поддержка файлов становится нелегкой задачей. Действительно, в

каждом компьютере необходимо сохранять собственный файл HOSTS или LMHOSTS, но изменение любого имени или IP-адреса необходимо зафиксировать во всех компьютерах сети. Нечего и думать о поддержке таких файлов одновременно с применением сервера DHCP, если IP-адреса компьютеров могут полностью изменяться каждые несколько дней.

Решить эту задачу можно только созданием сервера определения имен, и именно это было сделано. Имена NetBIOS, используемые в Windows NT 4 и последующих версиях, преобразуются в IP-адреса с помощью сервера WINS (Windows Internet Naming Service — Система присвоения имен Internet для Windows). Полностью определенные доменные имена, используемые в сетях UNIX и NetWare, поддерживаются сервером DNS (Domain Name Service — служба имен домена).

В компьютере Windows NT проще использовать сервер WINS, поскольку он может динамически обновлять информацию, а отображение имен, выполняемое сервером DNS, статично. Однако последующие версии Windows NT будут поддерживать динамическую систему DNS в сетях, состоящих из серверов W2K и клиентов. WINS будет использоваться для связи с устаревшими сетями (и клиентами) в сети Microsoft.

Доступность и целостность данных

Безусловно, доступ к серверу очень важен, однако если на сервере нет нужных данных или они недоступны, доступность собственно жесткого диска не имеет никакого значения. Поэтому очень важно гарантировать пользователям доступность и сохранность данных.

Архивирование. Архивирование — важнейшая функция любой NOS. Архивированию подлежат не только пользовательские данные, но также информация о системной конфигурации. Таким образом, если понадобится переустановить систему, вам не придется заново вручную конфигурировать компьютер. Кроме того, архивируется структура каталогов, созданная средствами обслуживания (если они используются в системе).

Единственным элементом, который невозможно включить в утилиту архивирования данных на внешнее устройство (но который, тем не менее, нужен), — способность архивирования открытых файлов. Например, утилита Backup, входящая в Windows NT, в процессе работы пропускает открытые файлы, в том числе файлы HOSTS. Эту проблему можно решить остановом программы, использующей открытые файлы, и повторным ее запуском по завершении архивирования. Однако практически это не всегда выполнимо. Немаловажна также возможность установить расписание архивирования, с тем чтобы для начала процедуры архивирования сервера не требовалось вашего физического присутствия. Кроме того, при сохранении больших объемов данных важна поддержка архивирования на нескольких магнитных носителях (кассетах).

Средства, входящие сегодня в состав NetWare и предусмотренные в последующих версиях Windows, позволяют архивировать редко используемые данные и в то же время размещать их на относительно недорогих устройствах хранения большого объема. Если в течение некоторого времени к этим файлам никто не обращался, они перемещаются на архивный носитель (backup media). При этом в главном каталоге поддерживается соответствующий указатель связи (link). Если пользователь вводит команду DIR, нужный файл отображается так, будто он находится здесь постоянно, хотя связь может указывать на ленточный накопитель, оптический диск либо другой носитель. Такая система имеет два недостатка. Первый: получение данных с ленточного накопителя или оптического диска занимает большее время, чем с жесткого диска. В конечном счете, это означает, что пользователь сети (клиент) почувствует разницу в отклике системы, если он щелкнет на указателе связи с файлом, которого в действительности нет на жестком диске, даже если он отображается так, как будто он там есть. Второй: если носитель архива (ленточный накопитель, оптический диск и т.п.) находится не там, где он был в прошлый раз (а указатель связи не был обновлен), может показаться, что операционная система зависла, хотя в это время она безуспешно ищет нужный файл. Данный метод рекомендуется использовать только в том случае, если ваша система (не только система

архивирования, но и конфигурация компьютера) очень статична.

Репликация данных. Один из методов обеспечения постоянного прямого доступа к жизненно важным данным заключается в их репликации на другой сетевой сервер. Если на первом сервере происходит сбой, в работу включается второй — автоматически или вручную. Не следует реплицировать в сети все пользовательские данные, поскольку это требует значительных временных затрат, однако вполне допустимо для данных, которые редко изменяются и необходимы для нормальной работы самой сети. Сюда относятся, например, профили пользователей или сценарии входа в систему. Кроме того, избранные файлы данных, которые нужны многим узлам, можно реплицировать ночью или в период слабой загрузки сети.

Поддержка RAID. RAID (Redundant Array of Inexpensive Disks - избыточный массив недорогих дисков) — общее название нескольких методов использования множества жестких дисков, гарантирующих целостность данных даже при аварии одного из них. RAID-поддержка может обеспечиваться аппаратно (с помощью внешнего массива дисков) либо программно, включением в массив RAID жестких дисков самого сервера. Программная поддержка чаще всего предлагается как дополнительное средство, однако аппаратная поддержка включена в качестве надстройки во все три NOS.

Существует пять видов RAID-поддержки, однако программным путем обычно поддерживают только три.

- 0 (чередование дисков без контроля четности).
- 1 (зеркальное отображение дисков).
- 5 (чередование дисков с контролем четности).

В целях восстановления сбоев рекомендуется использовать RAID видов 1 и 5. При зеркальном отображении дисков используют два отдельных физических диска, на которые записаны все данные. Поэтому если один из них прекращает работу, второй — по-прежнему остается доступным. Чередование дисков организовать сложнее, поскольку требуется совместно использовать несколько различных физических дисков (от 3 до 32 в чередующемся наборе с контролем четности). В данном случае вместо записи данных на единственный диск они (вместе с информацией о четности, которая может использоваться для восстановления утраченных данных) записываются в блоки на каждый физический диск чередующегося набора. При отказе одного из дисков массива, для восстановления данных с этого диска используется информация о четности с других дисков. Неисправный диск необязательно заменять немедленно, однако это следует сделать при первой же возможности, поскольку диск необходим для обеспечения полной защиты массива.

Роль кластеризации. Кластеризация намного эффективнее RAID, поскольку гарантирует доступ к данным даже при полном разрушении сервера. Кластер представляет собой группу из нескольких серверов, соединенных наподобие сиамских близнецов высокоскоростной сетью или линиями связи SCSI.

Как указано в гл. 16, кластеризацию можно использовать не только для обеспечения отказоустойчивости, но и для повышения производительности сервера. Точно так же, как использование множества дисков может сократить время на считывание данных тома (поскольку данные можно одновременно считывать с нескольких дисков), множество серверов, связанных друг с другом в кластер, могут выполнить эту же задачу.

Надежность защиты данных

Сетевым клиентам необходима возможность доступа к своим данным, и в тоже время им необходимо, чтобы никто другой не смог их получить. Операционные системы клиент/сервер спроектированы с учетом требований систем защиты, которые содержат следующие

элементы:

- парольную защиту и возможность установки разрешений на доступ к файлам;
- предоставление прав на доступ и идентификацию системных привилегий (system privileges);
- систему шифрования.

В сетях используются два типа разрешений: что вам разрешено делать, и к каким объектам предоставлен доступ. В данном случае, используя принятый в Windows NT жаргон, назовем их соответственно "правами" (rights) и "разрешениями" (permissions). В операционных системах клиент/ сервер права и разрешения определяются не паролями, а установками системы защиты, которые назначены сетевым клиентам. Сетевой сервер, спроектированный для этих целей, хранит базу данных всех пользователей, имеющих доступ в сеть. После того как пользователю будет разрешен доступ в сеть, его доступ к общим объектам сети (принтерам, каталогам и т.п.) будет определяться в соответствии с разрешениями, установленными для данного объекта.

Защита доступа определяется методами организации сетевых объектов. Например, в Windows NT 4 права и разрешения распределяются на основе идентифицирующего кода (ID) пользователя или группы, а в NetWare разрешения можно предоставить на основе защитных кодов (SID) или по их месту в организации.

Много шума вокруг C2

Многие люди буквально сходят с ума, размышляя о том, имеет ли NOS сертификат C2. Они думают, что его наличие означает официальное тестирование и сертификацию системы на соответствие требованиям, указанным в Оранжевой книге Агентства национальной безопасности США (Сертификат C2 получили операционные системы Windows NT 3.5 и NetWare 4.11, однако Windows NT Server 4 его не имеет). Поэтому в глазах скептиков Windows NT Server официально защищен хуже Windows NT 3.5 или NetWare 4.11.

Это, однако, не так. Обратите внимание на слова "официальное тестирование". Тестирование любого продукта федеральным правительством требует времени (фактически, нескольких лет). NetWare 4.11 выпущена значительно раньше Windows NT 4, поэтому она стоит в очереди впереди (Windows NT 4 все еще находится в процессе тестирования). NetWare 5 вообще не имеет сертификата C2, поскольку выпущена в сентябре 1998 г., но это не означает, что она не получит сертификат.

Что же представляет собою сертификат C2? Вот цитата с Web-узла www.radium.ncsc.mil: "Система, которая оценена как система уровня C2, обеспечивает TCB (Trusted Computing Base — доверительная база вычислений), в которой применяется подход DAC (Discretionary Access Control — Независимое управление доступом) для защиты информации и разрешения пользователям совместно использовать информацию под ее управлением и вместе с другими, точно указанными пользователями, идентификацию и удостоверение подлинности пользователей с целью управления доступом к системе и обязательной подотчетности, защиту доступа к информации, оставшейся от действий предыдущего пользователя и обеспечение аудита защиты связанных событий".

Другими словами, это означает, что системы, имеющие сертификат C2, позволяют пользователям управлять доступом к своим файлам на уровне пользователя (per-user base), предотвращать повторное использование объекта и к тому же способны выполнять аудит доступа. И это все. Некоторые правительственные агентства требуют сертификат C2, прежде чем они смогут начать использовать продукт. Однако при этом не обязательны какие-либо средства защиты системы сверх упомянутых пределов.

Microsoft Windows NT

В современном виде Windows NT появилась в 1993 г. и первоначально разрабатывалась как версия LAN Manager (диспетчер LAN) фирмы Microsoft с отчетливыми признаками операционной системы VMS. (Это не удивительно, поскольку ведущие разработчики Windows NT прежде занимались операционной системой VMS для фирмы Digital, пока Microsoft не переманила их к себе.) Некоторое время в новой NOS использовался интерфейс OS/2, однако растущая популярность Microsoft Windows вынудила принять решение о замене графического пользовательского интерфейса (GUI) OS/2 на интерфейс Windows.

После выпуска Windows NT, средства ее защиты произвели потрясающее впечатление. Но именно сходство с Windows сделало ее популярной (во всяком случае, на первых порах). Это была NOS, которая не требовала больших трудов для изучения. Конечно, вы не станете экспертом по NOS за 1—2 дня, но за это время сможете установить и запустить сеть на основе Windows NT. Это одна из причин ее популярности, и в то же время — тревог по поводу возможного усложнения следующего поколения Windows NT.

За годы своего существования Windows NT прошла долгий путь. Поскольку эта NOS целиком основана на системах, созданных Microsoft, ей понадобилась совместимость с NetWare. Кроме того, Windows NT работает с UNIX. С этой целью в последней бета-версии, выпушенной за время создания этой книги, используется Services for UNIX (Службы для UNIX). И хотя Windows NT не отличается такой же зрелостью, как NetWare или UNIX, за шесть лет существования она значительно выросла.

Домены - основа структуры Windows NT

С точки зрения администрирования, система Windows NT Server основана на доменной структуре. Домен — это набор, содержащий до 10 000 объектов, представляющих компьютеры, пользователей, группы пользователей, файловые объекты (каталоги и файлы), а также принтеры. Каждый объект имеет собственный защитный код (SID), идентифицирующий объект в домене. Домен можно представить как рабочую группу с централизованной базой данных системы защиты. Сеть может состоять из одного или нескольких доменов. Домен, в свою очередь, может состоять из одной или нескольких частей LAN. Как и рабочие группы, домены — административные единицы (рис. 10.4).

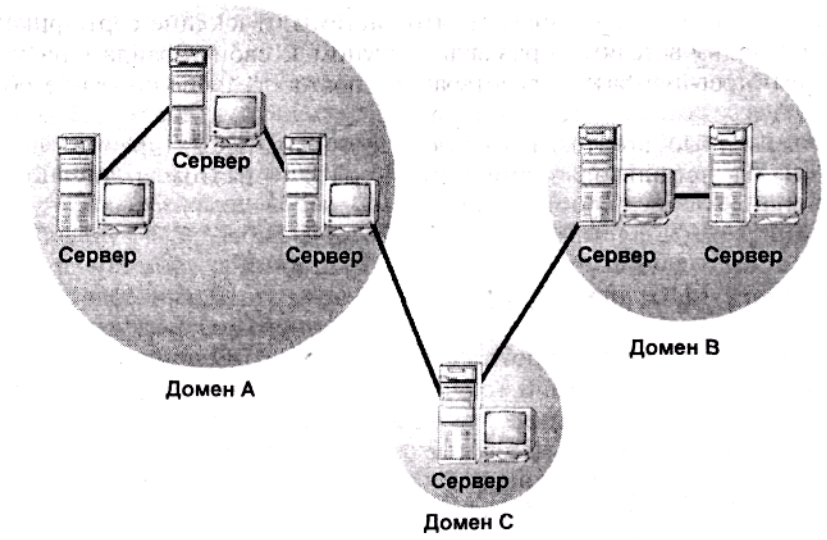


Рис. 10.4. Структура доменов отделена от структуры сети

Примечание

Домены также имеют защитные SID-коды. Вообще-то вы не можете присвоить двум доменам одинаковое имя, однако в данном случае имена предназначены для идентификации

домена пользователем, а не NOS. На этапе просмотра сети схема именования NetBIOS, используемая в Windows NT, не позволяет различить два домена с одинаковыми именами (имя домена отлично от SID). Это означает, что если вы прекращаете использовать один домен, а затем создаете другой домен с тем же именем, вы должны вновь создать защитную структуру домена "с нуля", т.е. он не будет интерпретироваться как старый домен. Точно так же можно переименовать домен, не изменяя его SID.

В домене используется плоская (flat) структура защиты. Иными словами, объекты рассматриваются индивидуально, а не как члены иерархической структуры. Например, не существует группы принтеров, в которую входят все принтеры домена. Наоборот, существуют Принтер1, Принтер2 и т.д., причем каждым придется управлять отдельно.

Система защиты основана на членстве в группе: все учетные записи пользователей относятся к той или иной группе. Каждая группа использует предварительно заданный (но редактируемый) набор прав, ассоциированный с ней. Разрешения на доступ к объектам основаны на разрешениях, предоставленных группам или отдельным пользователям, и определяются как набор свойств в списке управления доступом (ACL — Access Control List). Когда пользователь пытается получить доступ к объекту, скажем, принтеру, операционная система просматривает ACL этого принтера и на основе полученной информации предоставляет доступ на соответствующем уровне. Каждый объект имеет свой собственный ACL.

Защитой же управляют серверы Windows NT особого типа, которые *называются контроллерами домена (domain controllers)*. В них хранится база данных системы защиты домена, идентифицирующая входы пользователей и доступ к объектам. Для идентификации доступа, в домене обязательно должен быть предусмотрен контроллер домена. В Windows NT Server используется двухуровневая система контроллеров. Защиту домена обеспечивает единственный первичный контроллер домена (PDC — Primary Domain Controller). По желанию базу данных системы защиты можно реплицировать на один или несколько резервных контроллеров домена (BDC — Backup Domain Controller), с тем, чтобы они помогали работе PDC по идентификации процесса доступа пользователей. В принципе, домену достаточно единственного PDC, однако в домене желательно использовать хотя бы один BDC. Это необходимо как для равномерного распределения рабочей загрузки, так и для повышения статуса BDC до PDC при отказе первоначально используемого PDC. В то же время излишние BDC нежелательны, поскольку трафик при репликации базы данных системы защиты на BDC может занять немалую долю ресурсов сети.

Доверительные отношения. Хотя управлять однодоменными сетями проще, возможно вам придется разделить сеть на домены по нескольким причинам. Первая: в домен можно включить не более 10 000 объектов, поэтому в очень крупных сетях с множеством объектов вы можете столкнуться с этим ограничением. Вторая причина: PDC должен реплицировать базу данных системы защиты на BDC. Если же доменные контроллеры соединены медленной или перегруженной линией связи, репликация приведет к задержкам трафика.

Если вы логически разделите сеть на множество доменов, то уменьшите трафик примерно так же, как и при использовании маршрутизаторов, физически разделяющих сеть (их применение снижает трафик, фиксируя его в том сегменте, к которому он относится). Кроме того, точно так же, как сетевые маршрутизаторы вызывают задержки, разделение сети на домены затрудняет администрирование. Например, как быть, если вы находитесь в группе домена A, но хотите получить доступ к общей папке домена B? Конечно, это возможно, однако для этого между доменами необходимо установить доверительные отношения (trust relationship).

Доверительные отношения представляют собой обоюдное соглашение между доменами, по которому один домен может использовать ресурсы другого, доверяющего ему. Эти отношения необязательно двусторонние. Фактически, по умолчанию это и не так. Кроме того, они не транзитивны. Иными словами, если домен A доверяет домену B, а домен B доверяет C, то A не доверяет C. Доверительные отношения между доменами A и C следует установить отдельно.

Структура доверительных отношений — одна из причин, по которым Windows NT Server — лучший сервер небольших сетей, состоящих из нескольких доменов. Установка двусторонних доверительных отношений между доменами A и C — настоящая пытка. Для этого

необходимо следующее.

1. В PDC домена A вы должны позволить C доверять A.
2. В PDC домена C вы должны добавить A в список доверительных доменов.
3. В PDC домена C вы должны позволить A доверять C.
4. В PDC домена A вы должны добавить C в список доверительных доменов.

Примечание

Вы не можете просто начать "доверять" другому домену: прежде всего, следует получить от него разрешение. И только после этого, вы сможете доверять домену.

Эти действия должны быть выполнены для двух PDC в приведенном выше порядке. Если же PDC находятся на значительном удалении друг от друга, вам придется немало побегать между компьютерами либо воспользоваться телефоном, чтобы давать указания по ходу процесса. Кроме того, поскольку доверительные отношения не транзитивны, придется повторить эту работу в каждом домене, с которым хотите совместно использовать ресурсы. Далее, вы не сможете просто объединить два домена. Чтобы переместить пользователей из одного домена в другой, необходимо вручную добавить их в этот домен, а чтобы переместить серверы Windows NT их необходимо переустановить и включить в существующий домен. Изменение имени домена не поможет — домены идентифицируются операционной системой не по именам NetBIOS, а по защитным кодам (SID), а отредактировать SID средствами пользовательского интерфейса невозможно. Обеспечение доступа к ресурсам всем доменам. Предположим, что ваша сеть достаточно проста (для создания доверительных отношений), а работа по предоставлению доступа к ресурсам каждого домена членам других доменов еще не выполнена. В операционной системе Windows NT 4 (и ранних версиях) различают два класса групп пользователей: локальные и глобальные. Локальными группами называют такие, которые определены только внутри данного домена, в то время как глобальные — в нескольких доменах. Глобальные группы можно включать в локальные, но никогда — наоборот.

Примечание

Существуют только три глобальные группы: Domain Administrators (администраторы), Domain Users (пользователи) и Domain Guests (гости).

До сих пор все шло гладко. Однако члены одного домена не могут получить доступ к ресурсам другого, если они не входят в глобальную группу. В этом случае вы можете сделать следующее.

- Вручную добавить каждого члена домена A в базу данных учетных записей домена C. Это возможно, хотя и очень трудоемко, а, кроме того, приводит к увеличению размера базы данных системы защиты за счет дублирования записей.
- Предоставить разрешения глобальной группе Domain Users и убедиться, что в нее входят все члены домена A. Однако это означает, что вы должны переустановить разрешения в домене C, чтобы гарантировать необходимый доступ группе Domain Users домена A.
- Вы можете включить в группу Domain Users домена A всех пользователей, которым необходим доступ к общим ресурсам, а затем включить ее в группу Local Users домена C. Это — простейший путь, поскольку всем членам глобальной группы Domain Users домена A предоставляются такие же права и разрешения, как и членам Local Group домена C.

Итак, если вы собираетесь установить между доменами доверительные отношения, рекомендуем включать пользователей в глобальные, а не локальные группы.

Будущее Windows NT Server

С технической точки зрения у версии Server операционной системы Windows NT, как и у версии Workstation, будущего нет. Этот продукт переименован в Windows 2000 Server, а версия Windows NT Server Enterprise Edition получила название Windows 2000 Advanced Server. Через шесть месяцев после выпуска остальных версий Windows 2000 ожидается выпуск версии Windows 2000 DataCenter — дополнительного продукта, предназначенного для конкурентной борьбы на рынке мэйнфреймов. Но поскольку они все еще будут построены на базе Windows NT, замена имени не означает исчезновение самого продукта.

Улучшенная защита. Windows NT позиционируется на рынке как защищенная NOS, однако некоторые стандартные средства ее системы защиты не обеспечивали должной безопасности из-за требований по обратной совместимости. В следующей версии Windows NT предусмотрена поддержка четырех протоколов защиты.

Протокол NTLM (NT LAN Manager). Предназначен для сетевых клиентов, использующих сквозную аутентификацию (pass-through authentication) и для старших версий Windows NT.

Kerberos. Долгие годы используется в сетях UNIX и обеспечивает в каждом сеансе связи двустороннюю аутентификацию (two-way authentication) клиента и сервера.

Протокол TLS (Transport Layer Security protocol — Протокол защиты на транспортном уровне). Следующая версия протокола SSL (Secure Sockets Layer — уровень защищенных гнезд).

Распределенная идентификация паролей (DPA — Distributed Password Authentication). Используется в оперативных службах, таких как Microsoft Network и CompuServe.

Предупреждение

В гл. 14 эти средства защиты рассматриваются более подробно. Сейчас же только укажем, что их необязательно использовать во всех сетях. В целях обратной совместимости с операционными системами, в которых не поддерживаются более совершенные протоколы, в W2K предусмотрена поддержка протокола NTLM (который весьма уязвим). Другими словами, если в вашей сети есть персональные компьютеры, работающие под управлением Windows или старших версий Windows NT, вам придется использовать NTLM.

Более гибкая файловая система. Windows 2000 будет поддерживать новую версию NTFS, в которую включены дополнительные средства.

- Дисковые квоты для мониторинга или ограничения использования диска на уровне пользователя (per-user base).
- Дополнительные атрибуты, позволяющие увеличить гибкость средств поиска файлов.
- Журнал изменений (change log), позволяющий записывать время изменения файлов, а не только их временные ярлыки (timestamps).

Предупреждение

В новой версии NTFS не предусмотрена обратная совместимость с прежними версиями, а выполняемое при ее установке обновление файловой системы необратимо.

С помощью новой версии NTFS можно назначать файлам дополнительные атрибуты и использовать их для сортировки и поиска. Кроме того, в нее включена поддержка архивирования редко используемых файлов на оптические диски и магнитные ленты, предусматривающая сохранение связи с основным каталогом.

Средства обслуживания каталогов. Одно из наиболее широко рекламируемых средств Windows 2000 - средство обслуживания каталогов, называемое Active Directory (Активный каталог). По существу, Active Directory — система организации пользователей, групп, общих ресурсов и установок системы защиты, которые операционная система отыскивает при аутентификации пользователей. Она спроектирована для улучшения управляемости доменной структуры крупных сетей. С этой целью домены логически группируются в "деревья" и "рощи". "Деревья" — это семейства доменов, совместно использующих единое пространство имен, а "рощи" — группы деревьев.

Предполагается, что между доменами, входящими в дерево, устанавливаются транзитивные доверительные отношения (transitive trust relationships), облегчающие связи между ними. Если же в каком-либо конкретном случае полные транзитивные отношения не нужны, их можно заменить односторонними доверительными. (Если же доверительные отношения вообще нежелательны, домен не должен находиться в исходной позиции дерева.)

Примечание

В настоящее время фирма Cisco разрабатывает версию Active Directory для UNIX.

Novell NetWare

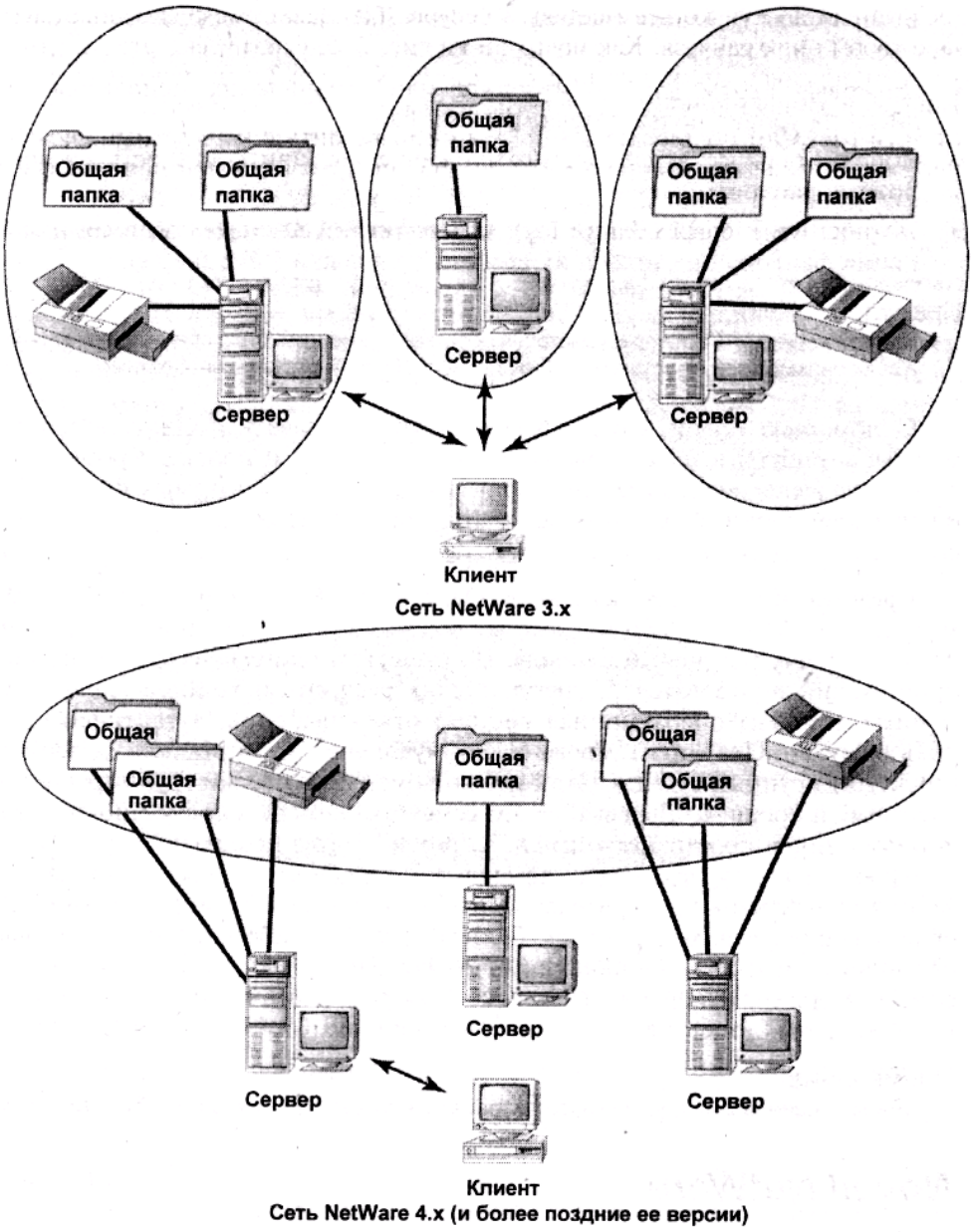


Рис. 10.5. Организация ресурсов в NetWare 3.x и 4.x

С точки зрения предоставляемых средств операционные системы NetWare 5 и Windows NT весьма схожи. С помощью как собственных, так и разработанных независимыми производителями надстроек, они могут выполнять все функции серверной операционной системы. Чем же они различаются? Одно из различий заключается в структуре каталогов NetWare (рис. 10.5), которая радикально отличается от доменной структуры, используемой в современных версиях Windows NT. Как показано далее, в разделе "Структура каталога", она также отлична и от Active Directory.

Источники NOS

Подобно Windows NT, современные версии системы NetWare в своей работе опираются не на индивидуальные компьютеры, предоставляющие общий доступ к своим ресурсам, а на

групповую деятельность, обеспечивая прозрачный доступ ко всем сетевым ресурсам, независимо от компьютера, на котором они хранятся. Как показано на рис. 10.5, фактически это означает отказ от подхода, применяемого в системе NetWare 3.x, в основном опирающейся на использование серверов. В этих сетях для получения доступа к своим ресурсам пользователи должны были входить в конкретный сервер. NetWare 4.x более напоминает Windows NT, потому что в ней используется унифицированная система входа (unified logon system). Это в еще большей мере относится к современной версии NetWare 5, выпущенной в сентябре 1998 г.

Причина такого изменения вполне очевидна. Разумеется, можно организовать вход в индивидуальный сервер сети на 100 пользователей, но это трудоемкая и сложная задача. Выполнить же ее для сети на 1000 пользователей, разбросанных по разным местам, не только трудно, но практически невозможно. Для того чтобы стать расширяемыми, сетям NetWare пришлось превратиться из "набора серверов" в "набор ресурсов".

Структура каталога

Унифицированный вход в сеть NetWare основывается не на доменной структуре, а на системе службы каталогов NetWare (NetWare Directory Services — NDS), которая впервые появилась в 1993 г. в NetWare 4. Если NDS не используется, то каждый сервер NetWare поддерживает собственный плоский файл базы данных (flat-file database) системных объектов, называемый базой регистрационных данных (bindery). С другой стороны, NDS служит глобальной базой данных всех сетевых ресурсов, организованных в многоуровневую иерархию. Эта база данных логически разбита на разделы и распределяется (и реплицируется) по сетевым серверам. Это позволяет решить две задачи. Первая: если один из серверов откажет, структура каталога не теряется и ресурсы по-прежнему остаются доступными. Вторая: пользователь всегда сможет получить доступ к подходящему серверу, вместо того чтобы пытаться войти в сервер по медленной линии связи глобальной сети, или на перегруженный сервер. Возможно, точно также пришлось бы поступить и в домене Windows NT, в котором установлен единственный PDC и отсутствуют BDC, что позволяет распределить рабочую нагрузку.

В NDS могут существовать объекты двух типов: контейнеры и листья (leaf objects). Объекты-контейнеры, как ясно из названия, могут состоять из других объектов, а также организаций (O - Organization) и организационных единиц (OU — Organization Unit). В свою очередь, организационные единицы могут содержать другие организации, или объекты-листья, которые, в основном, представляют собой отдельные ресурсы, а не их категории.

Серверы, пользователи, принтеры и другие объекты-листья могут входить в организации или организационные единицы и идентифицироваться по полностью определенному доменному имени (fully qualified domain name), которое определяется по месту объекта в иерархии. Поскольку в NetWare используют иерархическую систему, ее объекты могут иметь общие "первые" имена и в то же время находиться на разных ветвях дерева.

Совет

Чтобы не слишком усложнять имена, фирма Novell рекомендует создавать деревья каталогов глубиной не более четырех уровней.

Деревья каталогов часто строят соответственно производственным функциям или географическому положению, но в принципе конструкция зависит от вас. Фактически, при использовании NDS конструирование дерева каталогов составляет труднейшую задачу, поскольку от нее зависит доступ клиентов к сетевым ресурсам. В целом, при конструировании дерева основное внимание следует уделять ресурсам, необходимым клиентам, а не их должности или зданиям, где они работают.

Чем различаются NDS и Active Directory

Хотя обе системы называют "системами обслуживания каталога", они различны. Важ-

нейшее различие между ними — метод назначения и хранения разрешений.

Организация разрешений на доступ к объектам. В NDS разрешения на доступ к объектам организованы не в соответствии с кодами групп и пользователей, а в соответствии с организациями (O) или организационными единицами (OU). Если вы перемещаете учетную запись пользователя из организационной единицы (OU) с названием ENGINEERING в единицу, называемую MARKETING, она теряет все разрешения от ENGINEERING, но приобретает все разрешения от MARKETING.

С другой стороны, Active Directory организует разрешения на доступ в соответствии с кодом пользователей и групп, как и доменная система, используемая в Windows NT. Перемещение пользователей из одной организационной единицы в другую совершенно не затрагивает их разрешения. Чтобы изменить набор разрешений пользователя, необходимо удалить его из группы ENGINEERING и включить в MARKETING. Если же вы просто включите пользователя в группу MARKETING и не удалите из ENGINEERING, пользователь сохранит оба набора разрешений.

Какой подход лучше? Это зависит от того, как вы привыкли работать. Если вам проще запомнить набор разрешений, ассоциированный с организационной единицей, то предпочтительнее использовать подход, предлагаемый NetWare, но если вам проще запомнить членство в группе, то, вероятно, вам больше понравится подход Windows NT.

Хранение разрешений на доступ к объектам. В NDS разрешения сохраняются по возможности на самом верхнем уровне дерева каталогов, а затем распространяются на все нижележащие объекты данного дерева. В Active Directory, наоборот, все разрешения на доступ к объекту сохраняются в самом объекте. Поэтому размер объектов Active Directory (и, соответственно, баз данных Active Directory) намного больше, чем в NDS, поскольку они должны сохранять собственные права (rights). Но в то же время такой метод хранения разрешений несколько ускоряет работу операционной системы, поскольку ей нет нужды "подниматься" по дереву, чтобы установить, какие разрешения определены на вершине организационной единицы.

И опять-таки, все зависит от выбора. Тем, кто предпочитает иметь базы данных разумного размера, вероятно, понравится подход Novell. Те же, кому необходим быстрый доступ, оценят метод Microsoft.

Еще одно различие заключается не в организации разрешений, а в организации самого дерева, когда оно охватывает несколько физических местоположений. В Active Directory наименьшей организационной единицей является домен. В NDS же это - раздел, который может иметь меньшие размеры, чем домен. Каждая фирма уверяет в превосходстве своего метода — Microsoft указывает на то, что доменная структура стимулирует концентрацию сетевых ресурсов в одном месте, а Novell обращает внимание на то, что разделение на разделы (partitions) позволяет сегментировать запросы ресурсов и снизить трафик.

Версии операционной системы UNIX

На заре появления сетей, операционные системы и оборудование, как правило, взаимно зависели друг от друга: чтобы запустить компьютер данной модели, требовалось установить на нем операционную систему, спроектированную именно для данного компьютера. Первоначально UNIX была спроектирована фирмой Bell Labs как опытный образец операционной системы со следующими характеристиками.

- Независимость от платформы.
- Совместимость с другими платформами и приложениями, которые придерживались тех же правил.
- Способность к взаимодействию (в том отношении, что UNIX могла работать в сетях различных поставщиков);

Благодаря антимонопольному законодательству фирма AT&T не могла продавать новую NOS (UNIX изначально разрабатывалась как сетевая операционная система), но программа быстро распространилась по исследовательским организациям и учебным заведениям. В последующие годы эти организации создали на основе данной NOS множество взаимно несовместимых и неупорядоченных операционных систем, в которых, тем не менее, сохранилось ядро UNIX. Фактически, существует около 20 версий этой OS. Наибольшую популярность приобрели HP/UX фирмы Hewlett-Packard, SunOS/Solaris фирмы Sun Microsystems, AIX фирмы IBM и другие.

Упрощенная версия UNIX – Linux

В конце 1998 г. широкую популярность начала приобретать одна из версий UNIX, называемая Linux. Со времен ее зарождения в 1991 г. и начала бесплатного распространения в 1993 г. Linux дорабатывалась сотнями программистов всего мира. Причину понять несложно — исходный код Linux распространялся бесплатно, и людям нравилось дорабатывать его, каждому на свой лад. В то же время все внесенные исправления и улучшения становятся всеобщим достоянием. Все стоящие изменения операционной системы санкционируются ее создателем — Линусом Торвальдсом (Linus Torvalds), и отнюдь не всякое изменение вносится в "официальную" версию.

Как можно понять из документов Halloween, упомянутых в гл. 1 при обсуждении модели OSI, фирма Microsoft озабочена угрозой Windows NT со стороны Linux. И на то есть основательные причины. Linux опирается на группу преданных своему делу разработчиков (и многим из них ничего не нужно, кроме доказательства превосходства Linux). Эта сетевая операционная система работает с компьютерами x86, станциями Digital Alphas и Sun SPARC, поэтому она действительно более гибкая, чем Windows NT, которая в настоящее время может работать только на x86 и Alpha. Многих пользователей Linux привлекает относительно скромными требованиями к оборудованию. Так, вы можете использовать ее для спокойного запуска Web-сервера на 486 компьютере. Требования же Windows 2000 намного серьезнее. Кроме того, Linux поддерживается ведущими производителями оборудования и программного обеспечения.

Тем не менее, в настоящее время Linux пока не в состоянии одержать верх над Windows NT. Во всяком случае, это произойдет не скоро. Пользователи пока еще недостаточно заинтересованы в загрузке операционной системы с ftp-узла фирмы RedHat (доступного по адресу www.redhat.com), а те, кто специально ее заказывают, не собираются ее использовать в коммерческих целях. До сих пор большинство установок системы Linux — единичные или любительские по сравнению с установками Windows NT в деловой сфере. Другой аспект, ограничивающий распространение Linux как серверной операционной системы, связан с характером распределения процессорного времени. Windows NT и другие основные коммерческие операционные системы распределяют время процессора для операций ядра (kernel operations) по потокам, а Linux — по процессам, благодаря чему распределение ресурсов процессора намного менее детализировано. Кроме того, потоки, как и приложения, исполняются в пользовательском режиме, а метод постановки последних в очередь ухудшает отклик приложений Linux по сравнению с теми, что созданы для Windows NT и Windows 9x. Фактически, Linux более напоминает систему Windows 3.x, использующую коллективную многозадачность (cooperative multitasking) и требующую, чтобы приложения освобождали процессор по завершении работы, а не многозадачный режим с приоритетами (preemptive multitasking), используемый в 32-битовых версиях Windows, который заставляет приложения освобождать процессор через регулярные интервалы. Наконец, Linux не может эффективно поддерживать многопроцессорное оборудование, поскольку его программный код спроектирован для одновременной работы с единственным процессором. Таким образом, эта NOS не способна работать со многими производственными серверными приложениями.

В настоящее время Linux в основном применяется в качестве исследовательской платформы и платформы для Web-серверов. Однако после некоторых изменений его архитектуры, а также из-за большой доступности для пользователей, он может стать конкурентом Windows NT, по крайней мере, в каком-то сегменте рынка.

Примечание

До сих пор усилия разных производителей UNIX не привели к созданию единой унифицированной версии этой операционной системы, однако работа продолжается.

Что же делает UNIX уникальным? Во-первых, его сетевая файловая система (NFS — network file system), разработанная фирмой Sun Microsystems в конце 80-х гг. NFS позволяет совместно использовать файлы и ресурсы нескольких серверов так, как будто они находятся на одном компьютере. Причем NFS позволяет делать это, даже если ресурсы расположены не просто на разных компьютерах, но и на компьютерах, использующих разные платформы. Так, мэйнфреймы и серверы Windows NT отображаются NFS как совершенно одинаковые ресурсы. NFS экспортирует их, а затем сетевые клиенты монтируют (mount), или подсоединяют ресурсы, когда они им нужны, в соответствии с предоставленными разрешениями, что и составляет основу сетевой технологии клиент/сервер.

Другое нововведение UNIX — сетевая информационная система (NIS — Network Information System), которая необходима всем NOS. NIS представляет собой часть операционной системы, унифицирующей вход в сеть. По существу, это средство обслуживания каталогов для сети, содержащее такую информацию, как пароли, списки групп пользователей, физические адреса, IP-адреса и т.д. Если вам необходимо найти в сети какой-либо компьютер, он должен отображаться где-нибудь в NIS.

Windows NT имеет многие достоинства UNIX, именно поэтому их структура и средства во многом схожи, как было указано ранее, в разделе "Общие средства". Подобно Windows NT, в UNIX встроена поддержка обязательных средств обслуживания файлов и печати, интранет, защиты на уровне объектов, программной RAID-поддержки и т.д. А вот что есть в UNIX, и чего пока нет в Windows NT — отличные возможности расширения. В настоящее время Internet в основном является сетью UNIX с небольшой добавкой Windows NT. И в своем нынешнем состоянии, в другой ситуации, Windows NT не могла бы работать. Просто доменная структура Windows NT не может масштабироваться, а если ее заставить обрабатывать слишком много процессов сразу, то Windows NT разрушится.

Что ждет UNIX в будущем? Это — зрелая операционная система, и хотя, вероятно, UNIX будет в какой-то мере адаптироваться к современным требованиям, ей не требуется какой-либо особой доработки, как Windows NT и NetWare. Действительно, развитие Windows NT и NetWare в основном заключается в добавлении средств, которые уже есть в UNIX. Более существен вопрос выпуска унифицированной версии UNIX, с тем чтобы предоставить пользователям единую платформу, решив тем самым некоторые проблемы совместимости. Однако в настоящее время это представляется маловероятным. Слишком многие понесут крупные убытки, если перейдут на единый стандарт. Более того, политическая обстановка в мире UNIX не поощряет возникновение унифицированного подхода, который возможен, если продукт выпускает единственная фирма, как, например, фирма Microsoft выпускает Windows NT Server или фирма Novell — NetWare. Скорее, нововведения станут более корректными, и Линус Торвальдс (Linus Torvalds) сумеет их оценить. Таким образом, хотя UNIX никуда не уходит и все еще сохраняет популярность в крупных сетях, маловероятно, что она сумеет вытеснить Windows NT и NetWare.

Выводы

В соответствии с отчетом Международной корпорации обработки данных (International Data Corporation — IDC), выпущенном в конце 1998 г., большую часть рынка все еще удерживает UNIX, занимая 45,8% всех серверных операционных систем, проданных в 1997 г. Второе место занимает Windows NT (34,2%), далее следует NetWare (19%). Возможно, доля продаж UNIX возрастет, и это будет сюрпризом для тех, кто предсказывал ее неизбежное вытеснение системой Windows NT.

Примечание

Между прочим, в отчете не указано, как используется каждая сетевая операционная система. Так, UNIX в испытательной среде (test environment) рассматривалась наравне с Windows NT в деловом окружении.

Какая же NOS лучше всех? Это зависит от того, что вы собираетесь делать с ее помощью. UNIX — превосходная гибкая, стабильная и защищенная операционная система для крупномасштабных сетей. Так и должно быть — она работает и развивается уже 30 лет, так что вы можете надеяться, что имевшиеся ошибки уже исправлены. Однако в ней по-прежнему остается узким местом проблема межсетевого взаимодействия с широко распространенными клиентами Microsoft. Кроме того, до сих пор не создана единая версия этой NOS.

Windows NT все еще борется за то, чтобы ее приняли всерьез в крупномасштабных сетях. Это - хорошая операционная система для сетей средних размеров, где ее простота и совместимость имеют большое значение при работе с множеством установленных клиентов Microsoft. Однако в ней все еще не решены проблемы расширяемости, возникающие из особенностей организации ее системы защиты, основанной на доменной структуре. Поэтому на рынке крупных сетей господствуют UNIX и, в меньшей степени, NetWare. Проблему расширяемости частично должно решить включение в следующее поколение Windows NT средств обслуживания каталогов. Однако несмотря на большие надежды, во время создания этой книги Windows 2000 существовала только как вторая бета-версия, поэтому пока еще рано говорить, как проявят себя при испытаниях заложенные в нее хорошие идеи. Кроме того, по-прежнему остаются нерешенными вопросы защиты, хотя это относится, скорее, к следующей версии, в которой предусмотрена поддержка Kerberos — протокола защиты, первоначально разработанного для UNIX. (Интересно, насколько Windows NT станет похожа на UNIX после внесения всех исправлений?)

А NetWare? NetWare постепенно уступает рынок Windows NT, но те, кто ее используют, работают с хорошо обустроенной NOS, имеющей множество средств, которые еще только появляются в Windows NT (средства обслуживания каталогов, реальная поддержка связи с UNIX и т.д.). Кроме
того, в настоящее время работает огромное число серверов NetWare, так что эта NOS не скоро уйдет со сцены.

Итак, на чем бы вы ни остановили свой выбор, в этой главе перечислены все основные, пользующиеся наибольшей популярностью операционные системы, как одноранговые, так и системы типа клиент/сервер. В гл. 11 мы рассмотрим основные типы приложений, которые можно исполнять с помощью этих операционных систем.

Упражнение 10

1. Вы добавили нового пользователя в свою одноранговую сеть, состоящую из компьютеров Windows 95 и Windows NT Workstation. Он пытается получить доступ к общей папке на компьютере Windows NT, однако не может сделать это — система требует ввести пароль для общего ресурса IPC. В то же время, пользователь может получить доступ к любому ресурсу компьютера Windows 95. В чем тут дело?

2. При прочих равных условиях, в какой службе каталога больше размер базы данных: NDS фирмы Novell или Active Directory фирмы Microsoft? Почему?

3. Насколько существенно то обстоятельство, что NetWare 4.11 имеет сертификат C2, а NetWare 5 - нет?

4. В каких случаях UNIX предпочтительнее Windows NT? В каких случаях Windows NT предпочтительнее UNIX?

5. Характеристики Linux более сходны с Windows NT, чем Windows 3.x в том, что относится к распределению рабочих циклов процессора между исполняемыми потоками? Ответьте "да" или "нет".

6. Linux конкурирует со следующими операционными системами.

   A. Windows NT.
   B. Windows 9x.
   C. NetWare.
   D. Ни с одной из перечисленных.

Глава 11

Приложения локальных сетей и их лицензирование

Сетевая операционная система — всего лишь средство поддержки важнейших инструментов локальной сети. В этой главе рассматриваются приложения, которые могут понадобиться вашим сетевым клиентам, и их взаимодействие с сетью. Прочитав главу, вы будете лучше знать возможности, которые может предоставить сеть после установки прикладного программного обеспечения, а также требования к лицензированию программ.

Взаимодействие приложений с сетями

В некоторых случаях приложения выполняются на сетевых компьютерах не так, как на автономных. Одни приложения работают в сети точно так же, как и на автономном компьютере, другие же, наоборот, требуют наличия соединения с сетью, а некоторые при подключении к сети предоставляют дополнительные средства.

Неосведомленные о сети приложения (LAN-unaware applications) не слишком "беспокоятся", подключен компьютер к сети или нет. Единственное дополнительное функциональное средство, которое они могут "заметить" — большее число дисков, где они могут сохранять данные. Однако такое приложение не ощущает разницы между дисками с сетевым и локальным доступом. Примером такого приложения может быть Microsoft Word 97, позволяющий просматривать содержимое Web-узлов.

Осведомленные о сети приложения (LAN-aware application) могут работать и на автономном компьютере, однако при подключении к сети предоставляют дополнительные функциональные средства, которые позволяют им взаимодействовать с другими сетевыми компьютерами. Например, приложению, работающему с базой данных, установленному на автономном компьютере, нет надобности блокировать доступ к записям и файлам, поскольку одновременно его может получить только один пользователь. После того как это приложение начинает работать в сети, ему понадобится такая возможность. Конкретным примером приложения, "распознающего" сеть, может служить операционная система Windows, поскольку ее интерфейс и функционирование средств изменяются при подключении к сети ранее автономной машины.

Зависимые от сети приложения (LAN-dependent application) выполняют работу, которая обязательно требует подключения к локальной сети. Утилиты одноранговой речевой связи (peer chat utilities), офисная электронная почта, групповое планирование и подобные приложения полностью зависят от подключения к сети.

Как работает хорошее сетевое приложение

В большинстве случаев хорошее автономное приложение (stand-alone application) прекрасно работает и в качестве сетевого приложения, поскольку и к тому, и к другому предъявляются в принципе одинаковые требования: оно должно быть простым в использовании,

обеспечивать, необходимые пользователю средства, а также устойчиво работать. К приложениям, предназначенным для работы в тонких клиентных сетях, предъявляются более специфические требования (они рассматриваются в гл. 12). В то же время мобильным пользователям необходимы такие приложения, которые могут повсюду "следовать" за ними.

Независимо от того, какие именно клиентные машины подключены к сети (тонкие или обычные сетевые), сети с мобильными пользователями предъявляют особое требование к пользовательским приложениям: возможность получать доступ к его установкам (user preferences), откуда бы он ни вошел в сеть. В сетях некоторых типов, например Windows, поддерживаются профили пользователя, сохраняются наборы установок — цвета, экранная заставка, содержимое меню Пуск (Start) и т.д. Когда задействованы профили пользователя, установки сохраняются в папке, зарезервированной для данного сетевого клиента. В этом случае, независимо от того, с какого компьютера пользователь Джон войдет в сеть, его рабочий стол будет выглядеть совершенно одинаково.

В профилях пользователя могут также сохраняться установки приложений (application settings), так что Джон увидит не только свою любимую заставку, но также свои пользовательские словари, а также файлы и закладки, сделанные в броузерах документов (browser bookmarks). Единственная тонкость заключается в том, что приложение должно быть спроектировано таким образом, чтобы эти пользовательские установки сохранялись вместе с другой информацией, относящейся именно к конкретному пользователю, но не конкретному компьютеру. В противном случае словари Джона должны храниться на единственном компьютере, но без его персональных установок глобальных параметров, следующих за ним, откуда бы он ни вошел в сеть.

Поясним сказанное выше примером. Предположим, что в понедельник Джон входит в компьютер FROGGIE, работающий под управлением Windows, и использует Microsoft Word 97, а также Netscape Communicator 4.5. Microsoft Word 97 сохраняет пользовательские установки текстового процессора в том разделе системного реестра (Registry) (базе данных системной конфигурации Windows), который относится к пользователю, в данный момент вошедшему в систему. Netscape Communicator, наоборот, сохраняет пользовательские установки части системного реестра, относящейся к компьютеру. Следовательно, когда в четверг Джон войдет в компьютер EGRET и запустит Word и Netscape Communicator, он сможет получить доступ к личным словарям, но не к закладкам. Гарри же войдет в компьютер FROGGIE и получит в свое распоряжение стандартные словари Microsoft Word с закладками Джона.

Конечно, это не самое страшное, что может случиться, однако это достаточно неудобно, поскольку Джон должен всегда использовать один и тот же компьютер либо отказаться от сохранения закладок (несомненное неудобство). В худшем случае это нарушает конфиденциальность его данных и даже представляет потенциальную угрозу системе защиты, что зависит от установок, которые он использовал при настройке Communicator. Таким образом, если вы поддерживаете мобильных пользователей, желательно применять для работы такие приложения, которые сохраняли бы информацию, полученную от конкретного пользователя, вместе с остальными его установками.

Типы приложений

Какие типы приложения чаще всего можно встретить в сети? Фактически — любые, однако их можно разделить на две основные категории.

- Допускающие работу независимых пользователей.
- Допускающие работу пользователя как члена группы.

В следующем разделе описываются приложения обоих типов.

Деловые приложения

Деловые приложения предназначены для персонального использования. Разумеется, проект, над которым работает пользователь, может быть групповым, но с приложением должен работать единственный пользователь. Понятие "деловые приложения" — это почти все, что можно сделать с помощью компьютера.

- Текстовые процессоры.
- Настольные издательские системы.
- Бухгалтерские пакеты.
- Электронные таблицы.
- Клиентные приложения баз данных.
- Программное обеспечение для управления проектами.
- Графические приложения.

Хотя деловые приложения могут использоваться индивидуально, имеет смысл применять какой-нибудь общий формат файлов, с тем чтобы при необходимости разные пользователи могли совместно применять эти файлы. Например, всем клиентам сети желательно пользоваться одинаковыми текстовыми процессорами — это значительно упрощает совместное использование файлов, даже если для их конвертирования из одного формата в другой не приходится прилагать значительных усилий.

Средства координирования

Программное обеспечение для организации связи (communications software) зачастую зависит от сети. Оно используется для таких приложений, как электронная почта, отправление факсов, управление звонками (call management) и во многих других ситуациях, когда пользователям сети необходима связь друг с другом и внешним миром.

Использование электронной почты. Электронная почта прошла путь от занятной игрушки для недоумков (geeks) до обязательного компонента офисной связи. Она не просто "еще один циркуль для вычерчивания окружностей". Скорее, это инструмент обеспечения оперативной и сравнительно конфиденциальной офисной связи. Ее преимущества таковы.

- Для переписки не используется бумага.
- Нет нужды знать местоположение лица, с которым вам необходимо связаться.
- Возможность прилагать к сообщению файлы, необходимые получателю.

При использовании электронной почты следует учитывать, что она обеспечивает только относительную, но не полную конфиденциальность. Даже если удалить сообщение электронной почты, оно не исчезнет полностью. Как правило, копии отброшенных сообщений сохраняются в архиве или другом месте. Как довелось убедиться фирме Microsoft (и не только ей) по ходу изучения ее деловой практики Министерством юстиции США, сообщение электронной почты может использоваться как улика. "Благодаря" сообщениям электронной почты многие фирмы были привлечены к ответственности, поэтому некоторые из них прекратили ее использовать для передачи важной информации.

Использование факсимильных услуг. Возможно, вам уже доводилось использовать программное обеспечение для факсимильной связи. В автономном компьютере оно работает подобно принтеру, перенаправляя печатные задания с параллельного порта на модем, соединенный с последовательным портом.

Точно так же, как работа сетевого принтера отличается от работы локального принтера,

по-разному работают сетевые и локальные средства факсимильной связи. В первом случае сетевые клиенты подключаются к серверу, имеющему программное обеспечение для организации факсимильной связи. Входящие факсы распределяются по клиентам (часто — с помощью почтового сервера, скажем, Microsoft Exchange), чтобы все входящие сообщения поступали в единственный почтовый ящик.

Использование программного обеспечения для управления вызовами. Чтобы объединить электронную почту, факсимильную связь и даже голосовую почту, можно использовать программное обеспечение для управления вызовами. Весь входящий трафик сообщений маршрутизируется на сервер управления звонками (call management server). Для каждого клиента этот сервер выделяет унифицированный почтовый ящик (unified inbox) для приема сообщений всех типов, чтобы они могли найти все свои сообщения в одном
месте.

Групповое программное обеспечение

Групповое программное обеспечение (groupware) — общее название любого приложения, спроектированного для групповой работы. В частности, в "разбросанной" сети, когда трудно собрать всю рабочую группу в одном месте, оно позволяет:

- облегчить связь, повысить ее скорость и качество (в некоторых случаях это единственно возможный тип связи);
- облегчить координацию расписаний встреч и планирование проектов;
- организовать надомную работу или снизить расходы на командировки путем улучшения связи между членами группы, даже если группа разделена.

Вероятно, вы подумали, что именно для этого и создаются сети. Верно. Но в данном случае существует некоторое отличие. Групповое программное обеспечение предназначено для использования не всеми пользователями сети, а только рабочей группой, независимо от ее размеров. В этом отношении оно отлично от приложений, которые предназначены для всех пользователей сети, а не только замкнутого "кружка".

Как правило, для выполнения возложенных на него функций групповое программное обеспечение поддерживает средства электронной почты, голосовой связи, группового планирования, организации личных календарей и списков заданий (to-do lists), репликации документов и прочие функции, необходимые для успешной совместной работы членов группы. По этой же причине групповое программное обеспечение часто называют программным обеспечением "для рабочей группы".

Примечание

В некоторых случаях применяют выражение "программное обеспечение для команды". Так называют любое приложение, спроектированное для совместной работы над проектом группы сотрудников, разбросанных по обширной географической области. Обычно оно работает через Internet. Однако, поскольку в современном групповом программном обеспечении предусмотрена также возможность связи через Internet, это различие несущественно.

Как бы его ни называли, понятно, что в групповое программное обеспечение входят два компонента: клиентный и серверный. Серверные компоненты управляют функциональными средствами группового
программного обеспечения: почтовым сервером, публикацией документов, личными календарями и т.д. Клиентные компоненты организуют (предоставляют) пользовательский интерфейс всех функциональных средств.

В качестве примера современного группового программного обеспечения рассмотрим программу Lotus Notes (в настоящее время фирма Lotus входит в состав IBM). Почему именно

Notes? Отчасти потому, что Notes получила широкое распространение. Notes была создана в 1989 г. задолго до появления на рынке других подобных продуктов и широко используется американскими корпорациями не только благодаря слабой конкуренции — немало значат ее гибкость и совместимость почти со всеми популярными платформами. Итак, рассмотрим Notes как пример группового программного обеспечения и его эволюцию от локальной сети к Internet.

Эволюция. Первоначально Notes разрабатывался как продукт, предназначенный для мэйнфреймов. Программа получила название PLATO Notes. По замыслу она должна была просто отмечать в отчетах ошибки в датах и кодах пользователей. Однако разработчики, осознав потенциальные возможности продукта, дополнили его имя и возможности. Новый продукт PLATO Group Notes позволял:

- создавать личные предметные папки (personal subject folders);
- создавать списки доступа (access lists);
- выполнять сортировку данных по датам заметок и ответов;
- создавать анонимные заметки;
- размечать (marking up) документ пользовательскими комментариями;
- запускать игру с несколькими игроками.

Сейчас все это выглядит как потертая шляпа, но по тем временам было новшеством. PLATO Notes не пользовалась особой популярностью до середины 80-х гг., когда стало очевидно, что рынок персональных компьютеров угрожает рынку мэйнфреймов. При поддержке Lotus Corporation разработчики создали продукт Notes для персональных компьютеров -первую версию Lotus Notes. Эта версия, официально купленная фирмой Lotus в 1986 г, имела средства организации электронной почты, списков деловых контактов и базы данных документов. Со стороны клиента использовалась либо DOS 3.11, либо OS/2, а на стороне сервера поддерживались DOS 3.1 (или 4) и OS/2.

С момента выпуска в 1989 г. Notes значительно расширился. В настоящее время продукт обеспечивает форматирование документов, прием сообщений электронной почты, групповое планирование и отсылку документов по электронной почте. Кроме того, он поддерживает множество подключений (hookups) к Internet, Web, группы новостей, и даже публикацию документов непосредственно в Web с помощью сервера Lotus Domino. В следующей версии предусмотрено использование интерфейса Internet Explorer, и вам будет нелегко отличить операционную систему Windows 98 от этого группового планировщика. Кроме того, в нем предусмотрены дополнительные инструменты для разработчиков приложений. Notes спроектирован с учетом гибкости и возможности настройки. Тем не менее, его первые разработчики были бы весьма удивлены, насколько популярной оказалась их платформа (development platform).

Средства группового программного обеспечения. По мере неуклонного "сращивания" сетей и приложений оказалось, что некоторые средства группового программного обеспечения можно обнаружить даже в тех продуктах, которые формально не относятся к этой категории. Хорошим примером служит Microsoft Office 97. В частности, уже в несколько поколений текстового процессора Word встроены средства отметки исправлений (revision marking). Отметка исправлений относится к функциям группового программного обеспечения, поскольку позволяет нескольким лицам просматривать один и тот же документ и вносить в него собственные исправления независимо друг от друга. (Каждый раз, когда я получаю на авторский просмотр главу от корректора и технического редактора, я вспоминаю это средство группового программного обеспечения, предусмотренное Microsoft.) Кроме того, как и во всех офисных приложениях, в Word встроен доступ к Web, поэтому его можно использовать для создания документов HTML, сохранения их на Web-сервере и распространения по интрасетям. Возможно, существует более эффективная HTML-кодировка, но, тем не менее, это та же HTML.

Некоторые средства группового программного обеспечения предусмотрены и в системах электронной почты, поскольку они поддерживают не только отправку писем и файлов, но и составление списков заданий (to-do lists), а также встроенные программы-планировщики (integrated schedulers). Так что, хотя термин "групповое программное обеспечение", вероятно, сохранится как категория, по мере распространения сетей следует ожидать включение таких средств во многие приложения.

Лицензирование программного обеспечения

Одно из замечательных достижений (и несомненных преимуществ) сетевых технологий — огромное упрощение проблемы установки приложений на сетевых клиентных машинах. Для установки и обновления программного обеспечения нет необходимости переходить от одной рабочей станции к другой с пачкой дискет — многие приложения можно установить на центральном сервере. Если же приложения невозможно корректно запускать с центрального сервера, то для их установки на клиентные компьютеры можно использовать автоматические инсталляторы (automated installers), например, входящие в состав сервера управления системами (SMS — Systems Management Server) Microsoft, либо более совершенные средства автоматической инсталляции Windows 2000.

Во всем этом есть единственный недостаток, вернее, опасность: вы должны располагать лицензиями на программное обеспечение для всех пользователей, даже если оно устанавливается в одном месте. Покупка одного пакета программного обеспечения отнюдь не означает, что вам автоматически предоставляется право устанавливать его где угодно и позволять использовать его любому числу людей. Это означало бы, что вы допускаете пиратское использование программного обеспечения (software piracy), т.е. нарушаете законы об интеллектуальной собственности, что относится к федеральным преступлениям. Повторяю: вы покупаете не программное обеспечение, а право на его использование.

Предупреждение

Хотя это и очевидно, все же следует подчеркнуть: любое коммерческое программное обеспечение, которое вы загружаете с различных (не фирменных) узлов без оплаты лицензии разработчику, относится к пиратскому. Кроме того, это программное обеспечение - опасный источник вирусов.

Что такое лицензия

Лицензия на программное обеспечение (software license) — это гонорар пользователя: вы оплачиваете лицензию, а затем — право на ее использование по числу пользователей (per head — "по головам") или по числу компьютеров. Очень часто "использование" определяется как "присутствие в ОЗУ". Кроме того, приобретение лицензии предполагает соблюдение производителем правил распространения продукта. В простейшем случае лицензия представляет собой доказательство легального приобретения программы и предоставляется в одной из следующих форм.

- Конверт с дисками или компакт-дисками, на которых распространяется программное обеспечение. Как правило, конверт запечатан наклейкой, на которой написано что-нибудь вроде "By breaking this seal you are agreeing to the terms of the license agreement" ("Нарушив эту печать, вы подтверждаете согласие с условиями лицензионного соглашения").

Примечание

Мой любимый пример соглашения "When you break this seal you demonstrate that you're agreeing to the terms of the license agreement" ("Нарушив эту печать, вы подтверждаете согласие с условиями лицензионного соглашения"), которое принято фирмой Citrix Corporation

для продукта MetaFrame - надстройки терминального сервера Windows (WTS) фирмы Microsoft. Наклейка на компакт-диске сообщает, что, нарушив ее, вы подтверждаете, что прочитали и согласились с условиями лицензионного соглашения. Хитрость заключается в том, что само-то лицензионное соглашение находится внутри запечатанной упаковки компакт-диска. Увы - вам придется открыть ее в любом случае.

- Оригиналы дисков или компакт-дисков.
- Страница в руководстве, озаглавленная "Licensing information" (Сведения по лицензированию).
- Квитанция об оплате программного обеспечения.

Если вы собираетесь устанавливать программное обеспечение многократно, обычно проще купить одно запечатанное приложение (boxed application), а к нему — набор лицензий, чем запечатанное приложение для каждого пользователя, которому оно необходимо. Как правило, пользовательские приложения поступают с единственной лицензией, а сетевые операционные системы — с небольшим числом (5—10) лицензий. Если вам необходимо, чтобы программное обеспечение использовалось большим числом людей, следует приобрести дополнительные лицензии.

Ассоциация издателей программных продуктов (SPA)

Ассоциация издателей программных продуктов (SPA — Software Publisher's Association) — некоммерческая организация, расположенная в г. Вашингтоне, округ Колумбия. Она создана в 1984 г. двадцатью пятью фирмами для защиты прав производителей программных средств. Антипиратская деятельность SPA началась с 1989 г. (организация занимается не только борьбой с пиратским использованием программ). В конце 1998 г. в SPA входило около 1200 коммерческих фирм по разработке программного обеспечения, от самых крупных (например, Microsoft) до небольших фирм, еще только "встающих на ноги".

Большинство антипиратских акций SPA начинается с конфиденциальных сообщений, получаемых по "горячей" линии (тел. 800-388-7478), число которых за день достигает около 30. Служащий, отвечающий по телефону, оценивает сведения на основе представленных фактов, серьезности нарушения и мотивов позвонившего лица. Иначе говоря, он пытается уяснить, действительно ли позвонившее лицо озабочено нарушением правил лицензирования либо действует из чувства мести, а если так, то насколько законна поступившая жалоба? Оценка сообщения основана на чутье агента, предоставленной информации и данных о собственных расследованиях, проводимых SPA.

После того как SPA принимает решение рассмотреть сообщение, она расследует его, проверяя достоверность заявления. Если она не может сделать это, расследование прекращается. Если же SPA в состоянии собрать достаточно информации для проведения аудита, она извещает фирму-нарушителя о том, что она идентифицирована как нарушитель правил лицензирования и сообщает о действиях, которые намерена предпринять.

В большинстве случаев SPA проводит аудит фирмы-нарушителя, в ходе которого аудиторы физически проверяют программное обеспечение каждого компьютера на соответствие доказательствам его приобретения, которые предоставлены фирмой. Часто лучшим доказательством покупки служит счет или ордер на оплату. В среднем аудит занимает шесть месяцев — точное время зависит от размера фирмы и ее готовности к сотрудничеству. Во время аудита фирма все еще может работать в нормальном режиме, не мешая работе аудиторов. Если же аудит подтверждает нарушение, фирма платит SPA штраф, размер которого определяется розничной ценой продукта, а нелегальные копии разрушаются или удаляются. Кроме того, от организации требуют вновь закупить все необходимое программное обеспечение, чтобы все пользователи могли получить доступ к законно приобретенному программному обеспечению.

В более серьезных случаях вместо аудита SPA предъявляет гражданский иск фирме-нарушителю. SPA имеет разрешение от всех ее членов проводить от их имени аудит,

однако для предъявления судебного иска должна получить отдельное согласие. Если судебный процесс проходит успешно, фирма-нарушитель должна уплатить до 100 000 $ за каждое гражданское правонарушение и до 250 000 $ — за каждое уголовное (если соответствующая сторона предъявляет уголовное обвинение). Как и ранее, все нелегальные копии уничтожаются.

В самых драматических случаях SPA может запросить у судьи ордер на внезапный "рейд" на подозрительную фирму-нарушитель. В этом случае аудиторов сопровождает федеральный судебный исполнитель, чтобы защитить их и объявить, что они имеют право находиться в данном месте. Это звучит драматически, но фактически сводится к внезапному аудиту. Защитные действия SPA обычно распространяются на фирмы, входящие в нее — это не федеральное агентство и не карательная организация. Это означает, что если SPA получает "наводку" на нарушителя правил лицензирования программного обеспечения фирмы, которая не входит в SPA, она не предпринимает каких-либо действий. Однако если нарушение достаточно велико для начала преследования, то весьма вероятно, что, в конце концов, будет обнаружено и нарушение прав лицензирования члена SPA. В таком случае возможна та или иная проверка. Если SPA сумеет собрать достаточную информацию для начала аудита, она выполнит его, даже если пострадавшая фирма не является членом SPA. Это не влечет каких-либо последствий для фирмы-нарушителя, поскольку все штрафы выплачиваются SPA, а не пострадавшей фирме. Впоследствии штрафы используются для финансирования расследований и воспитательных компаний, проводимых для поощрения использования законного программного обеспечения, а также оплаты труда работников SPA.

Лицензированию подлежит отнюдь не всякое программное обеспечение. Существуют следующие категории лицензированного программного обеспечения.

Коммерческое программное обеспечение. Основной источник дохода коммерческих разработчиков, таких, как Microsoft, Lotus, Adobe и других. Оно предназначено для продажи, не подлежит перепродаже и обычно выпускается только в конечном формате (final format), а не в виде исходного, не компилированного кода.

Ограниченное опытное программное обеспечение. Обычно это демонстрационные версии коммерческих продуктов (усеченные и/или предоставляемые на время), предназначенные для стимулирования объема продаж коммерческих версий. Иногда ограниченное опытное программное обеспечение распространяется и бесплатно.

Испытательные (условно-бесплатные) версии программ (shareware). Как и коммерческие, испытательные версии программ содержат все функциональные средства коммерческой программы. Так же как и бесплатное или ограниченное опытное программное обеспечение, испытательные версии программ могут распространяться бесплатно. Если использовать их дольше оговоренного для испытаний срока (в зависимости от продукта 10, 30 или 60 дней), то в соответствии с правилами лицензирования их требуется оплатить. В большинство испытательных версий не закладывают "бомбы замедленного действия". Вместо этого используют "назойливые экраны", напоминающие о необходимости зарегистрироваться по окончании оценочного периода.

Примечание

По форме оплаты некоторые испытательные версии программ подобны бесплатным программам: например, имеется одна испытательная программа, автор которой требовал в качестве оплаты отправить ему домой в Австралию пиццу. И в самом деле, несколько раз ему посылали пиццу, однажды даже из Германии.

Бесплатное программное обеспечение (freeware). Бесплатные программные про-

дукты также имеют полный набор функциональных средств (по сравнению с испытательными и коммерческими версиями более ограниченный) и могут беспрепятственно распространяться далее. Есть типы бесплатного программного обеспечения, которые представляют собой "усеченные" опытные образцы, есть и другие — они распространяются ради самого распространения.

Программное обеспечение некоммерческого использования. Некоммерческие организации и отдельные пользователи могут использовать продукт бесплатно, но коммерческие учреждения должны их оплачивать.

Не требующие авторского вознаграждения двоичные файлы (royalty-free binaries). Программное обеспечение, которое можно свободно использовать и распространять только в двоичном формате (binary form).

Открытые программные средства. Допускается свободное распространение двоичных файлов и кодов. Разработчики некоторых открытых программных средств (например, Linux) требуют, чтобы все изменения, вносимые в них, становились всеобщим достоянием.

Подводя итог, можно сказать, что лицензия необходима как для коммерческого, так и для некоммерческого программного обеспечения. Исключения допускаются для некоммерческих учреждений и испытательных версий программ. В остальных случаях вы можете использовать и распространять программный код только в рамках пользовательского соглашения. Иными словами, вы столкнетесь с проблемами лицензирования, даже если какой-нибудь программист во время обеденного перерыва начнет ковыряться в программном коде Linux или Mozilla.

Типы лицензий

Лицензии различных типов предоставляют разные возможности и привилегии. Чаще всего лицензии распределяют соответственно количеству пользователей или компьютеров, которые будут выполнять данное программное обеспечение. Кроме того, в зависимости от конкретного продукта программное обеспечение может лицензироваться для всей сети, узла или предприятия в целом (эти варианты рассматриваются в следующих разделах).

Лицензирование по количеству пользователей. Лицензия по количеству пользователей дает владельцу лицензии право загрузить программное обеспечение в любое число компьютеров при условии, что использовать их будет только владелец лицензии. Например, если вы владеете настольным и портативным компьютерами, вы можете загрузить в них свой любимый текстовый процессор, но использовать его можете только вы. Однако нельзя установить его на собственный компьютер и на компьютер вашего приятеля либо разрешить ему пользоваться вашим портативным компьютером, а самому запустить то же самое приложение на настольном компьютере. Лицензирование по количеству пользователей предусмотрено во многих клиентных приложениях, однако прежде чем принять эти условия, внимательно прочтите лицензионное соглашение и убедитесь, что оно устраивает вас.

Для сетей лицензирование по количеству пользователей можно назвать "лицензированием по числу сеансов" выхода в сеть. Если вы загрузили лицензированное программное обеспечение (NOS или пользовательское приложение) в сетевой сервер, и пользователь может получить к нему доступ, то само по себе это отнюдь не означает расходование лицензии по числу сеансов. Лицензия расходуется только тогда, когда пользователь получает доступ к этим продуктам. Например, если в вашей сети работает сервер Windows NT, а у вас есть лицензия на 10 пользователей, то рядовой пользователь (Joe User), приступив с 9 часов утра к работе, не использует лицензию. Однако если он войдет в сервер Windows NT, то израсходует (займет) одну из 10 лицензий.

Лицензирование рабочих станций (по количеству рабочих мест). Лицензирование рабочих станций (workstation license) позволяет одновременно использовать программное обеспечение только на одном компьютере. Оно подобно лицензированию по количеству пользователей, однако право "предоставляется" компьютеру, а не пользователю. Следовательно, вы можете совершенно легально использовать свой портативный компьютер с загруженным текстовым процессором на пару с товарищем. Однако вы уже не имеете права загружать текстовый процессор как в настольный, так и портативный компьютер, хотя они находятся в вашей полной собственности.

В сетевой среде лицензирование по количеству рабочих станций можно назвать "лицензированием по количеству рабочих мест" (per-seat). Например, то, что клиент может получить доступ к сетевому приложению, теперь означает расходование лицензии. Это не так уж плохо, как может показаться. С одной стороны, если в вашем офисе установлено 20 клиентных компьютеров, и все они могут получить по сети доступ к программному обеспечению, то вам придется приобрести лицензию для каждого компьютера. С другой стороны, если офис работает в три смены, и каждый день каждый клиентный компьютер используют три сменщика, то вам не придется оплачивать их лицензии.

Лицензирование сети, узла и предприятия. Как указано выше, большая часть программного обеспечения лицензируется по количеству пользователей или по количеству компьютеров, даже если оно продается блоками на 50 или 100 пользователей. Однако иногда встречаются лицензии для групп, а не отдельных пользователей. Сетевая лицензия (network license) предоставляет право применять приложение всем клиентам локальной сети. Лицензия на использование узла (site license) позволяет работать с приложением в офисе или здании независимо от числа пользователей и установленных локальных сетей. Наконец, лицензия на предприятие (enterprise license) предоставляет право применять программное обеспечение всем работникам предприятия, независимо от их численности и места нахождения.

Разработка и реализация политики лицензирования

Итак, вы знаете, на какое программное обеспечение следует приобрести лицензии и каковы их типы. Как же гарантировать выполнение лицензионных соглашений?

Чтобы гарантировать лицензирование всего программного обеспечения на предприятии, следует решить две основные проблемы. Первая: следует убедиться, что в сети нет нелицензированного программного обеспечения (испытательных версий программ и самовольно установленных приложений). Вторая: вы должны иметь возможность доказать, что с данным пакетом программ работает только оговоренное в лицензии число пользователей.

Первая проблема решается "полицейскими" мерами - следует убедить пользователей не устанавливать какое-либо программное обеспечение без разрешения сетевого администратора или другого ответственного лица. Если вы не доверяете работникам, можно блокировать на клиентных сетевых компьютерах дисководы и устройства CD-ROM. Можно даже физически снять (демонтировать) жесткие диски (и дисководы) и перейти на бездисковые терминальные устройства, рассмотренные в гл. 9 (подробнее — в гл. 12). Однако если пользователи сети имеют доступ к Internet, вы должны постоянно сохранять бдительность. Для людей без предрассудков Web — обильный источник любого программного обеспечения, в том числе коммерческого. Для его загрузки не нужны ни дисководы, ни устройства CD-ROM.

Для решения второй проблемы, как показано ниже, следует использовать либо ручное, либо автоматическое отслеживание и мониторинг программного обеспечения (software metering and monitoring).

Отслеживание вручную. В небольших сетях, где программное обеспечение загружается локально, его состояние можно отслеживать вручную. В одной небольшой компьютерной фирме, к примеру, пользователи были достаточно компетентны для того, чтобы взять на себя ответственность за используемое программное обеспечение. Каждой программе был присвоен

номер, и этот же номер был присвоен служащему. Каждый служащий отвечал за физический доступ к дискам, предназначенным для установки программных средств на его компьютер. Кроме того, каждый пользователь составлял личный список программного обеспечения, установленного на компьютере, и передавал его коммерческому директору. Эта информация сохранялась на твердом носителе, но могла быть без труда введена в базу данных пользователей.

Совет

Если вы решите использовать эту модель отслеживания лицензирования программного обеспечения, присваивайте пакетам программ номера, а не имена. В противном случае, когда Джиллиан (Jill) уволится из фирмы, а на ее место поступит Тимон (Timon), ему будет предоставлен "набор программ Джиллиан".

Ручное отслеживание возможно не всегда. Во-первых, оно требует от клиентов сети ответственности и загружает дополнительной работой. Если же ваши клиенты безалаберны, такая система отслеживания бесполезна. Во-вторых, физическая охрана дисков не всегда возможна. Если пользователи обеспечивают физическую охрану своего программного обеспечения, то каждая рабочая станция начинает занимать слишком много места в помещении, а это не всегда возможно. Кроме того, клиенты сети имеют возможность самовольно устанавливать любое программное обеспечение. Помимо очевидного нарушения лицензионных соглашений, при этом возможно заражение компьютера вирусами, если они есть на домашней машине. Поэтому по возможности, даже если вы используете ручную систему отслеживания, предусмотрите блокировку программного обеспечения, чтобы оно использовалось только при необходимости.

Ручное отслеживание несовершенно, однако в небольших сетях с хорошо подготовленными пользователями — это простейший путь следить за установленными программными средствами. В одноранговых же сетях только оно и оказывается возможным, поскольку они не поддерживают иные средства для отслеживания состояния программного обеспечения.

Отслеживание и мониторинг программного обеспечения. В крупных сетях типа клиент/сервер учет использования системных ресурсов слишком сложен, чтобы выполнять его вручную. В этом случае можно воспользоваться многочисленными программами отслеживания и мониторинга программного обеспечения как независимых разработчиков, так и встроенных в NOS.

Чем различаются отслеживание (metering) и мониторинг (monitoring)? В основном, системами управления, но отнюдь не фундаментальными различиями структуры. Так, некоторые программы отслеживания (metering programs) могут использоваться и для мониторинга. Отслеживание предотвращает нарушения, сравнивая текущее число клиентов, получивших доступ, с числом разрешенных подключений. Например, если лицензия на данное приложение допускает одновременную работу 50 пользователей, а с ним пытается связаться пятьдесят первый, он получит сообщение об ошибке, указывающее, что приложение в настоящее время недоступно. Мониторинг означает только "слежение" за соединениями и занесение их в журнал, использующийся в дальнейшем для справок, позволяя тем самым точно определить число пользователей, конкурирующих за доступ к приложению.

Выводы

Сетевые приложения - это часто те же самые приложения, что используются в обычных автономных компьютерах: текстовые процессоры, электронные таблицы, настольные издательские системы и т.д. В то же время специализированные коммуникационные приложения, например, электронная почта, управление вызовами и групповое программное обеспечение, как правило, предназначены только для работы в локальных сетях.

При использовании приложений любого типа вы должны убедиться в их надлежащем лицензировании в соответствии с правилами, установленными производителями. Еще раз напомним, что вы покупаете не программу, а лицензию на ее использование. Если не приобретете для своей организации достаточное число лицензий, то можете понести ответственность, даже подвергнуться уголовному преследованию, если нарушение окажется достаточно ощутимым для производителя программного обеспечения, и он начнет тяжбу. Чтобы избежать такой ситуации, следует организовать учет программного обеспечения, используемого в сети. Это можно сделать либо вручную, либо воспользоваться программами автоматического отслеживания и мониторинга. Надлежащее лицензирование необходимо как при загрузке приложений на каждый клиентный компьютер, так и на сервер приложений, либо на сервер терминала, работающий под управлением многопользовательской операционной системы тонких клиентов. Серверы терминалов и тонкие клиентные сети рассматриваются в гл. 12.

Упражнение 11

1. Ваша офисная сеть состоит из 20 сетевых клиентных компьютеров, а копия приложения WordPerfect хранится на сервере приложений. Предположим, WordPerfect лицензирован по количеству пользователей. Сколько лицензий на это приложение расходуется в следующих случаях:

   A. До входа пользователей в сеть.
   B. После входа в сеть 10 пользователей.
   C. При входе в сеть 15 пользователей, причем пять из них работают с WordPerfect.
   D. В сеть вошли 20 пользователей, 7 работают с WordPerfect, один держит его на экране в свернутом виде (minimized) и работает с электронной таблицей Excel, а другой прекратил работать с ним 10 минут назад и закрыл приложение.

2. Ваша офисная сеть состоит из 20 сетевых клиентных компьютеров, а копия приложения WordPerfect хранится на сервере приложений. Предположим, WordPerfect лицензирован по количеству рабочих мест (per-seat). Сколько лицензий на это приложение расходуется в следующих случаях.

   A. До входа пользователей в сеть.
   B. После входа в сеть 10 пользователей.
   C. При входе в сеть 15 пользователей, причем пять из них работают с WordPerfect.
   D. В сеть вошли 14 пользователей, 7 работают с WordPerfect, один держит его на экране свернутым (minimized) и работает с электронной таблицей Excel, а другой прекратил работать с ним 10 минут назад и закрыл приложение.

3. Зачем используют лицензирование по количеству рабочих мест (per-seat)?
4. Где должна сохраняться пользовательская информация сетевого приложения, необходимая для поддержки мобильных пользователей?

5. Примером чего является электронная почта?

   A. Группового программного обеспечения.
   B. Программы связи.
   C. Делового приложения.
   D. Ни одной из перечисленных программ.

6. Чем групповое программное обеспечение отличается от коммуникационного?

Глава 12

Тонкая клиентная сеть

Тонкой клиентной сетью называют любую сеть, в которой львиная доля общих ресурсов всех выполняемых приложений расположена на сервере, а не на клиентном компьютере. Этот термин по определению относится к сетям, поэтому он не касается небольших автономных компьютерных устройств типа PDA (Personal Data Assistant - персональный цифровой ассистент) и других специализированных компьютеров, использующих операционные системы с лучшей, по сравнению с Windows, организацией. То, что делает тонкую клиентную сеть и вычислительную систему "тонкой", не связано с размерами операционной системы и/или с исполняемыми клиентом приложениями, а определяется тем, где именно в сети происходит обработка данных.

Примечание

Многопользовательская версия операционной системы Windows NT вовсе не является единственной доступной системой такого типа, например, в UNIX также поддерживаются функции терминального сервера. Однако для упрощения в этой главе внимание фокусируется на тонких клиентных сетях на базе Windows NT. Хотя детали работы других продуктов, поддерживающих многопользовательские серверы, могут и отличаться, но основные моменты, относящиеся к средствам обработки данных и их применению, остаются одинаковыми.

По своему уровню тонкие клиентные сети представляют собой возврат к концепции, примененной к мэйнфреймам — приложение локализовано на центральном сервере и доступно клиентным компьютерам, имеющим локальные вычислительные средства относительно небольшой мощности. Эта аналогия не вполне точна, поскольку современные приложения могут выполнять функции, не поддерживаемые мэйнфреймами, например, обработку текстов. Однако характер управления тонкими клиентными сетями напоминает средства, применяемые к мэйнфреймам.

Почему же произошел такой переход от централизованной вычислительной обработки к персональной и обратно? Ведь ранее деловые приложения стимулировали развитие ПК. Они просто не могли работать в окружении, предоставляемом мэйнфреймами. Не все мэйнфреймы можно было считать непригодными для этих целей, но все новые и новые разрабатываемые приложения требовали настолько интенсивной работы аппаратных средств, что эффективно исполняться в совместно используемом вычислительном окружении они уже не могли.

Возврат (по крайней мере, в некотором смысле) к тонким клиентным сетям подтверждается двумя достоверными тенденциями. Во-первых, они сложны для администрирования. Требуются довольно большие временные затраты на установку и обновление локально хранящихся приложений. К тому же, ПК предоставляют сетевым пользователям пугающе обширный контроль над средствами расширения своих клиентных сред, что может означать большой объем работ по обратной реконфигурации этих сред в случае злоупотреблений. Во-вторых, теряется много ресурсов клиентных компьютеров. Современные приложения весьма прожорливо потребляют ресурсы, однако они не всегда могут быть поддержаны мощными процессорами и объемом памяти клиентных аппаратных средств. Особенно это касается окружения, в котором сетевые пользователи активно работают с приложением лишь время от времени (локальная загрузка такого приложения будет означать потерю поддерживаемых ресурсов).

Доступны ли тонкие клиентные сети всем и каждому? Заменят ли они собой ПК-центрический мир и не сделают ли ненужными средства, не требующие администрирования? Почти наверняка, нет. По крайней мере, на конец 1998 г. тонкие клиентные сети не поддерживали множество пользователей и, уж совершенно точно, не подходили для всех прило-

жений и всех вычислительных сред. Но для приложений, ориентированных на выполнение специфических задач или не требующих интенсивного взаимодействия с пользователем, они могут быть весьма полезны.

Общие принципы работы

В этой книге тонкие клиентные сети уже были упомянуты несколько раз, теперь же, наверное, настало время рассмотреть их более детально. Тонкая клиентная сеть должна включать как минимум три элемента:

- терминальный сервер под управлением многопользовательской операционной системы;
- клиент (клиентную машину) под управлением любой операционной системы;
- протокол дисплея, являющийся протоколом канального уровня, устанавливающего виртуальный канал между клиентом и сервером при входе клиента в терминальный сервер и начале сеанса работы с сервером.

Сеанс начинается с момента входа клиентного компьютера в терминальный сервер (рис. 12.1).

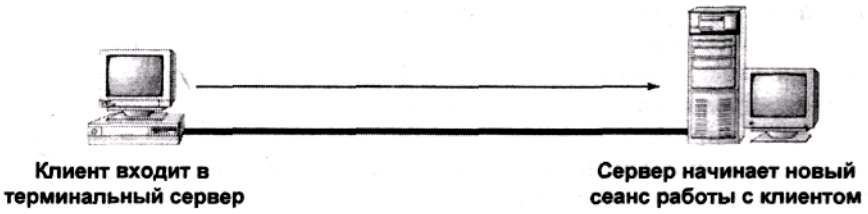


Рис. 12.1. Клиент инициализирует сеанс работы с терминальным сервером

В течение этого сеанса вводимые клиентом щелчки мыши и нажатия командных клавиш передаются на сервер через установленный виртуальный канал. Обратно через этот же виртуальный канал клиенту загружают команды визуализации растровых изображений, составляющих элементы пользовательского интерфейса (рис. 12.2).

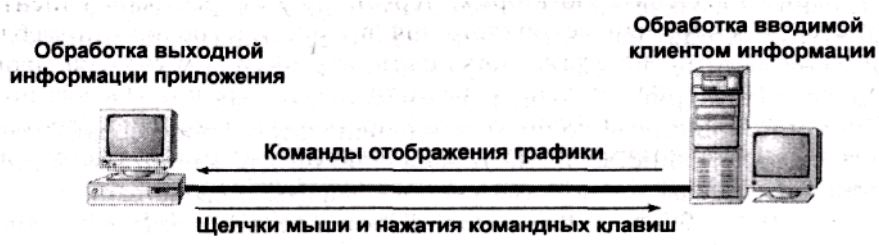


Рис. 12.2. Графические операции выполняются на клиентной машине, остальная обработка - на сервере

Примечание

В терминальном сервере Windows (WTS) многопользовательской версии NT 4 при активном сеансе работы изображение на экране обновляется 20 раз в секунду. Если же сетевой клиент приостанавливает работу, терминальный сервер замечает отсутствие активности и понижает скорость обновления до 10 раз в секунду до начала следующего пика активности клиента.

Обработка изображений

Одна из команд обработки изображения, переданная клиенту, выполняется за счет ресурсов клиентного компьютера. Установленные на нем процессор и оперативная память практически полностью применяются для воспроизведения соответствующих изображений. Требования к клиентным средствам обработки уменьшаются. Во-первых, отображение имеет 256 цветов, поэтому из-за отказа от сложных цветовых сочетаний требования к видеоадаптеру не слишком велики. Во-вторых, по крайней мере, некоторые протоколы дисплея содержат средство кэширования клиента (client side caching), позволяющее "помнить" изображения, которые уже загружались в течение сеанса. При использовании кэширования при каждом обновлении изображения на экране клиенту можно передавать только изображения изменившихся частей экрана. Например, если пиктограмма Microsoft Word уже была загружена в клиентный компьютер, то нет необходимости загружать ее снова при обновлении изображения на экране. Данные хранятся в кэше в течение определенного времени и, в конце концов, "выбрасываются" из него с помощью алгоритма LRU (Last Recently Used — "наиболее давно использовавшийся"). При этом хранимые в нем данные, которые не использовались наиболее продолжительное время, выбрасываются и освобождают место новым данным.

Управление сеансом

Во время сеанса пользователь может работать с терминальным сервером так, словно он физически находится рядом с ним и использует его мышь и клавиатуру. Когда на клиентной машине выполняют приложение, загружают данные в память, обращаются к совместно используемым ресурсам в сети (рис. 12.3) и, как обычно, работают под управлением операционной системы, то приложение использует процессорное время и память сервера. Единственными ограничениями для клиента являются те, которые определены установками системы защиты и свойствами протокола дисплея. Как это будет описано далее в этой же главе в разделе "Создание тонкой клиентной сети", не все протоколы дисплея имеют одинаковые характеристики.

Рис. 12.3. Клиент не ограничен в доступе к терминальному серверу и может использовать общие ресурсы внутри домена

Терминальный сервер обрабатывает сеанс с каждым пользователем совершенно независимо от других, и каждому сеансу отводится часть имеющихся на сервере ресурсов. Это значит, что сеанс полностью изолирован от любого другого исполняемого и запущенного сеанса (см. рис. 12.4). Однако все сеансы эксплуатируют последовательно одни и те же ресурсы — процессорное время, память, функции операционной системы — так что операционной системе приходится распределять эти ресурсы между всеми сеансами. Их число зависит от того, как много сеансов может поддерживать оборудование и сколько лицензий доступно для ис-

пользования. По завершении сеанса виртуальный канал к клиентному компьютеру закрывается, а отведенные данному сеансу ресурсы освобождаются.

Заметим: в дополнение к сеансам каждого клиента имеется также сеанс, используемый самим сервером. Все приложения, выполняемые локально, исполняются в окружении этого сеанса сервера.

Создание тонкой клиентной сети

Создание тонкой клиентной сети требует несколько большей подготовки, чем для обычной сети клиент/сервер. Требования к ее клиентной части немного меньше, но требования к серверу значительно выше и более сложны в реализации, что не должно быть неожиданностью. Хорошей новостью может быть то, что требования к самой сети не меняются. Фактически (если это необходимо), вы можете использовать значительно более медленные соединения, чем те, которые требуются для эффективной работы с обычной сетью типа клиент/сервер.

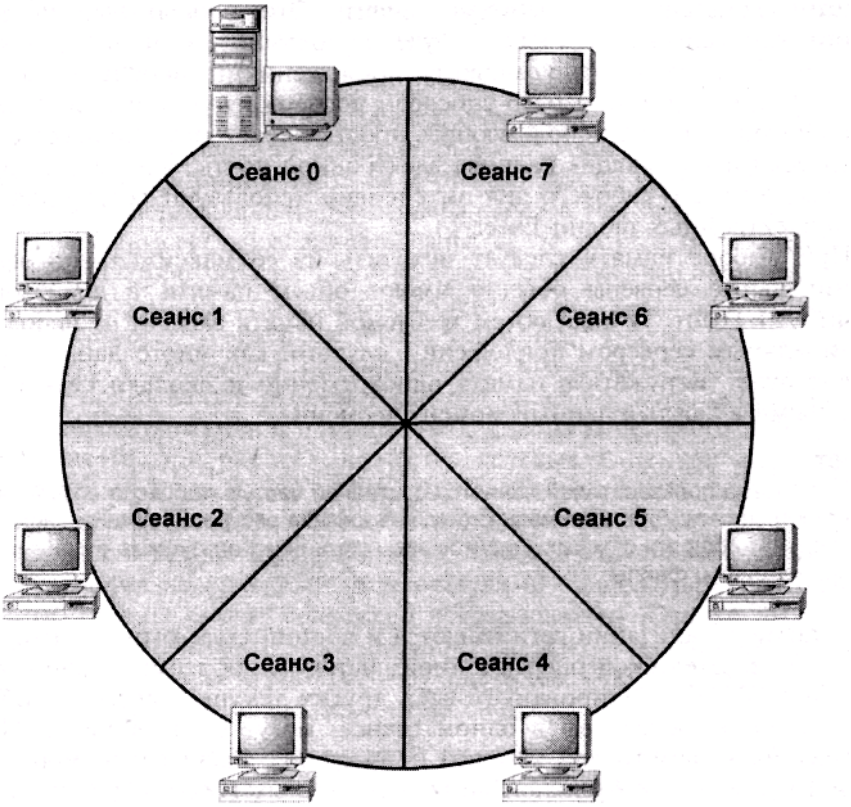


Рис. 12.4. Сеансы изолированы друг от друга, но используют одни и те же ресурсы

Требования к серверу

На сервере должна быть установлена многопользовательская операционная система, поддерживающая нужный вам интерфейс, используемый сетевыми клиентами, оборудование, достаточное для поддержки этих клиентов, и протокол дисплея, который будет переносить клиенту отображаемые данные. Все эти требования и рассматриваются далее.

Требования к оборудованию

Во-первых, требуется обеспечить поддержку всего оборудования, необходимого клиентам. Для этого нужно принять во внимание следующее.

- Какой производительности процессор необходим для поддержки требуемых вычислительных циклов (compute cycles)?
- Какого объема оперативная память требуется серверу для обслуживания всех данных и приложений, используемых клиентом?

В среднем следует рассчитывать на поддержку 12—15 клиентов каждым процессором в компьютере, но реальное число зависит от того, сколько вычислительных циклов требуется клиенту. Это, в свою очередь, зависит от того, как часто каждый клиент будет использовать компьютер и как интенсивно будут загружать компьютер приложениями, используемыми клиентом. Таким образом, сервер способен поддержать намного большее число клиентов, изредка использующих простые текстовые процессоры и периодически проверяющих наличие электронной почты, чем тех, которые на протяжении всего рабочего дня интенсивно используют сервер для подготовки электронных таблиц Excel.

При выборе памяти следует исходить из ее максимальной загрузки. Терминальные серверы обычно имеют объем памяти в диапазоне 256 Мбайт — 1 Гбайт. Точный объем требуемой памяти зависит от исполняемых терминальным сервером приложений, от того, как много данных каждый клиент будет загружать в память одновременно и сколько сеансов будут активными в каждый данный момент времени.

Совет

Подготовка пользователей является составной частью процесса создания тонкой клиентной сети. Для максимального использования ресурсов терминального сервера следует поощрять сетевых клиентов закрывать неиспользуемые в данный момент приложения и файлы.

В такой организации сети имеются и достоинства: хотя каждый сеанс в многопользовательской операционной системе типа терминального сервера Windows (WTS) изолирован от всех других текущих сеансов, объекты, используемые более чем в одном сеансе, могут быть общими. Поэтому требования к памяти для каждого приложения значительно меньше суммарного размера виртуальной памяти отдельных ПК, количество которых совпадает с числом пользователей приложения. Тем не менее, как это почти всегда справедливо для серверов: чем больше у него памяти, тем лучше будет работать серверная платформа.

Программное обеспечение и протоколы

После рассмотрения вопросов, относящихся к оборудованию, самое время поговорить о его поддержке со стороны программного обеспечения.

- Будет ли оборудование сервера доступно для использования вновь подключающимся клиентам многопользовательской операционной системы?
- Будет ли обеспечено достаточное адресное пространство в виртуальной памяти для поддержки клиента?
- Будет ли операционная система поддерживать запросы ваших клиентов?

Примечание

Не все многопользовательские операционные системы (или протоколы для поддержки подключающихся к ней клиентов) соответствуют этим требованиям.

Очень сложно установить для решения всех этих вопросов твердые правила, применимые во всех ситуациях. Однако можно использовать некоторую основополагающую информацию, которую вам следует собрать, ответив на вопросы о типе многопользовательской операционной системы, установленной на сервере, и о протоколе дисплея, используемого для

связи клиента с сервером.

Какое оборудование доступно для использования? Будет ли оборудование сервера доступно клиентным компьютерам? Это зависит от самого оборудования, от операционной системы и от того, какие установки обработки запросов выполнены для данного сервера. Дело в том, что не все операционные системы могут обрабатывать запросы от разных пользователей ко всему оборудованию сервера. Это — не то же самое, что маршрутизируемые запросы от множества сетевых клиентов. Все запросы от них помещаются в "сетевую" очередь. А теперь вспомним, что вся требуемая клиентам работа выполняется на многопользовательском сервере, поэтому технически пользователи работают как бы локально, хотя данные отображаются и обрабатываются с помощью отдельного клиентного компьютера. Таким образом, при работе множества сетевых клиентов информация направляется в "локальную" очередь. Некоторые типы оборудования, например, дисководы CD-ROM и гибких дисков, а также последовательные и параллельные порты изначально не предназначались для совместного применения несколькими пользователями одновременно. Это не означает, что они не смогут совместно использоваться. Однако вы должны обсудить с поставщиками многопользовательских операционных систем вопросы, относящиеся к конкретному оборудованию, чтобы определить, что можно потребовать от операционной системы.

Ограничение объема виртуальной памяти. А что можно сказать об адресном пространстве виртуальной памяти? Тем, кто мыслит категориями одиночного пользователя или сервера, проблема выхода приложений за пределы адресного пространства виртуальной памяти не относится к числу таких, на которые следует тратить много времени. Все согласны, что физической памяти может не хватить, но серверная операционная система обеспечивает доступ к 4 Гбайтам адресного пространства виртуальной памяти, и трудно вообразить себе нехватку такой большой виртуальной памяти на однопользовательской системе. Даже если отвести под пользовательские данные 2 Гбайта, оставшиеся 2 Гбайта, зарезервированные для функций ядра операционной системы, все еще представляют собой достаточный объем адресного пространства виртуальной памяти.

Примечание

В Windows NT 4 с (или без) установленной операционной системой WTS 2 Гбайта адресного пространства виртуальной памяти могут быть использованы для работы пользователя, в то время как другие 2 Гбайта резервируются для функций ядра операционной системы. С помощью Windows NT Enterprise Edition (или Windows NT с загруженным Service Pack 3) это разделение может быть сделано в пропорции: 1 Гбайт - для операционной системы, и 3 Гбайта - для нужд пользователя.

Однако в случае многопользовательской системы все выглядит несколько иначе. Допустим, имеется 100 пользователей, вошедших в четырехпроцессорную систему и загрузивших установленную оперативную память так, что физические ресурсы не будут слишком переполнены. Каждому из этих пользователей требуется примерно 30 Мбайт виртуальной памяти для всех исполняемых ими приложений — не такое уж непомерное количество с любой точки зрения. С учетом ресурсов, требуемых для самой операционной системы, вы приблизитесь к опасной черте занятости всех 4 Гбайт адресного пространства виртуальной памяти, доступных серверной операционной системе. Как показывает опыт, выход за пределы адресного пространства виртуальной памяти в лучшем случае приведет к генерации команды останова (Stop), в худшем — к полному отказу системы.

Вывод таков: помните, что каждый сеанс работы с сервером выполняется изолированно от других, однако все сеансы "борются" за одни и те же резервы процессорного времени и пространства памяти. У терминального сервера имеется всего один стек виртуальной памяти, а не по одному стеку на каждый сеанс. Таким образом, оборудование может поддержать все сеансы, но функциональные свойства операционной системы — нет. К слову, противопоставить этому нечего, исключая только распределение пользователей по терминальным серверам и объяснение им важности закрытия более не используемых открытых файлов и приложений.

При использовании Windows 2000 адресное пространство виртуальной памяти может быть и больше 4 Гбайт, что, безусловно, поможет пользователям WTS при работе с ней.

Многопользовательская операционная система для сервера. Многопользовательская система Windows NT, вероятно, претендует быть ответом на вопрос: "Какая операционная система может служить терминальным сервером?". Сейчас имеется две доступные разновидности многопользовательской NT.

- WinFrame фирмы Citrix.
- Терминальный сервер WTS фирмы Microsoft.

Разработанная первой, система WinFrame представляет собой набор средств (расширений) Windows NT 3.51, позволяющих ей функционировать в многопользовательском окружении. Фирма Microsoft лицензировала технологию, вернувшуюся из фирмы Citrix, для разработки терминального сервера WTS, который, в основном, остался тем же самым продуктом, но оснастился интерфейсом от NT 4. Сервер WTS в данное время является продуктом-надстройкой фирмы Microsoft, но далее будет средством обслуживания, которое можно будет включать и выключать в Win2R Server и Win2K Enterprise Edition. При работе в однопользовательском режиме WTS и Win2K являются практически одинаковыми операционными системами.

Планирование приложений и многопользовательские операционные системы

Между работой системы Windows 2000 Server в однопользовательском и многопользовательском режимах имеется одно различие, связанное с планированием потоков. В гл. 10 упомянута одна особенность, отличающая серверную операционную систему от клиентной. Она заключается в том, что серверная операционная система оптимизирована таким образом, что она предоставляет больший приоритет сетевым функциям, чем отдельным приложениям. По этой причине вы не только добьетесь большей локальной производительности от клиентной операционной системы, но и большей сетевой производительности — от серверной клиентной системы.

Терминальный сервер выполняет персонально используемые приложения, наподобие текстового процессора или электронных таблиц. Он не разделяет EXE-файлы с сетевыми клиентами, но исполняет приложения локально. Это является проблемой для NT 4, поскольку такие свойства фактически не относятся к числу тех, которые добавляются с установкой многопользовательских расширений. Таким образом, планировщик задач Windows 2000 Server спроектирован немного по-другому, чем в NT Server. Система Windows 2000 Server позволяет корректировать работу планировщика. При этом задается, что именно будет быстрее работать: локально используемые приложения или сетевые. Ваш выбор будет зависеть от того, используете ли вы возможности терминального сервера, имеющиеся у операционной системы.

Таковы некоторые "закулисные" изменения, внесенные в архитектуру Windows NT, что позволяет ей функционировать как многопользовательской операционной системе (а именно, иметь возможность организовать распределение памяти и доступ к объектам нескольким пользователям, а не одному единственному). Однако самый важный момент в функционировании этих средств не связан напрямую с операционной системой. В операционной системе клиент видит лишь то, что выполняет терминальный сервер и отображают средства его интерфейса. Ключевым моментом в их работе является наличие функций, выполняемых средствами протокола дисплея, позволяющими клиенту и серверу взаимодействовать друг с другом.

Протоколы дисплея. Напомним: протоколы дисплея работают на канальном уровне и

обеспечивают организацию виртуального канала между сервером и клиентом, передающего клиенту отображаемую информацию (для ее визуализации), а также вводимую клиентом информацию для обработки на сервере. Многопользовательская операционная система, реализованная на базе NT, поддерживает два протокола дисплея: RDP (Remote Display Protocol — протокол удаленного дисплея) и ICA (Independent Computing Architecture — архитектура независимой вычислительной системы).

Примечание

Вы знакомы с протоколом X, используемым с терминальными службами UNIX? RDP и ICA имеют функции, во многом подобные протоколу X.

Протокол RDP, поставляемый вместе с терминальным сервером WTS, основан на протоколе T. 120 фирмы Microsoft, изначально спроектированном для приложения NetMeeting, поддерживающего видеоконференции. Он предназначен только для клиентов Windows (как 16-битовых, так и 32-битовых, включая Windows CE); предоставляет клиенту целый рабочий стол; организует ограниченное взаимодействие между процессами, исполняемыми на клиентном компьютере (если они есть), и процессами, исполняемыми на терминальном сервере и отображаемыми на клиентном компьютере.

Протокол ICA, используемый в надстройке MetaFrame фирмы Citrix для терминального сервера WTS, поддерживает следующие функции (отсутствующие у протокола RDP).

- Звук.
- Доступ к множеству сеансов.

Примечание

Состав протокола RDP делает его технически способным к поддержке множества сеансов, но в коммерческом продукте в настоящее время его поддержка не предусмотрена.

- Поддержка публикации отдельных приложений (вместо всего рабочего стола).
- Поддержка не-Windows клиентов (DOS, Macintosh, UNIX) при запуске приложений Windows.
- Совместное использование буфера Clipboard различными приложениями: и локальными, и исполняемыми на терминальном сервере.
- Поддержка как IPX/SPX, так и TCP/IP-протоколов.
- Поддержка затенения сеансов (session shadowing), позволяющая администратору брать на себя управление терминальным сервером для диагностики неисправностей.
- Поддержка локальной печати из приложений, находящихся на терминальном сервере.
- Последовательное кэширование информации на стороне клиента, понижающее сетевой трафик, связанный с обновлениями экрана.

Почему же вообще используют RDP, если он имеет более ограниченные по сравнению с ICA возможности? Из-за одного его прекрасного свойства: он поставляется вместе с WTS, поэтому при его использовании не требуется платить за лицензию, как пришлось бы делать в случае использования другого протокола дисплея. Если ваши запросы скромны (в случае, например, обслуживания клиента Windows, не нуждающегося в звуке, или при возможности локально выполнять приложения и работать в сети TCP/IP), то протокол RDP совершенно удовлетворителен.

Функциональные возможности протокола RDP в некоторых случаях могут быть расширены. Хотя Windows 2000 на момент написания книги (конец 1998 г.) все еще оставался Beta-2 версией, текущие планы его развития предусматривают добавление следующих функций в RDP (которые в данное время имеются лишь в протоколе ICA).

- Затенение сеансов.
- Локальная печать из удаленного приложения.
- Совместное использование буфера Clipboard локальными и удаленными приложения-

ми.
- Звук.

Другими словами, когда появится окончательная версия системы Windows 2000 (если в ней останутся эти функциональные возможности протокола RDP), то данный протокол возьмет на себя дополнительные функции, ныне имеющиеся только у протокола ICA.

Скорость работы всегда важна, и некоторое время общее мнение было таково, что протокол ICA по определению работает быстрее RDP. Однако когда в лаборатории Windows NT Magazine выполнили контрольное тестирование этих двух протоколов, оказалось, что это не совсем так. В некоторых случаях протокол RDP фактически работает лучше ICA. Различие обусловлено количеством окон, отображаемых на экране клиентного компьютера. Протокол RDP спроектирован для пересылки полноэкранных изменений, поэтому окна приложений, работающих в режиме максимизированных окон и не содержащих дочерних окон, перерисовывались на экране быстрее с помощью протокола RDP, а не ICA. Приложения же, отображающие окна, и приложения с дочерними окнами перерисовывались быстрее с помощью протокола ICA, чем PDP. Эти результаты были получены независимо от быстродействия линии связи между клиентом и сервером. Короче говоря, если вам нужна скорость, то выбирайте протокол RDP для выполнения полноэкранных приложений, которые не содержат дочерних окон, и протокол ICA, если требуется перерисовка.

Требования к клиентной машине

Требования к оборудованию клиентов терминального сервера варьируется в зависимости от оборудования клиентной машины и от того, что от нее потребуется при работе. Тип процессора и объем памяти зависят от следующих обстоятельств.

- Будет ли клиент запускать какие-либо приложения локально?
- Какова сложность отображаемой видеоинформации? Это видеофильмы, или только рисунки?

Первый вопрос существенен, поскольку ответ повлияет на способ использования ресурсов компьютера. Визуализация видеоинформации загружает процессор и память, требуя значительных затрат процессорного времени для отображения рисунков. Если процессор и память еще и поддерживать локальную обработку данных, то они должны быть значительно более мощными, чем процессор и память в терминальных устройствах, не выполняющих локальные приложения.

Терминалы Windows, которые обычно не выполняют приложения локально, предъявляют низкие требования к клиентным устройствам по сравнению с микрокомпьютерами, выполняющими свои собственные приложения. Они не сохраняют данные локально, поэтому не имеют жестких дисков, и обычно не имеют и внешних устройств, например, CD-ROM или подсоединенных принтеров. Чаще всего терминалы Windows содержат процессор с некоторым объемом памяти и портами, позволяющими подключать монитор, клавиатуру и сеть. Наиболее часто используется сеть Ethernet с кабелем UTP, но также встречается коаксиальная сеть Ethernet или Token Ring, в виде либо уже встроенных средств, либо реализуемых по запросу.

Требования к сети

Для реализации тонкой клиентной сети не требуется ничего особенного. Информация передается от клиента к серверу достаточно постоянным потоком, и ее объем не очень велик. Таким образом, вы можете работать в тонкой клиентной сети через относительно медленное соединение, аналогично работе в сети VPN, организованной через Internet, или коммутируемое подсоединение, как это описано в гл. 6.

Протоколы дисплея не предусматривают перенос данных всех типов — это требует наличия установленного транспортного протокола. Как уже было описано в разделе "Протоколы дисплея", оба протокола (и ICA, и RDP) поддерживают протокол TCP/IP. ICA поддерживает также протокол IPX/SPX. Ни один из них не поддерживает протокол NetBEUI. Для обеспечения функционирования глобальных сетей или удаленных подключений оба протокола дисплея поддерживают соединение, управляемое PPP.

Выбор приложений для тонких клиентов

Не все приложения работают одинаково хорошо в среде терминального сервера. Наилучшими приложениями являются следующие.

- Не требующие большого числа вычислительных циклов.
- Сводящие к минимуму отображение ненужных изображений.
- Эффективно организующие локальные и глобальные данные.
- Использующие имена пользователей вместо имен компьютеров. Давайте познакомимся поближе со всеми этими важными свойствами.

Минимальное количество вычислительных циклов

Поскольку все сеансы используют процессорное время совместно, то для них требуется еще большее число циклов процессора, чем в однопользовательских системах. Таким образом, приложения, выполняющиеся на терминальном сервере, должны в известной степени обходиться меньшим количеством вычислительных циклов. Функции, выполняющие интенсивное "перемалывание" чисел (number crunching), и другие вычисления, должны быть возложены на клиентные приложения.

Примечание

Как уже указывалось, все клиенты в процессе активного сеанса должны бороться за вычислительные циклы на равных условиях. Однако предполагается, что Windows 2000 Server будет поддерживать функциональное средство, которое сможет ограничить использование общих ресурсов, так что сеансы, чрезмерно поглощающие общие ресурсы, не будут мешать работе других сеансов.

Минимизация отображения ненужных изображений

В отдельных случаях обновления изображений неизбежны: изменения изображения на экране, происходящие при перемещении по Web-страницам с помощью броузера, обновления содержимого окон, необходимые при открытии нового документа или нового приложения, и т.д. При неизбежных обновлениях экрана просто убедитесь, что соответствующие тонкие клиентные средства способны обработать требуемые данные при визуализации изображений.

Однако некоторые изменения изображения на экране не нужны, потому что они не служат какой-либо полезной цели. В этом смысле анимация, вероятно, является наихудшим вариантом, поскольку ее вывод требует как вычислительных циклов, так и регулярных обновлений изображения на экране. Желательно, чтобы в приложениях либо вообще не использовалась анимация, либо, по возможности, все средства такого рода (например, Помощник в Microsoft Office 97) были выключены. Хранители экрана, автоматически включающиеся на клиентном компьютере, также не должны использоваться по аналогичным соображениям.

Корректное сохранение информации

Хорошим приложением для многопользовательского окружения, безусловно, является то, которое в состоянии эффективно организовать хранение информации. Некоторые приложения, предназначенные для одного компьютера с одним пользователем, явно не годятся для работы в многопользовательском окружении. Эта особенность может привести к невообразимому хаосу, когда, например данные, которые должны быть доступны только определенному пользователю, становятся доступными всем, работающим на данном компьютере. Принадлежащая пользователю информация должна быть записана в специально отведенном пользователю месте, например "домашнем" каталоге пользователя, но не в системном каталоге.

Идентификация пользователей по имени

Если предположить наличие соответствия "один компьютер, один пользователь", то возникает специфическая- ситуация, связанная с передачей сообщений между пользователями. Приложения типа Windows Chat ориентированы на работу компьютера с компьютером — сеанс переговоров устанавливается между двумя компьютерами, а не двумя пользователями. Другими словами, приложение Chat нельзя использовать для переговоров между двумя пользователями, вошедшими в один и тот же терминальный сервер, поскольку приложение фактически выполняется на одном компьютере. Команда NET SEND, наоборот, ориентирована на пользователей, поскольку инициирует поиск имен вошедших пользователей, а не имен компьютеров. Если вам требуется использовать для передачи сообщений приложение, ориентированное на компьютеры, вам следует запускать его на клиентных компьютерах, а не на терминальном сервере.

Разделение публикуемых приложений

Существует компания, которая сделала возможным публикацию приложений для выполнения тонкими клиентами вообще без многопользовательской операционной системы. В 1998 г. компания New Moon Software выпустила продукт, называемый Liftoff, который разделяет процесс запуска приложения между сервером и клиентом без всякого дополнительного оборудования. Вместо существующих терминальных серверов, предоставляющих сетевым клиентам доступ к виртуальным сеансам на сервере, используется компьютер, работающий как сервер приложений, работающий под управлением однопользовательской операционной системы и публикующий приложения с помощью приложения Liftoff.

Выполнение опубликованного приложения разделяется таким образом, что (как и в случае терминального сервера) обработка данных выполняется на сервере, а клиенту "достается" обработка команд визуализации графики. Однако окончательные действия, выполняемые приложением, должны выполняться на клиентной машине, что не свойственно сеансу работы с терминальным сервером.

Зачем же тогда нужен терминальный сервер? Выбор подхода зависит от клиентных средств, которые вы используете или собираетесь использовать. Приложение Liftoff работает только с 32-битовыми клиентами Windows. Оно не имеет надстройки, позволяющей не-Windows клиентам выполнять приложения Windows. Более того, большие ресурсы, требуемые для поддержки клиентов, означают, что приложение Liftoff, вероятно, не самый лучший способ использования старых аппаратных средств, поскольку клиент должен быть в состоянии поддерживать Windows NT Workstation или Windows 95/98. Отсутствие поддержки каких-либо других операционных систем, отличных от 32-битовых Windows, препятствует использованию приложения Liftoff на терминалах Windows, даже работающих под управлением Windows CE. Однако этот подход может оказаться полезным для тех, кто имеет высокоуровневые клиентные средства и не хочет использовать терминальный сервер, а просто собирается воспользоваться некоторыми фрагментами тонкой клиентной сети.

Почему используются тонкие клиентные сети

Теперь вы знаете, что собой представляют тонкие клиентные сети и что требуется для обеспечения их функционирования. Теперь самое время задать трудный вопрос: зачем вообще нужно делать всю эту работу?

Год или два назад, когда идея основанной на Windows тонкой клиент-ной сети только начинала свой взлет, можно было услышать множество высказываний по поводу того, насколько эти сети лучше традиционных локальных сетей, поскольку значительно упрощают сетевые клиентные средства и этим уменьшают их стоимость.

Ничего подобного.

Во-первых, стоимость новых ПК, способных выполнять клиентные приложения, ощутимо снизилась. Сейчас можно приобрести полностью оснащенный современный ПК примерно за 1000 $, иногда вместе с монитором. "Низкоуровневые" системы могут стоить до 500 $ (без монитора). Поскольку стоимость памяти, наоборот, слегка подскочила, следует ожидать соответствующего повышения цен, но настольные ПК от этого не станут дороже.

Во-вторых, терминалы Windows и прочие тонкие клиентные устройства отнюдь не всегда являются такими уж дешевыми. Обычно компьютеры Net PC стоят от 300 до 500 $, не включая монитор. После этого вы получаете компьютер, который не сможет работать без помощи дорогостоящей терминальной операционной системы, запущенной на полноценном компьютере (часто с SMP - симметричной мультиобработкой), поддерживающем всех своих пользователей.

В-третьих, вам не дешево обойдется и отказ от уже имеющихся компьютеров и покупка новых ПК, да плюс к тому же еще новой серверной операционной системы. Разумно ли это? Иногда, да. Дешевле ли это покупки новых персональных компьютеров? Возможно. Но не дешевле сохранения имеющихся компьютеров или их модернизации, которая вдохнет в них вторую молодость.

Ясно, что причина перехода на тонкие клиентные сети заключается не в понижении стоимости оборудования. Вместо понижения общей стоимости собственности (TCO — Total Cost Ownership) применение тонких клиентных сетей понижает общую стоимость администрирования (TCA — Total Cost Administration). Размышляя на эту тему, фокусируйте свое внимание на том, куда реально идут деньги, направленные на поддержку и обслуживание компьютеров. Ведь это не просто дорогостоящий ящик с оборудованием, помните об этом.

Понижение общей стоимости администрирования (TCA)

Стоимость эксплуатации ПК значительно превышает стоимость его оборудования. Она состоит из следующих компонентов.

- Обнаружения неработоспособных состояний, возникающих из-за ошибок пользователя, и восстановление работоспособности.
- Инсталляция или обновление приложений.
- Ремонт неисправных ПК.
- Модернизации оборудования ПК.
- Разрешение проблем, возникающих из-за конфликтов приложений друг с другом.

Тонкие клиентные сети помогут вам установить контроль над клиентными компьютерами в сети путем централизации всего того, что к ним относится. Приложения, пользовательские установки — одним словом все, что требуется для работы сети, располагается в одном

центре, вплоть до операционной системы. В сочетании с системными правилами, определяющими, что пользователи могут и чего не могут делать на своих настольных системах, эти средства значительно уменьшают объем работы по поддержке пользователей, выполняемой с помощью советов справочной системы. Если неопытные пользователи будут лишены возможности удалять ярлыки на своих рабочих столах или переключать свои экраны в другой режим, то им не потребуется вызывать соответствующие средства поддержки пользователей (Support) для решения проблемы после того, как сами же ее и создали.

Даже на уровне аппаратных средств можно воспользоваться возросшими возможностями средств управления. Тонкими клиентами могут быть обычные ПК (иногда это желательно), но они могут быть также и до предела разукомплектованными компьютерами, представляющими собой всего лишь маленькую "пристройку" к мыши, клавиатуре, и монитору (бездисковая станция). Пользователь не сможет установить нелицензированное программное обеспечение или игры (или занести загрузочные вирусы (boot viruses) в компьютер). Терминальные устройства имеют дополнительные преимущества — их простота оборачивается уменьшением занимаемого ими объема по сравнению с полностью укомплектованными обычными ПК. Это удобно, особенно если приходится работать в тесных помещениях, например на кухне или в кладовке.

Устранение циклических модернизаций

Еще один довод в пользу применения тонкой клиентной сети состоит в возможности продления срока службы старых ПК. Порой кажется, что большая часть программного обеспечения (коммерческих приложений) вообще ничего не делает, но, тем не менее, требует для себя больших ресурсов, и значит, они необходимы и вашему компьютеру. Это не обязательно относится к самим приложениям: ныне сами данные стали более обширными, поскольку в них широко используются мультимедиа-данные. Эта проблема имеет циклический характер. Закон Паркинсона, определяющий, что основным свойством работы является захват всего отведенного на ее выполнение времени, может быть применен и к данным — они также склонны захватывать все доступные ресурсы. Поэтому, чем больше вы получите в свое распоряжение ресурсов (памяти, дискового пространства) для хранения данных, которые вы используете сегодня, тем обширнее, станут эти данные завтра.

Короче говоря: время морального старения ПК составляет два года, поэтому процесс модернизации может оказаться дорогостоящим хобби. К несчастью, от него трудно отказаться, поскольку трудно не участвовать в циклической модернизации, если им занимается кто-то другой. Устаревший на два поколения текстовый процессор можно прекрасно использовать при подготовке документов у себя на дому, но он может оказаться неспособным отобразить новый документ, который вам пришлют из соседней фирмы.

Однако, к сожалению, компьютеры не обновляются автоматически, когда перестают соответствовать "запросам" новейших приложений. Если ваш ПК перестал им соответствовать, вы можете его модернизировать или заменить.

Модернизация обычно обходится дешевле, так как экономятся средства на приобретение оборудования, но она необязательно окажется дешевле из-за длительности работы. Во-первых, она требует затрат времени (которое для большинства из нас поистине драгоценно) на добавление памяти или установку нового жесткого диска. Модернизация, к тому же, иногда становится трудной, или даже невозможной, без замены материнской платы — вы пробовали найти SIMM на 30 выводов для старых компьютеров с 486 процессором?

Приобретение нового ПК каждые два года представляет собой другую возможность, но она таит в себе скрытые расходы. Покупка нового ПК отнюдь не сводится к покупке нового корпуса процессора и подключения его к сети, но также требует приведения новой машины в "полное подобие" старой. Это означает переустановку приложений, архивирование локально хранящихся данных и параметров конфигурации пользователя с последующей их перезаписью и так далее.

Примечание

Проблемы замены старого ПК на новый являются убедительным аргументом в пользу централизованного хранения всех данных и информации о конфигурации пользователей, даже если вы не заняты созданием тонкой клиентной сети.

Теперь, когда вы уже доведены всем сказанным выше до отчаяния, самое время указать способ, который позволит вам избежать этого круговорота модернизации или, по крайней мере, упростить его. В случае, когда все приложения выполняются на единственном сервере тонкой клиентной сети, клиентные компьютеры, фактически, не имеют возможности самостоятельно выполнять приложения (а может быть и поддерживающую ее операционную систему). Единственным компьютером, который нужно модернизировать, чтобы привести его в соответствие с "запросами" приложений, является сервер. Таким образом, с помощью тонкой клиентной сети можно значительно продлить жизнь ваших клиентных компьютеров.

Простые приложения для тонкой клиентной сети

Если вы все еще не знаете, что можно сделать с помощью тонкой клиентной сети, представьте себе следующую ситуацию, взятую из реальной "жизни" тонких клиентных сетей.

Примечание

Полный текст этого сценария, дополненный перечнем оборудования и другими деталями, доступен на узле www.winntmag.com в выпусках за октябрь 1998 г. и январь 1999 г.

Держите наготове докторов

В одной клинике на Среднем Западе пришли к выводу, что им необходимо изменить способ хранения данных. Предыдущие 10 лет (или около того) клиника работала с историями болезней своих пациентов и их счетами с помощью комбинации мэйнфрейма и нескольких автономных ПК. Мэйнфрейм устарел и стал ненадежным, а нужда в информации о пациентах критически возросла, поскольку требовалось управляться с 10000 пациентов, ежегодно прибегающих к услугам клиники.

Новое техническое задание содержало два требования. Первое: предоставить надежный доступ к историям болезней, чтобы медицинский персонал клиники мог выписывать счета и решать другие задачи, требующие информации о пациентах. Второе: предоставить персоналу доступ к данным о пациентах без нарушения отношений докторов с пациентами. Доктора привыкли читать файл данных о пациенте, находясь рядом с ним (в кабинете или в палате), и им не очень-то понравилась идея прекращения такого общения, связанная с необходимостью перехода в другую комнату с клиентным компьютером. В результате этого возникло техническое решение о применении ПК, работающих под управлением операционной системы Windows NT Workstation для персонала госпиталя и беспроводных клиентных устройств Wyse для докторов. Медицинский персонал мог использовать ПК для быстрого и надежного доступа к данным о "пациентах, в то время как доктора могли носить с собой при обходе устройства Wyse, делая записи на сенсорном экране, как на обычном пюпитре с бумагой.

Предоставление доступа к компьютеру студентам

Одной из наибольших помех в путешествии является необходимость повсюду таскать за собой портативный компьютер. Даже самый легкий — он достаточно тяжел, неудобен в работе (особенно в самолете во время перелета) и в большинстве случаев менее удобен, чем его "настольный" собрат. Однако если вы не возьмете с собой в путешествие персональный компью-

тер, вы не сможете работать с файлами, читать сообщения электронной почты, просматривать сообщения Web и тому подобное.

Однажды администрация учебного центра решила облегчить жизнь своим студентам, предоставив им доступ к ПК во время двухдневного пребывания в центре. В каждой комнате гостиницы был установлен компьютер, который постояльцы могли использовать для запуска электронной почты, текстовых процессоров, Web-броузеров и т.д. Постояльцы были довольны, но сетевые администраторы - нет. Чтобы защитить данные каждого постояльца, сетевые администраторы вынуждены были стирать некоторые файлы с жесткого диска каждого ПК после их отъезда. Это причиняло большие неудобства, учитывая, что центр принимал сотни студентов в неделю и каждый останавливался лишь на несколько дней. Вдобавок, исправление повреждений и ошибок в конфигурации компьютеров также отнимало у администраторов много времени, которое они могли бы потратить с большей пользой на разработку новых сетевых средств.

Для разрешения этой проблемы сетевые администраторы решили заменить ПК в каждой комнате на тонкие сетевые устройства — фактически, на сетевые компьютеры. Системные правила для их пользователей разрешали доступ только к отдельным приложениям, но не к установкам, выполняемым с помощью панели управления. Средства для начала сеанса работы в сети поддерживали два сервера. Они предоставляли средства хранения файлов в выделенном каждому пользователю "домашнем" каталоге (с помощью разработанных сотрудниками центра сценариев), который мог быть автоматически создан при регистрации в момент прибытия, и удален после отъезда из отеля. Четыре сервера приложений обеспечивали доступ к сетевым приложениям. При такой конфигурации пользователи имели ограниченный контроль над своим рабочим столом, что соответственно ограничивало и их возможности вносить путаницу в конфигурацию рабочего стола, но не препятствовало доступу к нужным приложениям.

Централизованное управление рабочим столом

Не все тонкие клиентные сети однородны — многие для удовлетворения запросов пользователей представляют собой "смесь" тонких и толстых клиентов. В данном случае разработчики сети были просто счастливчиками, поскольку начали работу с того, что выбросили всю свою существующую сеть — все это сборище серверов OS/2, персональных компьютеров с Windows 3.1, мэйнфрейм с набором неинтеллектуальных терминалов и т.п.

С целью предоставления наиболее современного вида строящейся сети и предоставления доступа к некоторым приложениям, которые не могли исполняться ни в среде Windows 3.1, ни на неинтеллектуальных терминалах, компания решила полностью заменить существующую сеть. Использовались устройства Net PC (аналогичные сетевым компьютерам, но способные исполнять приложения как локально, так и удаленно) и терминальный сервер. Для квалифицированных пользователей (power user) в нее были добавлены несколько ПК с операционной системой Windows NT Workstation, поскольку им требовался доступ ко всем приложениям (они вряд ли смогли бы внести ошибки в конфигурацию своих компьютеров). Остальные пользователи получали свои Net PC и доступ только к отдельным приложениям. Некоторые пользователи по объективным причинам были лишены возможности подстраивать рабочие столы под свои запросы (что обычно является источником жалоб, как правило, возникающих при блокировании части или вообще всех системных конфигураций). Однако, в конце концов, все были удовлетворены достигнутой оперативностью и надежностью работы системы.

Выводы

Итак, следует ли использовать тонкие сети везде и всюду? В общем, нет. Не верится, что это та волшебная палочка, которая решит все проблемы. Тонкие клиентные машины пригодны для работы в сетях только в том случае, если можно без значительных затруднений и с наибольшей эффективностью (по стоимости) централизовать вычислительные ресурсы сети, исполняемые в среде распределенной обработки. Чем более целенаправленно и нерегулярно ваш клиент использует сеть, тем больше ему подходит тонкая клиентная сеть.

Тонкие клиентные сети нежелательно применять для объединения сетевых клиентов, которые интенсивно загружают ресурсы компьютера приложения. Они требуют очень стабильной работы серверного окружения, и одно такое приложение может затребовать больше ресурсов, чем вся сеть. Это также потребует от обслуживающего персонала умения поддерживать работу центрального сервера. Короче, тонкая клиентная сеть не всегда удовлетворяет запросам всех пользователей сети. С этой точки зрения заслуживает внимания возможность использования сети, являющейся гибридом "тонких" и "толстых" клиентов.

Одно удачное применение тонкой клиентной сети состоит в использовании централизовано хранимого Web-броузера. В гл. 13 описывается построение сервера интрасети, предоставляющего такой Web-броузер в распоряжение сетевым клиентам.

Упражнение 12

1. В терминальный сервер вошли шесть пользователей. Сколько сеансов будет выполняться?

2. Назовите два протокола дисплея, поддерживаемые терминальным сервером WTS.

3. Какой из протоколов дисплея может быть использован в каждой из указанных ниже ситуаций — RDP или ICA? (В некоторых ситуациях возможно использование сразу двух.)

   A. Использует Windows CE.
   B. Требуется поддержка звука.
   C. Работает в UNIX.
   D. Работает в Windows 95.

Глава 13
Создание корпоративной Web-сети

Практически всемирное распространение World Wide Web и других частей Internet превратило броузеры в существенную часть офисных приложений. Зачем же создавать Web-структуру на базе интрасети, если с ней будут работать только служащие офиса?

В этой главе рассматривается, что можно сделать с помощью корпоративной Web-сети, а также описываются основные методы создания и публикации (представления) Web-содержимого, (доступные типы форматов и инструменты, необходимые для публикации данных). Конечно, прочитав эту главу, вы не станете экспертом по программированию на языке Java, однако получите представление о том, что необходимо для создания страницы или узла, ознакомитесь с некоторыми идеями, которые могут понадобиться в дальнейшем.

Что можно сделать с помощью корпоративной Web-сети

Вероятно, вы полагаете, что основное назначение Web ограничено публикацией информации вашей фирмы, однако это — лишь малая толика того, что можно сделать с помощью Web-сети. Овладейте этим мастерством и вы сможете выполнять следующее.

- Отсылать обязательную для просмотра информацию и получать подтверждения о том, кто ее прочел, а кто — нет.
- Проводить виртуальные собрания служащих, не имеющих возможности встретиться лично.
- Автоматически запрашивать справочную систему или другие источники внутриофисной информации.
- Предоставлять служащим простой доступ к базе данных фирмы.
- Запускать FTP-узел фирмы.
- Публиковать собственные исследования так, чтобы позволить заинтересованным лицам использовать эту информацию совместно.

Примечание

Некоторые (но не все) варианты применения корпоративных Web-сетей, описанные в этой главе, взяты из итогов социологического исследования, подготовленного автором для статьи "1999 NT innovators" (Новаторы Windows NT 1999 года), опубликованной в журнале "Windows NT Magazine", в которой представлены все новые применения Windows NT по январь 1999 г. включительно. Если вас заинтересуют эти остроумные применения корпоративных сетей Web, войдите в www.winntmag.com и просмотрите в архивах выпуск за январь 1999 г. (доступный в апреле 1999 г. в оперативном (online) режиме).

Можно ли сделать что-нибудь еще с помощью корпоративной Web-сети? Превратите ее в "дегустационный зал" новых идей, посвященных содержимому вашего Web-узла в сети Internet. Если вы не уверены в своей концепции, почему бы не опубликовать ее там, где смогут с ней ознакомиться поначалу только ваши коллеги и дать несколько полезных советов? Прежде чем представлять свои идеи всему миру, убедитесь в их жизнеспособности. Кроме того, советы коллег помогут развить хороший замысел и избежать провала.

Простота распространения информации

Как и электронная почта, так и использование интрасети Web (intranet Web content) поможет вам сберечь немало бумаги. Вместо печати записок, извещающих служащих о переменах политики фирмы либо приглашающих на воскресный пикник, подобную информацию можно поместить на специальной странице Web. Это позволит избежать хлопот по рассылке бумаг, а также использовать "конструктивные" элементы, не всегда доступные электронной почте. Причем от сотрудников здесь не требуется доступ к приложению, с помощью которого создавался исходный документ. Кроме того, отсылка документов на Web-узел удержит их от уточнений и изменений исходного документа.

Еще одно преимущество публикации в Web документов для обязательного просмотра заключается в возможности подтверждения их прочтения служащими. Ваши возможности не ограничены простой отсылкой информации в надежде, что ее прочтут нужные люди. Просто создайте раздел, в котором можно, щелкнув на кнопке "Да, я прочел это и понял, о чем идет речь", отослать по электронной почте подтверждающее письмо коммерческому директору либо другому руководителю. Что-нибудь в этом роде можно использовать, для получение согласия (RSVP) на встречу в офисе или организацию общего собрания. Для этого создайте форму, в которой можно указать, будут ли приглашенные присутствовать, сколько приведут гостей, предпочтительные даты организации, требования к закуске и тому подобную информацию. Служащий, отвечающий за координацию собраний офиса, высоко оценит автоматизацию подобного рода.

Организация собраний

В гл. 11 упоминались сеансы переговоров (chat sessions), которые могут заменить собрания, если их сложно организовать или невозможно вообще. Это делается с помощью приложений для проведения переговоров (chat applications). Другой способ — использование средств для Web-переговоров. Для этого достаточно установить Web-броузер, а приложения для проведения переговоров уже не нужны. Кроме того, интерфейс Web позволяет поддерживать видеоконференции.

Кроме того, приложения планирования Web можно использовать для группового планирования в тех случаях, когда на виртуальных собраниях не удалось достичь поставленной цели. Например, в Lotus Organizer предусмотрен выход в Web, чтобы служащие могли планировать личные расписания на собственных компьютерах или устройствах PDA, а затем передавали информацию в общий Web-календарь.

Совет

Если просмотр вашего календаря посторонними людьми нежелателен, защитите его паролем. Корпоративная Web-сеть предоставляет и другие средства связи. Например, она может помочь служащим найти друг друга. Офисы многих крупных фирм представляют собой настоящий лабиринт комнат, к тому же в таких фирмах люди не всегда знают друг друга в лицо. Одно из решений такой проблемы заключается в создании онлайновой карты (online map) офисов фирмы, на которой указаны рабочие места всех служащих. Достаточно ввести имя служащего, как на карте отобразится его портрет и офис в котором служащий работает.

Удешевление поддержки

Справочный стол пользователя Web весьма облегчает процесс поддержки. Во-первых, многие запросы пользователя можно предвидеть. Обычно ему нужен доступ к конкретной папке (либо они не могут забрать свою электронную почту, либо найти файл). Вы можете создать форму со списком типичных проблем, позволяющую пользователю указать в нем интересующий его вопрос. Если в списке нет таких вопросов, пользователи могут задать их в

текстовом поле на Web-странице.

Совет

Использование справочного стола пользователя Web позволяет сотрудникам пожаловаться на отсутствие доступа к электронной почте, не прибегая к телефону и электронной почте (которую они не всегда могут включить).

Во-вторых, возможность описать проблему или указать ее в списке — это стимул к обдумыванию и описанию проблемы , причем более подробно, чем возможно по телефону либо при личном общении. Личный опыт работы автора книги по поддержке запросов пользователей свидетельствует о том, что пользователи часто опускают начальный процесс уточнения проблемы, начиная прямо с сообщения вроде "WordPerfect не работает" или "WordPerfect закрывается, отобразив сообщение о нехватке ресурсов компьютера". Уточнение проблемы может занять несколько минут и даже более, если пользователь и лицо, отвечающее за поддержку, не могут понять друг друга. Намного проще и понятнее позволить пользователю самому описать проблему либо выбрать ее в списке проблем. Конечно, это не исключает вообще необходимость уточнения какой-то проблемы, но несколько упорядочивает этот процесс. Если же необходима дополнительная информация, то можно, в конце концов, связаться и по телефону.

В-третьих, обсуждение проблем с помощью электронной почты Web уменьшает как время на изложение проблемы, так и время, необходимое специалисту на ее обдумывание. Кроме того, электронная почта всегда доступна лицу, запросившему помощь (нет необходимости ожидать освобождения телефонной линии центра поддержки).

Упрощение доступа к базам данных

Постоянно возрастает интерес продавцов и менеджеров к использованию корпоративной интрасети Web для поддержки внешних баз данных. Последние имеют значительные преимущества по сравнению со стандартными, ежемесячно печатаемыми, отчетами. Во-первых, в стандартных отчетах могут отсутствовать ответы на конкретные вопросы продавцов или менеджеров. Во-вторых, мы снова сталкиваемся с проблемой распространения. Как переслать отчеты всем служащим фирмы, рассредоточенной по обширному региону? По факсу? Электронной почтой? Кто должен составлять отчеты?

Совет

Автору довелось ознакомиться с работой корпорацией, в которой пользователи могли отсылать запросы на сервер базы данных по электронной почте, причем для этого не требовалось знать синтаксис языка SQL (Structured Query Language -язык структурированных запросов). Пользователи могли составлять запросы, пользуясь средствами стандартных языков программирования, после чего генерировались предварительно заготовленные запросы. Однако используемый язык был слишком примитивен для создания сложных запросов. Более подготовленные пользователи, знакомые с синтаксисом SQL, могли отсылать по электронной почте запросы SQL и получать, таким образом, пользовательские отчеты.

Помимо всего прочего, когда пользователям необходимо редактировать базу данных или создавать отчеты, соответствующие Web-приложения позволяют сделать это даже тем, кто не разбирается в средствах внешнего интерфейса базы данных, ну, например, Access. Средства внешнего интерфейса можно спроектировать так, чтобы транслировать сформулированные пользователем запросы на язык SQL, который и используется для управления базой данных.

Распространение файлов

Может потребоваться предоставление пользователю доступа к отдельным файлам, а не к каталогом, в которых они хранятся. Возможно, каталоги доступны только через медленное

соединение глобальной сети, а возможно, в них сохраняются другие файлы, о существовании которых нежелательно знать остальным пользователям. В таком случае вы можете организовать FTP-узел, который будет работать как центральное хранилище входящих и исходящих файлов. Пользователи смогут выгружать и загружать файлы из более или менее доступного каталога. Степень защиты зависит от конфигурации — доступ может предоставляться по паролю, ограничиваться для некоторых пользователей или предоставляться всем, кто вошел в систему.

Совет

Чтобы обеспечить структурную согласованность файлов данных, реплицируйте их из исходных каталогов на FTP-узел.

FTP-узел необязательно "начинять" только текстовыми файлами. Если пользователи компьютеров вашей сети достаточно квалифицированы, то на сервере можно сохранять обновления программного обеспечения. Тогда пользователи могут запускать файлы SETUP с FTP-узла, избавившись от присмотра за своими дисками или от приглашений специалистов по обновлению приложений.

Поиск публикаций

Еще одно применение Web заключается в предоставлении общего доступа крупным организациям к результатам исследований. Например, несколько агентств Министерства обороны США совместно используют одну корпоративную интрасеть. В этой сети есть база данных Web, называемая IntelLink, в которой публикуются данные, собранные аналитическими отделами. Пользователи IntelLink, в том числе политики, военнослужащие ("борцы за войну" на армейском жаргоне), руководители, - словом, все, кто имеет право доступа, могут обращаться к базе данных IntelLink за статистическими сведениями, рисунками, картами и данными о военном снаряжении. Без такого Web-приложения им пришлось бы для подготовки специальных отчетов обращаться к аналитикам. Очевидно, аналитики все же занимаются пользовательскими отчетами и брифингами, однако ответ на запрос "в электронном виде" не требует от них особых усилий.

Почему используют Web

Корпоративная локальная сеть, в которой предусмотрено совместное использование файлов, голосовая связь и электронная почта также предоставляет совместный доступ к информации и позволяет проводить виртуальные конференции — для этого вовсе не требуется Web. Так зачем же создавать Web-узлы и приложения? Главным образом потому, что Web предоставляет простые средства обеспечения согласованного внешнего вида публикуемых данных и несложный метод управления доступом к ним.

Согласование внешнего вида

Интерфейс Web для работы с приложениями или информацией можно сделать сколь угодно простым или, наоборот, сложным. Обычный вход в локальную сеть с использованием приложений (см. гл. 11), требует от пользователей доступа к этим приложениям (как локального, так и на сервере приложений или терминальном сервере), и умения работать с ними. Но интерфейс Web-приложений для доступа к ресурсам любого типа требует использования броузера, а не приложения. Иными словами, независимо от того, получают ли пользователи доступ к базе данных либо отсылают электронную почту, они могут использовать свои Web-броузеры для загрузки созданного вами интерфейса. Это не только не ограничивает число приложений,

доступных пользователям сети, но также означает, что внешний интерфейс приложения (application front end) может быть сколь угодно простым или сложным, как того требует ваша пользовательская среда. Например, если пользователям достаточно средств для подготовки отчетов за некоторый период с помощью базы данных (database report), то можно создать интерфейс с местом для ввода дат и кнопкой, снабженной надписью "Генерировать отчет". В данном случае нет никакой необходимости учить кого-нибудь применению клиентных средств управления базой данных (database client).

Использование форм, созданных на основе Web, повышает степень взаимного соответствия документов не только у пользователей, но и у людей, принимающих вводимую пользователями информацию. Это наблюдение относится и к приложениям. Например, некоторые приложения электронной почты поддерживают HTML-протокол и таким образом могут отображать сформатированные приглашения на прием либо официальные сообщения. Однако электронная почта — "слабое" приложение для передачи важной информации, поскольку она не поддерживает работу с формами. Люди могут принять (RSPV) ваше приглашение по электронной почте, однако у вас нет возможности заставить их предоставить всю необходимую информацию. Приглашение же отобедать, отосланное по Web, может содержать раздел RSPV, в котором пользователи смогут указать, кто будет их сопровождать, количество гостей, которых они приведут с собой, а также выберут блюда из прилагаемого списка. Это же приглашение, отправленное по электронной почте, даст ответ в произвольной форме, который может содержать всю информацию либо ее часть, либо вообще ничего конкретного. Точно так же стандартные отчеты, которые пользователь сможет выбирать из списка, исключают возможность синтаксических ошибок (пользователя). Корректно используйте синтаксис языка составления запросов — это облегчит жизнь.

Безопасное распространение информации

Распространение информации с помощью Web-средств обеспечивает не только ее согласованность, но и некоторые дополнительные уровни защиты. Вспомните: некоторые оперативно распространяемые документы (online documents) намного сложнее исказить, чем распространяемые в форме, доступной для редактирования пользователем. Учтите: FTP-узлы позволяют предоставлять доступ к документам, без отображения исходного каталога. Более того:

- страницы можно защитить, чтобы предоставить доступ только некоторым пользователям либо тем, кто знает пароль;
- единственным интерфейсом для работы с базой данных могут служить только стандартные запросы (canned queries), а прочая информация из базы данных может не включаться в отчеты;
- доступ в комнату для переговоров (chat rooms) можно ограничить узким кругом пользователей, а для остальных — закрыть.

В общем, если вам нужен согласованный, но настраиваемый интерфейс для распространения (data dissemination) и поиска данных, корпоративная Web-сеть предоставляет для этого великолепную среду. Она динамична, повсеместно доступна, а ее содержимое нелегко исказить.

Создание содержимого для Web

Содержимое Web-среды может быть весьма простым — ограничиваться почтовыми сообщениями и несколькими рисунками, но может быть и сложным (содержать ссылки из текущего текста на внутренние приложения или иные страницы). Создавая содержимое, поразмыслите над тем, кто будет его использовать и, исходя из этого, выберите инструменты для

создания нужного эффекта.

Планирование содержимого и структуры узла

Как принято при подготовке к сложной работе, первый этап создания Web-узла начинается не с "просиживания" за Notepad или вашим любимым редактором HTML и копировании HTML для болванов, а планирования. Ответьте на такие вопросы.

- Кто будет просматривать информацию?
- Как следует организовать содержимое?
- Следует ли предоставить доступ к содержимому всем желающим либо следует скрыть некоторую часть от всех, кроме узкого круга лиц?
- Откуда будет поступать содержимое?

Если это обдумать заранее, то впоследствии вам будет проще скомпоновать материалы. Пока вы не уточните, кто будет просматривать информацию, вы не сможете планировать интерфейс или систему защиты. Пока вы не уточните, каким образом следует скомпоновать содержимое и откуда оно должно поступать, вы не сможете написать программу (код), позволяющую открыть доступ к содержимому.

Советы по разработке узла

Качество структуры Web-узла в немалой степени зависит от простоты и удобочитаемости содержимого. Множество Web-узлов загружено исключительно перепевами на тему "Мое_Мнение", но главное их назначение (в том числе Web-узлов интрасетей) - распространение информации. Если читателям прочесть эту информацию нелегко, то они и не станут ее читать. В таком случае незачем и время тратить на создание узла.

Организация данных. Как правило, Web-страницы — это трехмерные структуры, содержащие не только собственно содержимое страницы, но и ссылки на другие страницы. Разумеется, можно построить Web-узел, состоящий из набора несвязанных элементов, однако навигация по узлу значительно упрощается, если каждая страница является частью единого целого набора данных.

Совет

Единственное исключение из этого правила - защищенные страницы. Если всеобщий доступ к конкретной странице нежелателен, простейший способ ограничения доступа - не связывать ее с другими страницами, и не публиковать ее URL. Если содержимое страницы действительно секретно, защитите ее паролем - это пресечет праздное любопытство.

Начертите карту источников данных для вашего Web-узла, карту связей страниц (page links) и других компонентов. Это поможет вам организовать данные еще на стадии планирования (рис. 13.1). После реализации намеченной структуры узла вы готовы к вводу содержимого и началу работы.

Совет

Некоторые HTML-редакторы, например Microsoft FrontPage, позволяют создавать и графически упорядочивать страницы, значительно упрощая разработку Web-узлов.

Не перегружайте буферы пользователей. Мерцание элементов и их подсветка затрудняют чтение с экрана (по сравнению с чтением печатной копии). Большинство людей читает с монитора примерно втрое медленнее, чем "с листа". Таким образом, одно из основных

правил создания текста гласит: будьте кратки. По возможности поместите текст на одну страницу, чтобы не приходилось прокручивать ее содержимое. Если это невыполнимо (например, если вы кодируете длинный документ для распространения в онлайн-режиме (online dissemination)), используйте белое поле (white space), чтобы несколько упростить страницу. Ни в коем случае не форматируйте страницу так, чтобы людям пришлось прокручивать ее по горизонтали. Предусмотрите в коде динамическое самоупорядочение текста, с тем чтобы он автоматически масштабировался в соответствии с размерами окна броузера.

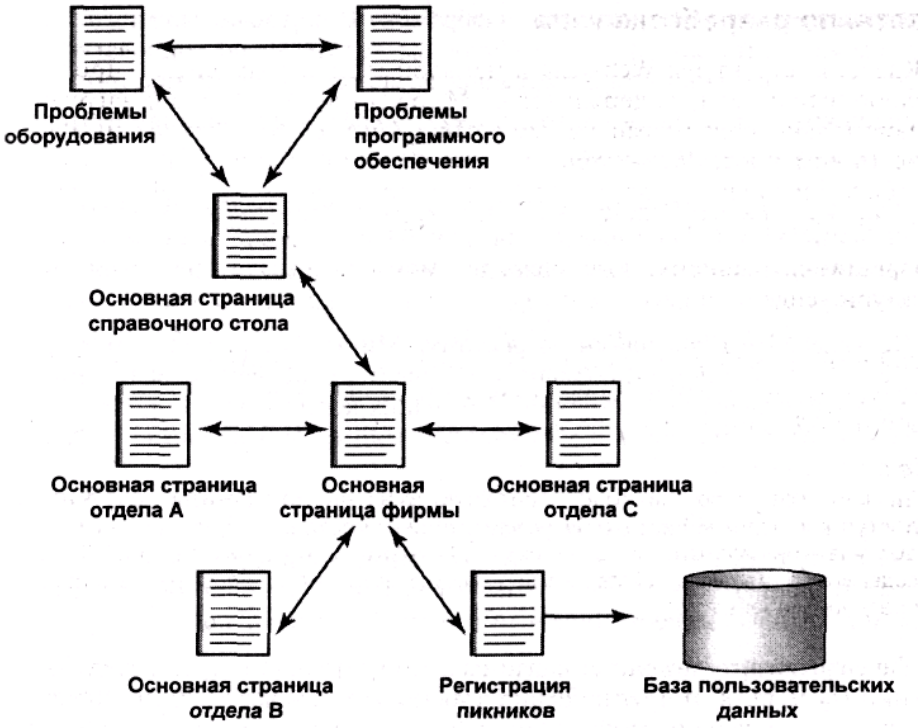


Рис. 13.1. Прежде, чем начинать ввод содержимого, начертите карту вашего Web-узла

Кроме того, выполняя организацию текста важно обеспечить четкое восприятие сообщений. Человеческий мозг в состоянии запомнить и воспринять одновременно не более семи предметов (Если быть более точным, то их количество колеблется от пяти до девяти — Прим. ред.). В соответствии с этим распределите содержимое. Избегайте длинных маркированных списков и нумеруйте небольшие наборы, а если создаете длинный документ для публикации в онлайн-режиме, попытайтесь разбить документ на разделы, которые можно загружать отдельно, пользуясь оглавлением.

Поддерживайте, а не подавляйте текст. Основное (по крайней мере, декларируемое) преимущество интерактивного документа — легкость чтения. Упустив это из виду, вы, безусловно, ухудшите визуальный эффект. Поэтому применяйте простой фон, который "помогает" тексту, а не отвлекает от него внимание.
Что сказать о фоновых изображениях? Опять-таки, они полезны, если помогают воспринимать текст, а не отвлекают от него внимание. В целом, следует избегать фоновых изображений, которые:

- состоят из повторяющегося узора того же размера, что использованный шрифт, поскольку в этом случае буквы будет трудно отличить от фона;
- составлены из рисунков или изображений, которые могут отвлекать внимание читателя от текста. Если вы хотите иллюстрировать текст, вставляйте рисунки или фотографии возле текста, но не под ним;

- очень яркие или очень контрастные, что вредно для зрения читателя;
- близкие по цвету с текстом.

Не следует рассчитывать на одинаково точную передачу оттенков цвета всеми мониторами. Цветовая схема должна быть достаточно рельефна, в противном случае некоторые элементы могут исчезнуть при передаче или преобразовании.

Не увлекайтесь внешними эффектами. Мигающие значки, крутящиеся глобусы и т.п. хороши в небольших количествах, особенно, если они способствуют привлечению внимания. В больших количествах они, безусловно, отвлекают от текста. Если же их чересчур много, они вызывают головную боль и раздражение.

А как быть со звуком? Автор книги не сторонник озвучивания Web-страниц, а в офисном окружении это вообще недопустимо — разве что каждый служащий работает в отдельном кабинете. Любой звуковой эффект мешает работе коллег, да и не каждый компьютер оборудован колонками, которые издают приятный (по крайней мере) звук.

Поддерживайте связи. Создайте связи, облегчающие навигацию по содержимому узла. В этом отношении удобны кнопки возврата (back buttons), но еще лучше использовать карту узла (site map), доступную из любого места. Если вам нравятся рамки, можете поместить карту узла в рамку на одной из сторон отображаемого в данный момент документа. Если рамки вам не нравятся, можно поместить связи с важными страницами (скажем, основной страницей узла) в верхней или нижней части каждой страницы.

Отличия содержимого интрасетей от содержимого Internet

Теперь, когда вы совершенно запуганы, сообщим вам и приятную новость: потенциально создание содержимого Web-узла в интрасети намного проще, чем в World Wide Web. Во-первых, вам намного проще контролировать пользователей, поскольку вам известно, какие броузеры они собираются применять и какие средства они поддерживают. Разные броузеры по-разному интерпретируют одну и ту же информацию и поддерживают разные средства. Например, в Netscape Navigator не встроена поддержка элементов ActiveX — для этого следует загрузить специальную надстройку. С другой стороны, Microsoft поддерживает нестандартный тип языка Java, поэтому поддержка со стороны Microsoft Internet Explorer страниц, использующих Java, крайне неопределенна — иногда они работают, иногда — нет.

Примечание

Java - это язык программирования, созданный фирмой Sun Microsystems для работы на любой компьютерной платформе без регистрации (recording). Подробнее язык Java и родственные с ним языки обсуждаются далее в специальном разделе этой главы.

Во-вторых, хотя вы, конечно, не хотите создавать страницы, которые заставят вашу офисную LAN со скрежетом остановиться, в корпоративной интрасети проблемы наличия достаточной полосы пропускания не столь серьезны, как в World Wide Web, работающей только по телефонной линии. Действительно, соединение, работающее со скоростью 100 Мбит/с, загрузит Web-страницу в броузер клиента намного быстрее, чем модем, работающий со скоростью 50 Кбит/с. Даже если интрасеть является частью глобальной сети, ее трафик может быть намного меньше трафика Internet в период пиковых нагрузок. И, конечно, им намного проще управлять.

В-третьих, защита данных в офисной локальной сети — не столь сложная задача, как в World Wide Web. В системе защиты Web-страниц остались просчеты, которыми может воспользоваться злоумышленник для редактирования содержимого вашей Web-страницы. (В конце 1998 г. общедоступный Web-узел газеты New York Times взломали хакеры. Чтобы

скрыть от мира такой позор, страницу пришлось закрыть.) Однако присутствие злоумышленника в локальной сети менее вероятно, чем в огромной Internet. Кроме того, вероятность взлома значительно ниже хотя бы потому, что потенциальный "шутник" знает, что он, весьма вероятно, будет обнаружен.

Совет

Об этих различиях полезно постоянно помнить при планировании переноса узлов из локальной сети Web в World Wide Web. Страницы, которые великолепно работают в локальной сети, могут оказаться непригодными для Internet.

Языки разметки текста

Иногда можно услышать о "программировании" Web-страницы, однако форматирование текста в окне броузера фактически не относится к программированию. Как следует из названий языков форматирования, они относятся к языкам разметки (markup languages). Иными словами, они состоят из различных символов, вставленных в тело документа, указывающих, как должен выглядеть файл при печати или отображении либо для определения его логической структуры (например, абзацев и маркированных списков). Если не использовать язык разметки, отображаемые данные представляют собой неструктурированный текст (raw text), без форматирования символов или абзацев.

Языки разметки определяют внешний вид документа с помощью кодов, называемых дескрипторами или тегами (tags), которые имеют примерно такую форму: <tag> </tag>. Первый дескриптор указывает точку начала форматирования, а второй (с наклонной чертой) — окончание кода. Если опустить второй дескриптор, кодирование, задаваемое первым дескриптором, применяется до конца документа.

Примечание

Язык разметки можно применить к неструктурированному тексту либо вручную, либо с помощью текстового редактора (например, Notepad), либо с помощью графического инструмента, добавляющего код, когда вы визуально упорядочиваете текст по собственному вкусу. Новичкам проще работать с графическими инструментами, которые не так точны, как текстовые редакторы.

Язык разметки гипертекста (HTML)

Язык HTML (HyperText Markup Language — язык разметки гипертекста) — основа кодирования и "становой хребет" большинства Web-страниц. HTML позволяет публиковать текст и рисунки, содержимое электронных таблиц и даже создавать отчеты на основе баз данных для чтения в интерактивном режиме. Он прекрасно подходит для организации и форматирования статической информации любого типа, поскольку позволяет:

- устанавливать размер и шрифт текста;
- форматировать текст полужирным шрифтом, курсивом или выделять подчеркиванием;
- задавать ссылки на другие страницы;
- вставлять изображения;
- создавать заголовки страниц;
- создавать таблицы;
- вставлять метаданные, необходимые для работы машин поиска.

Примечание

Метаданными (metadata) называют скрытые данные, которые не отображаются на Web-странице, однако могут быть обнаружены машиной поиска (engine search), что позволит попасть на данный узел.

Применяются дескрипторы HTML трех типов.

- Для форматирования текста или отдельных символов.
- Для форматирования абзацев либо иных крупных текстовых блоков.
- Невидимые дескрипторы, которые обеспечивают остальные функциональные средства, например метаданные, для выполнения поиска.

Основное преимущество HTML перед остальными языками разметки — потрясающая универсальность. Текущую версию HTML поддерживает практически любой броузер (разумеется, современный и поддерживающий графические средства). Это не всегда верно для динамического HTML (DHML), XML, Java и ActiveX. Если вы хотите, чтобы ваши Web-узлы были доступны для броузеров всевозможных типов, рекомендуем использовать HTML.

Динамический HTML (DHML)

Динамический HTML (Dynamic HTML — DHML) более гибок по сравнению с HTML. Вместо того чтобы выставлять на всеобщее обозрение статичную Web-страницу, вы можете использовать DHTML и создать Web-страницу, которую пользователь сможет настраивать без нарушения вида исходного документа. Например, страница, подготовленная с помощью DHTML, может содержать различные элементы, которые пользователь сможет перемещать по странице, чтобы перегруппировать ее содержимое (по собственному вкусу). Однако при обновлении (refreshing) изображения на странице изменения пропадают, и она принимает исходный вид.

DHTML поддерживает следующие средства, отсутствующие в HTML.

- Динамические стили.
- Точное позиционирование.
- Привязку данных.
- Динамическое содержимое.

Вам непонятно, что это такое? Не беспокойтесь — ниже приведены пояснения.

Применение стилей к документам Web. Динамические стили (dynamic styles) основаны на принципах каскадирования таблиц стилей (CSS — cascading style sheets), когда они применяются к странице в целом вместо ручного форматирования отдельных частей страницы. Если вы работали с современными текстовыми процессорами, то, возможно, знакомы с таблицами стилей (style sheets), позволяющими автоматически сформатировать текстовые блоки тем или иным методом в зависимости от стиля, который вы им задали. Форматирование подразумевает изменение цвета текста, шрифта, размещения, видимости - вообще практически всего, что относится к реквизитам текста. CSS (и DHTML), делает то же самое, только применяется для обработки Web-страниц, а не для текстов.

В динамических стилях, реализуемых с помощью DHTML, предусмотрены средства, отсутствующие в текстовых процессорах. Например, вы можете при создании ссылок разметить текст так, что его цвет будет автоматически изменяться при наведении на него указателя мыши либо отображаться, когда вы проводите курсор над определенной областью экрана. Единственный недостаток этих стилей заключается в том, что вы должны включать таблицы стилей в большинство документов. Это трудоемкая работа, особенно для тех, кто неопытен в работе с таблицами стилей или занимается конвертированием документов.

Размещение текста в нужном месте. Еще одно достоинство DHML — его способность точно указать место размещения элемента на странице. Для указания положения объекта используют горизонтальную (x), вертикальную (y) и даже объемную (z) координаты. (Задание положения объекта в трехмерной системе координат позволяет "перекрывать" объекты.) Точ-

ное позиционирование позволяет расположить текст вокруг изображения, а также перемещать объекты в пределах окна броузера.

Примечание

HTML без CSS не обеспечивает точного размещения объектов. В этом случае размещение элементов определяется броузером.

Вставка данных на страницу. Чтобы предоставить пользователям доступ к некоторой внутренней информации (back-end information), например, хранящейся в базе данных, обычные страницы HTML должны быть связаны с сервером, на котором находятся исходные данные, и требуется запрашивать разрешение на манипулирование этими данными. DHTML позволяет привязать данные к конкретной странице, допуская работу с привязанными (или точнее - связанными) данными (bound data) без нарушения исходных данных и даже без взаимодействия с сервером, хранящим их. Для этого источники данных вводят в страницу (их можно сортировать и фильтровать точно так же, как и содержимое любой базы данных). Это не только снижает загрузку сервера, но также позволяет пользователям просматривать и манипулировать данными без предоставления им доступа к источнику самих данных.

Создание динамического содержимого. Таблицы стилей (style sheets) дают возможность издателю (publisher) Web без труда изменять внешний вид страницы или набора страниц. Динамическое содержимое позволяет пользователю Web изменять внешний вид (представление) страницы исполнением сценария, чтобы:

- вставлять или скрывать элементы страницы;
- модифицировать текст;
- изменять структуру текста;
- перемещать данные из внутренних источников (back-end sources) и отображать их по запросу пользователя.

В отличие от языка HTML, допускающего изменение содержимого страницы только до ее загрузки в броузер пользователя, DHTML может воспринимать изменения в любое время. Динамическое содержимое дает возможность обеспечить высокий уровень интерактивности, если используется вместе со сценариями, позволяющими пользователям определять элементы, которые необходимо просмотреть.

Совет

В разделе "Организация собраний" (см. выше) упомянута карта здания, созданная на основе Web-данных, отображающая расположение конкретного офиса и портрет служащего, которого пользователь пытается отыскать. Эта карта создана с помощью DHTML-средств - языка разметки для создания динамического содержимого.

Расширяемый язык разметки (XML)

Язык XML (Extensible Markup Language - расширяемый язык разметки) не заменяет HTML (во всяком случае, он редко встречается на Web-страницах), однако поддерживает его, позволяя несколько повысить универсальность Web-страниц.

Идея такова: когда вы форматируете страницу с помощью HTML, то можете изменить внешний вид текста дескрипторами, форматирующими его полужирным шрифтом, курсивом, подчеркиванием, абзацами и т.д. Однако сами дескрипторы практически никак не связаны с содержимым текста, а только с его форматированием. Язык XML имеет дескрипторы, определяющие внешний вид текста. Вы можете с их помощью указать, что обозначает данный текст (имена, адреса, названия продуктов и т.д.).

Зачем это нужно? Прежде всего, эти метаданные позволяют машинам поиска найти предварительно заданные элементы. Если вы проведете в Web-узле вашей корпорации (созданном с помощью языка HTML) поиск по слову "name", просматривая все упомянутые в нем

имена, то в результате возвратятся все экземпляры слова "name", но не сами имена. Однако если при создании узла использовалось кодирование с помощью языка XML, в результате будет возвращен любой текст, имеющий дескриптор имени "name". Во-вторых, снабженные дескриптором части текста могут быть полезны, если вам необходимо применить некое средство (например, цвет или язык) только к отдельным частям документа Web. Пусть, например, интерактивный документ представляет собой краткий рассказ на испанском языке с переводом на английский. Тогда вместо переключения документа с поддержки испанского языка на поддержку английского, можно определить эти части рассказа дескрипторами <story></story> и применить правила испанского языка только к этим частям, а переводы оставить на английском. По существу, применение языка XML значительно облегчает разработку Web-страницы, особенно если некоторые его части необходимо создать как изолированные элементы.

Приложения и языки сценариев

Если необходимо, чтобы Web-страница могла делать что-нибудь еще, кроме отображения текста и изображений, в нее следует включить средства поддержки определенных мини-программ. С "точки зрения" клиента они принимают форму элементов управления ActiveX или аплетов Java. С "точки зрения" сервера мини-программы могут использовать внешний интерфейс общего шлюза (CGI — Common Gateway Interface) для программ, хранящихся на сервере, либо сценарий, встроенный в саму страницу с помощью страниц активного сервера (Active Server Pages — ASP) Microsoft.

Клиентные Web-приложения

Клиентные Web-приложения и исполняемые файлы загружаются клиенту с Web-сервера, но для их выполнения используются ресурсы клиентного компьютера. Клиентные приложения могут предоставлять такие средства, как программы голосовой связи либо иные приложения, наподобие тех, которые могут быть многократно использованы, пока страница остается открытой.

Язык Java. Java — язык, применяемый на многих платформах (cross-platform language), разработан фирмой Sun Microsystems. Основная его концепция — способность к взаимодействию. Аплеты Java — это миниатюрные приложения, которые могут исполняться на любой платформе — DOS, Windows, UNIX, Windows NT и многих других. При запуске аплет Java прежде всего создает для себя среду исполнения программы (называемую песочницей (sandbox)), а затем работает уже в ее контексте. Теоретически, использование этой среды имеет такие последствия. Во-первых, обеспечивается выполнение аплета на любой платформе, поскольку при этом создается операционная среда (operating environment), необходимая аплету. Во-вторых, аплет никоим образом не может повлиять на базовое операционное окружение (native operating environment), так как он никогда не соприкасается с ним.

К числу аплетов Java, с которыми, возможно, вам довелось встречаться, относятся Netcaster, входящий в Netscape Communicator, а также планировщики путешествий, применяющиеся в некоторых мобильных Web-узлах. Netcaster представляет собой средство внешнего интерфейса, используемого в технологии извлечения информации (pull technology) Netscape (т.е. извлечения содержимого из Web-узлов без фактического входа в узлы). Планировщики путешествий воспринимают введенные вами пользовательские установки, выполняют поиск в базе данных расписания авиарейсов, соответствующих вашим запросам, а затем возвращают результаты.

Возможно, вы уже слышали различные слова, используемые в языке Java. Хотя эта книга не может служить полным руководством по этому языку, но в табл. 13.1 поясняются некоторые, наиболее общие термины.

Таблица 13.1. Терминология языка Java

Термин	Описание	Комментарии
HotJava	Основной броузер для поддержки Java. Программа броузера написана полностью на языке Java.	HotJava поддерживает любую комбинацию нескольких различных режимов просмотра (интерактивных приложений), позволяющих с помощью броузера настраивать их средства.
Java Beans	Компоненты, которые можно использовать для создания различных приложений Java.	Упрощает программирование на языке Java, позволяя разработчикам многократно использовать программный код.
JavaScript	Язык сценариев, разработанный фирмой Netscape. Отнюдь не все броузеры одинаково хорошо поддерживают JavaScipt. Наиболее надёжен Netscape Navigator (что и неудивительно).	Помимо прочего, JavaScript можно использовать для поддержки форм, таймеров, выполнения расчётов и идентификации используемых броузеров.

Примечание

Не все броузеры одинаково хорошо поддерживают язык Java. Так, поддержка его приложением Internet Explorer неоднородна. Кроме того, в версию Java (называемую Java++), применяемую фирмой Microsoft, включены некоторые дополнительные средства (отсутствующие в версии Java фирмы Sun Microsystems), основанные на функциональных средствах Windows. Поэтому Internet Explorer, запущенный в иной операционной системе (кроме Windows), вероятно, не сможет предоставить полный набор функциональных средств аплетов Java ++.

Элементы управления ActiveX аналогичны Java, так как предоставляют способ присоединения к Web-страницам мини-приложений, однако они отнюдь не идентичны. Элементы ActiveX — это не язык программирования, независимый от платформы, а набор элементов управления, позволяющий создавать приложения с помощью множества различных языков, например, C++, Delphi, J++ и Visual Basic, доступ к которым можно получить через броузер. Элементы управления ActiveX исполняются не в специально создаваемом окружении, а подобно любому приложению — в пользовательском операционном окружении (user operating environment).

Серверные Web-приложения

Серверные Web-приложения (server-side Web applications) выполняются сервером: средствами серверного операционного окружения (server operating environment), а также за счет аппаратных ресурсов сервера. Серверные приложения более всего напоминают однократно запускаемые приложения (one-time applications), такие как механизмы поиска (search engine). Преимущество серверных приложений заключается в их универсальности: броузеру нет нужды поддерживать язык клиентного приложения. Для хранения и загрузки таких программ применяют разные подходы. Серверы CGI получают доступ к приложениям, хранящимся на сервере, в то время как ASP (Active Server Pages — страницы активного сервера) сохраняют сценарий, который должен выполняться на самой странице HTML.

Интерфейс общего шлюза (Common Gateway Interface — CGI). CGI представляет собой стандартный путь передачи информации, введенной пользователем Web, на внутреннее приложение или сценарий, а затем обратной передачи на броузер клиента. Например, когда вы заполняете онлайновую регистрационную форму (online registration form) и щелкаете на Submit (Подтверждение), введенная вами информация с помощью CGI передается в базу данных. После ее обработки вы получаете сообщение "Thank you!" (Спасибо!), опять-таки через CGI.

Основное преимущество CGI заключается в его согласованном интерфейсе. Платформа, на которой работает сервер, не имеет значения: пользовательские данные можно передавать приложению независимо от нее. Функциональные средства, которые вы можете получить с CGI для доступа к внутренним приложениям, не обязательно отличаются от тех, что можно получить, используя язык сценариев — просто они по-разному работают. Сценарий присоединяется к конкретной Web-странице, однако приложение, доступное через CGI, связано не с конкретной страницей, а, скорее, с конкретным шлюзом. С этим же шлюзом могут ассоциироваться любые Web-страницы.

Страницы активного сервера (Active Server Pages — ASP). Во многих Web-страницах имеются внедренные в них сценарии, которые запускаются при выполнении соответствующих условий — скажем, пользователь щелкает на Find (Найти) механизма поиска либо заполняет форму и щелкает на OK. Вы можете создать файл ASP, включив в документ HTML сценарий, написанный на языке VBScript (или ином поддерживаемом языке сценариев), а затем переименовать документ, воспользовавшись расширением .asp. Сценарий запускается, когда пользователь загружает эту страницу и выполняет надлежащие действия.

Примечание

Страницы активного сервера поддерживаются только информационным сервером Internet (IIS) в среде Windows NT.

Публикация Web-документов

Теперь вы ознакомились с инструментами, которые будете использовать для создания Web-страниц вашего узла. Чтобы собрать узел в единое целое, необходимо использовать еще один инструмент: Web-сервер.

Где взять программное обеспечение сервера?

Если вы используете продукты Microsoft, то, вероятно, у вас уже установлен Web-сервер. Если это не так, его можно получить без каких бы то ни было проблем. Windows NT Server 4 поставляется с уже упомянутым информационным сервером Internet (IIS) версии 2. Используя Service Pack 3 (и последующие пакеты) для Windows NT, можно автоматически дополнить его до IIS 3. Однако версия 4, так же, как и Peer Web Server (Одноранговый Web-сервер) для Windows 95 и Windows NT Workstation, входят в состав пакета Microsoft Option Pack. Продукт Peer Web Server находится на установочном компакт-диске Windows 98.

Примечание

Как найти эти продукты на узле Microsoft? Поскольку фирма Microsoft перегруппирует свой узел раз в месяц, не гарантируется достоверность конкретных URL-адресов, однако Option Pack должен находиться в разделе Free Downloads (Бесплатная загрузка) узла.

Кроме того, в настоящее время можно загрузить 90-дневную оценочную версию Site

Server (продукт для работы в интрасети для Windows NT Server) фирмы Microsoft.

Те, кто работает в сетях NetWare, могут воспользоваться одним из продуктов серии Intranet фирмы Novel.

IntraNetWare. В сущности, это сервер NetWare, в который включены средства маршрутизации FTP и IP/IPX.

IntraNetWare Host Publisher. Предназначен для публикации информации, хранящейся на мэйнфреймах IBM.

GroupWise Web Publisher. Групповое программное обеспечение, поддерживающее публикацию в Web информации любого члена группы GroupWise.

Примечание

Оценочные версии продуктов Intranet фирмы Novel можно загрузить с узла www.novell.com. Кроме того, средства составления Web-публикаций в интрасетях поддерживает текущая версия сервера Lotus Domino.

Пример: установка IIS 4

Windows NT Server 4 поставляется вместе с компонентом IIS 2, который можно установить, запустив программу SETUP из папки Internet Tools, помещенной в раздел Programs меню Start (Пуск). Сервер IIS 3 входит в состав Service Pack 3 (и последующих пакетов). Чтобы установить последнюю версию IIS 4, следует использовать пакет Option Pack, записанный на компакт-диске с месячной подпиской на Microsoft TechNet (выпущенный на конференции TechEd фирмы Microsoft в 1998 г.). Кроме того, его можно бесплатно загрузить с Web-узла фирмы Microsoft. Так или иначе, сервер IIS 4 всегда доступен всем, кому он нужен.

Подготовка к установке IIS 4

Прежде чем начать установку Option Pack на ваш компьютер, работающий под управлением Windows NT Server, следует установить Internet Explorer 4.x (IE4) и Service Pack 3 (SP3) (либо самую последнюю его версию), если вы еще не сделали этого. Можете и не использовать IE4 в качестве броузера вашего Web-сервера, если это вам не нужно, однако IIS 4 обращается к некоторым файлам IE4.

Где взять эти файлы? SP3 входит в состав Option Pack. SP4 доступен на узле фирмы Microsoft. IE4, хотя и включен в компакт-диск Option Pack, не входит в состав Web-узла "Option Pack". Его следует загрузить с того раздела Web-узла Microsoft, который относится к Internet Explorer.

Загрузка установочных файлов

Если у вас еще нет установочных файлов Option Pack, вы можете загрузить их с Web-узла фирмы Microsoft по адресу www.microsoft.com. Здесь не приведен точный URL, поскольку фирма Microsoft перегруппировывает свой узел примерно раз в месяц, однако, следуя описанным ниже ссылкам, вы сумеете найти нужные области. На основной странице Microsoft содержатся ссылки на все области узла.

1. Войдите в раздел Free Downloads (Бесплатная загрузка) Web-узла фирмы Microsoft и перейдите на Sever Software (Отдельные программы). В списке продуктов щелкните на IIS 4.

2. На этой же странице щелкните на ссылке (link) на элементе Windows NT 4 Option Pack.
3. На этой странице выберите продукты, которые вам необходимо загрузить.

- Internet Information Server 4 (Информационный сервер Internet версия 4).
- Transaction Server 2 (Сервер для обработки транзакций версия 2).
- Microsoft Message Queue Server 1 (Сервер очередности сообщений Microsoft версия 1).
- Internet Connections Services for Microsoft RAS (Средства организации Internet-связи для сервера RAS фирмы Microsoft).
- Windows NT Service Pack 3.

Выберите здесь IIS 4, IE4 и (если вы еще не установили) SP3.

4. На следующей странице вы найдете требования, предъявляемые к аппаратному и программному обеспечению и более подробную информацию о выбранных продуктах. Рекомендую прочитать ее. В нижнюю часть страницы помещена ссылка для регистрации и загрузки Option Pack.
5. Затем заполните форму (достаточно указать только тип процессора компьютера) и выберите параметры загрузки.
6. Далее выберите тип пакета Option Pack, который вам необходимо загрузить (в данном случае — Windows NT Server), а потом — язык.
7. Укажите место загрузки.

Примечание

Для снижения трафика Internet в соответствии с правилами сетевого этикета рекомендуется использовать для загрузки ближайший узел.

8. На последней странице прочитайте инструкции (это очень важно), а затем щелкните на каждой ссылке для загрузки соответствующего содержимого. Необязательно загружать все файлы строго по порядку, однако все они должны находиться в одном каталоге. Вы не сможете запустить программу SETUP, пока не загрузите содержимое всех ссылок.

Предупреждение

Время загрузки определяется двумя факторами: быстродействием соединения с Internet и интенсивностью сетевого трафика в период загрузки компонентов. Поскольку надо вручную загрузить все 52 части общим объемом более 70 Мбайт (в данном случае вы не можете начать загрузку и отправиться на ленч), то это случай, когда окупается быстрое сетевое соединение. При медленном соединении процесс может занять весь день.

Установка IIS 4

После копирования файлов и установки SP3 и IE4 перезагрузите компьютер. Теперь вы готовы устанавливать IIS 4.

1. Запустите файл SETUP.EXE из папки, в которую вы загрузили файлы. (Не запускайте программу INSTALL.EXE — в этом случае появится сообщение об ошибке, требующее предоставить параметры основных файлов .INF и исходных папок.) Вы увидите экран мастера установки Option Pack. Чтобы продолжить, щелкните на Next (Далее) и, перейдя на следующую страницу, примите лицензионное соглашение.

2. Если на вашем компьютере уже установлена какая-либо версия информационного сервера Internet (IIS), т.е. вы уже приняли лицензионное соглашение, можно выбрать либо простое обновление существующей версии, либо обновление с добавлением новых компонентов. В первом случае щелкните на Upgrade Only (Только обновление). Чтобы добавить новые компоненты, выберите Upgrade Plus (Обновление с дополнениями).

Обратите внимание: в обоих случаях не требуется удалять ранее установленные компоненты.

3. Выберите вариант Upgrade Plus. На экране появится диалоговое окно (рис. 13.2), в котором будут перечислены доступные компоненты. Ранее установленные компоненты будут отмечены затемненными флажками — удалить их невозможно. Убедитесь, что выбрана опция "Internet Information Server (IIS)" и щелкните на Next.

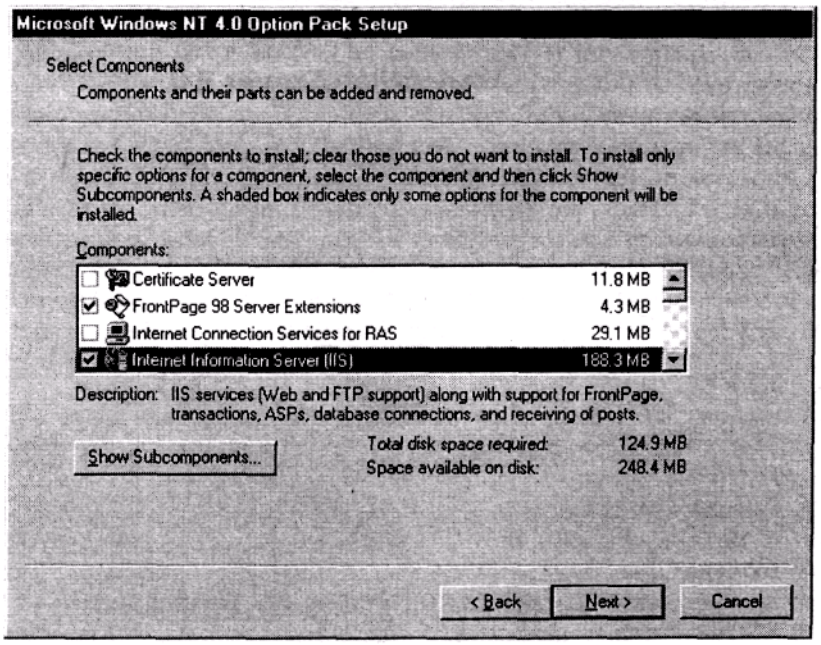


Рис. 13.2. Выберите компоненты Option Pack, которые необходимо установить

Примечание

Каждый компонент, как правило, состоит из нескольких субкомпонентов, и в этом отношении IIS - не исключение. Хотя вы и не можете удалить IIS, но можете включить в него несколько субкомпонентов, которые не установили ранее. К ним относятся, например, сервер новостей (NNTP) либо компонент SMTP, необходимый для работы электронной почты. Прежде, чем продолжить установку, обязательно просмотрите список субкомпонентов, входящих в IIS, и выберите нужные.

4. Введите имя локальной папки (можете воспользоваться подсказкой), в которую следует скопировать файлы для каждого компонента. По умолчанию программа установки копирует их в подпапку в C:\Program Files.

5. Если вам необходимы средства удаленного администрирования (remote administering) информационным сервером Internet с другого сервера Windows NT, введите имя и пароль существующей учетной записи администратора, которому следует предоставить это право (рис. 13.3). Если же вы собираетесь выполнять всю работу локально (стандартная опция), эти поля не надо заполнять.

6. После щелчка на Next программа SETUP скопирует необходимые файлы на жесткий диск сервера. Это может продолжаться достаточно долго. Когда же копирование завершится, и программа установки обновит файлы, то для запуска сервера IIS вам придется перезагрузить компьютер.

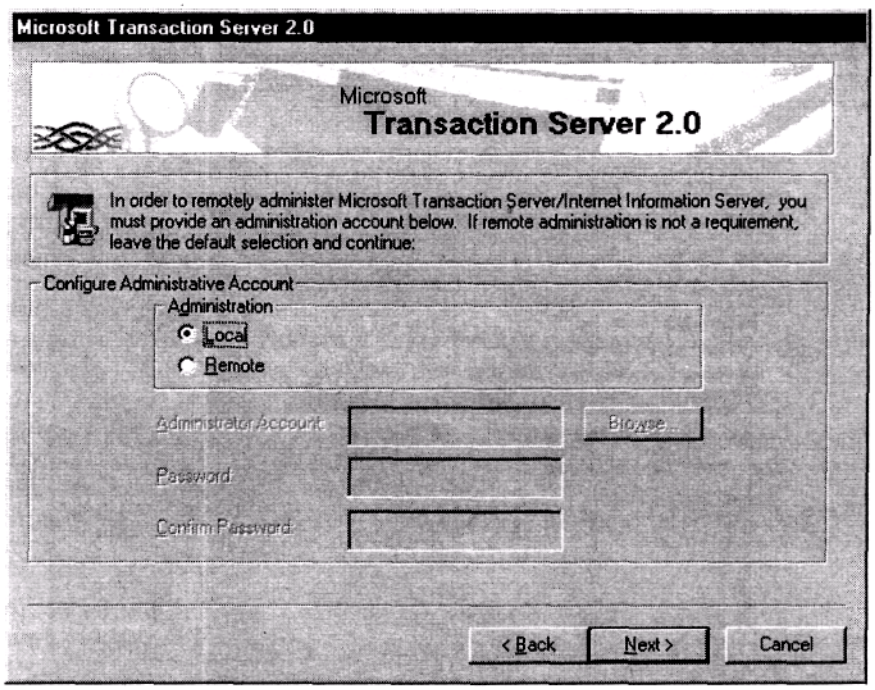


Рис. 13.3. Введите имя учетной записи удаленного администратора, если хотите управлять своим Web-сервером

Основные вопросы, возникающие при установке Web-узлов в интрасети

Эта книга не может служить полным руководством по использованию IIS 4, однако основные этапы создания Web-узла интрасети с помощью IIS 4 достаточно понятны и просты. Создайте Web-страницу на основе Notepad либо иного редактора HTML. Присвойте этому файлу имя DEFAULT.HTM и сохраните его в каталоге, заданном по умолчанию (default catalog) \InetPub\Wwwroot. Если вы уже установили в сети сервер DNS или иной механизм определения имен (name resolution mechanism), пользователям внутренней сети для получения доступа к узлу достаточно ввести имя Web-сервера. В противном случае, чтобы получить доступ к узлу, им придется вводить IP-адрес Web-сервера. Одним словом, вы сохраняете файлы в подходящем месте и публикуете их по сети. Затем вы можете изменить установки системы защиты, чтобы разрешить или запретить доступ к определенным страницам, настраивать страницы с описанием ошибок (error pages) (вроде всем известной и любимой "404 File Not Found" (Файл не найден)) или выполнять иные операции.

Выводы

Итак, теперь вы хорошо представляете работу корпоративной Web-сети. Если вы заботитесь об информационном обеспечении офиса, то следует установить приложения Web, предоставляющие средства для публикации отчетов, записи сотрудников на совместные пикники, быстрой поддержки запросов о помощи, создания карт офисов и т.д.

Для создания этих Web-приложений используются различные языки разметки (HTML, DHTML или XML) и программирования. Программы на этих языках могут исполняться как клиентной машиной, так и сервером, в зависимости от того, чьи ресурсы вы используете - клиента или сервера, а также от поддержки клиентных приложений броузерами клиентов.

Серверные приложения могут либо внедрять сценарии непосредственно в основную страницу, либо включать общераспространенные интерфейсные средства (common interface) в программы, хранящиеся на Web-сервере или другом компьютере. Создавая страницы, уделяйте основное внимание потребностям пользователей — страницы должны облегчать им работу, а не затруднять ее.

После создания Web-страниц вам понадобится Web-сервер для их публикации во внутренней сети корпорации. В этой главе была рассмотрена установка четвертой версии информационного сервера Internet (IIS 4) фирмы Microsoft, однако по существу в структуру всех Web-серверов (как и всех серверных операционных систем) заложены одни и те же идеи.

Мы завершили рассмотрение работы локальных сетей. В следующей главе подробнее изучим процесс администрирования в локальной сети, а начнем — с понимания основных принципов управления сетью.

Упражнение 13

1. Какой язык разметки, поддерживающий предметный поиск по категориям, следует использовать для создания Web-страницы?

2. Вам необходимо создать Web-страницу с функциональными средствами, которые смогут интерпретироваться любыми клиентными броузерами. Какой инструмент следует использовать с этой целью? Выберите все, что подходит.

   A. ASP.
   B. Java.
   C. XML.
   D. HTML.

3. Ответьте, "да" или "нет". CGI внедряет сценарий в Web-страницу, что позволяет использовать данный сценарий всем клиентам.

4. Какой язык разметки можно использовать для создания интерактивной формы?

   A. XML.
   B. DHTML.
   C. HTML.
   D. Все перечисленные языки.

5. Ответьте, "да" или "нет". JavaScript — это язык сценариев, разработанный фирмой Sun Microsystems.

Глава 14

Принципы управления сетями

В предыдущих разделах книги были рассмотрены компоненты, из которых состоит сеть — кабели, транспортные протоколы, компьютеры, операционные системы и приложения. Объединение всего этого не является самой сложной частью задачи организации сети. После установки и запуска сети следует ожидать иных трудноразрешимых проблем, связанных с поддержкой сети в ее нормальном состоянии. Пользователи часто настаивают на применении того, что обслуживается весьма хлопотно, и это тоже создает проблемы.

В логической последовательности со всем рассмотренным ранее в этой главе рассмотрим основные принципы управления сетями, включая несколько смежных вопросов.

- Что может произойти и где именно.
- Инструменты для наблюдения за сетевым трафиком и состоянием оборудования.
- Концепция средств нулевого администрирования (zero administration).
- Методы внесения изменений в сети, не приводящие к "восстанию" пользователей.
- Технические средства диагностики неисправностей.

Перечисленные вопросы — это большой объем информации, но идея, стоящая за концепциями управления, одна и та же: узнать, что у вас есть в наличии, и взять все под контроль. Если вы научитесь это делать, ваша работа значительно облегчится.

Источник знаний о сети – документация производителя

Первый шаг на пути к эффективному управлению сетью — получение разнообразной информации, начиная с инвентарных номеров плат, схемы компоновки всей сети и сведений о ее производительности. В гл. 4 было сказано о важности документирования параметров конфигурации плат расширения, установленных в ПК. Принцип документирования остается неизменным и на более высоких уровнях: каким иным образом вы сможете узнать, будут ли совместно работать различные сетевые компоненты, если вы не знаете точно, что они собой представляют? Следует целенаправленно собирать сведения об организации вашей сети, ее производительности и физических компонентах, и тогда при возникновении проблем вы будете лучше подготовлены к их разрешению.

Выполнение аудита

После того, как сеть установлена и начала нормально работать, не расслабляйтесь. Теперь самое время упорядочивать документацию. Познакомьтесь с вашей сетью поближе именно сейчас, пока все работает так, как надо. Это не слишком благодарная работа, и не всегда она кажется приятным времяпрепровождением, но окупается при возникновении неисправностей.

Примечание

Документация особенно необходима для аварийного восстановления (см. гл. 16).

Во-первых, если вы будете знать, что собой представляет сеть во время нормальной работы, вам будет легче обнаружить неисправность, когда она не работает. "Не работает" не обязательно из-за неисправностей в результате каких-то изменений в сети. Может быть, например, что часть сети работает, но с пониженной производительностью. Так будет продолжаться до тех пор, пока не будет определена и устранена причина.

Во-вторых, для поддержания работоспособности больших и протяженных сетей знание схемы физической компоновки вашей сети может быть весьма важным при установлении причины возникновения нарушений или при определении неисправной части сети.

Можно выделить две основные разновидности аудита локальных сетей: физический и нематериальный (intangible). Аудит имущества и оборудования чаще всего является физическим — используйте его для определения того, что имеется в наличии, и локализации местонахождения оборудования. Аудит производительности, эффективности и безопасности в большинстве случаев имеет нематериальную природу. Каков реальный уровень трафика локальной сети? Работает ли локальная сеть так эффективно, как это допускают ее возможности, или же следует перераспределить ее ресурсы с тем, чтобы требования пользователей были полностью удовлетворены? Какой уровень безопасности необходим для локальной сети и удовлетворяет ли она этим требованиям? В следующих разделах будет описано, что именно следует определять при проведении аудита локальной сети.

Физические аспекты организации сети

Самая легко выполнимая часть аудита сети заключается в инвентаризации оборудования: что имеется, и где оно находится. Такая работа может потребовать много времени, но она, в основном, исполняется неквалифицированным персоналом. По большей части эта работа состоит в составлении таблиц, содержащих описание компонентов вашего аппаратного и программного обеспечения без всякой связи со средой, в которую они установлены.

Проведение инвентаризации. Сначала точно определите, что у вас есть.

Соберите информацию о каждом компьютере.

- Тип оборудования и общее назначение (ПК, маршрутизатор, мост), название фирмы-изготовителя и номер модели.
- Серийный номер машины.
- Данные о пользователе машины.
- Информация о конфигурации машины, в том числе все имеющиеся у нее ресурсы, протоколы и подключенные устройства.

Проверьте установленное программное обеспечение.

- Типы операционных систем клиентных и серверных компьютеров, номера их версий, а также все инсталлированные на них вставки (patch) и исправления (fix).
- Установленные приложения и (если возможно) даты установки и версии.

Примечание

Какое значение имеет время установки приложений? Иногда ответ может быть ключом к определению причины некорректного функционирования приложения. Многие приложения Windows имеют предварительно созданные библиотеки данных или программ, называемые динамически подключаемые библиотеки, или DLL (Dynamic Link Libraries). Для работы большинства приложений достаточно одной DLL-библиотеки. Однако при этом могут возникнуть проблемы, особенно если DLL-файлы одного приложения будут заменены одноименными DLL-файлами другого с устаревшей информацией. Отслеживание дат создания и записи файлов при инсталляции поможет вам избежать или своевременно диагностировать

такие конфликты DLL.

- Кто имеет доступ к этим приложениям.
- Сколько существует лицензий для программного обеспечения.

Результаты инвентаризации оборудования могут быть поистине бесценными при анализе состояния компонентов компьютера, места их использования в сети, и их конфигурации. Инвентаризация программного обеспечения необходима не только для учета текущих версий, но также может помочь и при его лицензировании.

Проведение аудита оборудования. При проведении аудита оборудования сначала достаньте копию проекта вашего офиса и обойдите здание. На проекте следует отметить следующее.

- Места отводов кабелей и длину их прогонов.
- Места установки терминаторов, если это сеть Ethernet.
- Тип используемого кабеля в каждой части сети (например, в сети со звездообразной топологией используют кабель UTP категории 5 для соединений с настольными системами, но для магистральных соединений — оптоволоконный кабель).
- Сетевое оборудование (маршрутизаторы, мосты, коммутаторы и серверы).
- Цветовые или иные условные обозначения, примененные для идентификации прогонов кабеля.

Совет

Если вы еще не промаркировали прогоны кабелей, обязательно сделайте это во время аудита оборудования.

Сохраните копии проекта в сейфе, и в случае каких-либо изменений не забудьте обновить записи. Результаты аудита оборудования являются основой построения карты вашей сети (описываемой далее в этой главе в разделе "Создание карты сети").

Аудит оборудования — подходящий момент для ознакомления со всем зданием, а не только с сетью. Изучите месторасположение выключателей электропитания и водяных кранов, кондиционеров и нагревательных устройств, а также всего того, что может потенциально воздействовать на вашу сеть.

Нематериальные аспекты сети

Хотя и более субъективным (по сравнению с инвентаризацией средств физического уровня и аудита оборудования), но значительно более важным является аудит состояния сети (ее производительность и безопасность). На этом этапе аудита вы должны оценить эффективность функционирования и распределения сетевых ресурсов, определить степень безопасности и зафиксировать нормальную конфигурацию сети, чтобы можно было идентифицировать какие-либо отклонения от этой конфигурации.

Регистрация эффективности функционирования. Аудит функционирования — это учет всего, что может случиться в сети, но без каких бы то ни было катастрофических последствий. В процессе аудита следует зафиксировать:

- величину генерируемого сетевого трафика;
- сегменты, в которых сосредоточен этот трафик;
- изменение трафика и загрузки сервера в течение дня;
- наиболее перегруженные средства сервера;
- количество лицензий на приложения, используемые в каждый момент времени;

- источники сетевого трафика.

Даже если сеть работает хорошо, результаты аудита ее функционирования будут весьма ценными. Имея такую информацию легко идентифицировать изменения, которые могут привести к неисправности, или решить, где именно для улучшения работы сети предусмотреть новые ресурсы.

Определение сетевой эффективности. Аудит функционирования служит для контроля процессов, происходящих в сети. Аудит эффективности заключается в анализе полученной информации и определении эффективности работы сети. Этот аудит выполняется путем анализа результатов проверки операционной среды.

Задайте себе несколько вопросов.

- Равномерно ли загружена сеть, или же некоторые сегменты имеют небольшой трафик, в то время как другие перегружены?
- Можно ли маршрутизировать некоторую часть трафика иным образом с целью выравнивания нагрузки в сети?
- Насколько заняты серверы? Могут ли они удовлетворять требованиям пользователей все дневное время?

Сравните результаты аудита функционирования с аудитом эффективности, чтобы определить, как можно перераспределить сетевые ресурсы.

Определение установок системы защиты. Наконец, осталось только провести аудит системы защиты. Далее рассмотрим основные причины появления лазеек в системе защиты и способы их поиска, а здесь перечислим общие вопросы, на которые следует обратить внимание.

- Может ли каждый пользователь легко получить доступ к нужным ему ресурсам?
- Защищены ли ресурсы сети от пользователей, не имеющих к ним доступ как изнутри, так и извне компании, если ваша компания владеет внешней частью сети (extranet)?
- Какие меры предприняты для защиты от вирусов?
- Какие меры предприняты для защиты данных?

Для выполнения аудита системы защиты требуется объединить операции инвентаризации существующих систем и получения вводимой информации. Аудит системы защиты не только просто блокирует доступ пользователей к сети, но также и обеспечивает им гарантированный доступ к требуемым ресурсам. Определите, что именно на самом деле требуется пользователям для работы, и, если это практично и необходимо для дела, ослабьте защиту ресурсов, чтобы сделать их более доступными.

Хранение аудиторской информации

Получив всю упомянутую выше информацию, сохраните ее в одном (общем) месте.

По многим соображениям не рекомендуется делать записи на бумаге (исключая чертежи). Бумажные отчеты трудно обновлять, легко потерять или испортить, на них могут появиться неразборчивые надписи, сделанные вручную (а если они подготовлены на компьютере, то зачем нужно печатать все эти записи?), и они не всегда доступны. Единственный случай, когда полезно иметь твердую копию — во время планерок (planning meetings), на которых предполагается представить их руководству и подразделению, обслуживающему сеть.

Наилучшим местом хранения информации, по-видимому, являются базы данных. Они удобочитаемы, их легко обновлять, в них предусмотрены средства для проведения поиска, они всегда находятся под рукой и содержат достоверную информацию (пока вы регулярно их об-

новляете).

С этой целью можно приобрести какую-либо имеющуюся на рынке аудиторскую базу данных. Однако нетрудно и самому создать внутрифирменную аудиторскую базу данных, которая, скорее всего, больше вас устроит, поскольку вы сами ее разработаете. Для облегчения ввода информации можно даже создать формы для внешнего интерфейса с соответствующими таблицами данных. Если вы никогда не создавали приложение для ввода данных, то познакомьтесь с этим процессом.

1. Идентифицируйте главную тему каждой таблицы (например, аудиты инвентарных принадлежностей, оборудования, функционирования, и т.д.) и создайте таблицу.
2. Идентифицируйте категории данных, заносимых в каждую таблицу (тип устройства, серийный номер, число пакетов, посылаемых в час, даты установки и т.д.) и создайте соответствующие поля.
3. Создайте средства внешнего интерфейса с каждой таблицей, предусмотрев позиции для ввода пользовательских данных.

Совет

Для полей, имеющих заранее определенное множество допустимых значений, можно создать поля со списками выбранных пользователем пунктов. Это поможет предотвратить внесение в данные грамматических ошибок, которые могут помешать проведению поиска.

Создайте все это, и тогда при открытии базы данных вы сможете выбрать одну из таблиц в отображаемом списке (рис. 14.1).

Откройте таблицу, для которой вы создали форму, и вы увидите нечто, напоминающее форму, показанную на рис. 14.2.

Создание базы данных может показаться сложным делом, но это не так, и вполне доступно тем, кто этим не занимался ранее. Наиболее сложной частью такой работы является идентификация информации, вводимой в базу. После того как вы это сделаете, создание таблиц и форм в основном будет заключаться во вводе с клавиатуры имен полей и рисовании элементов внешнего интерфейса, удобных для восприятия. Конечно, чтобы создать базу данных соответствующего формата, может потребоваться некоторое время. Однако если это сделать, вы получите приложение, с помощью которого можно легко хранить и обновлять данные (и результаты) аудита, а также базу данных, позволяющую создавать отчеты в любое нужное время.

Создание карты сети

Часть данных по аудиту можно не только записывать в базу данных, но и хранить в форме карты, позволяющей легко определить связь частей сети друг с другом. Карта может быть выполнена в виде твердой копии или храниться в электронном виде и содержать описание сети на физическом уровне вместе с ее логической организацией.

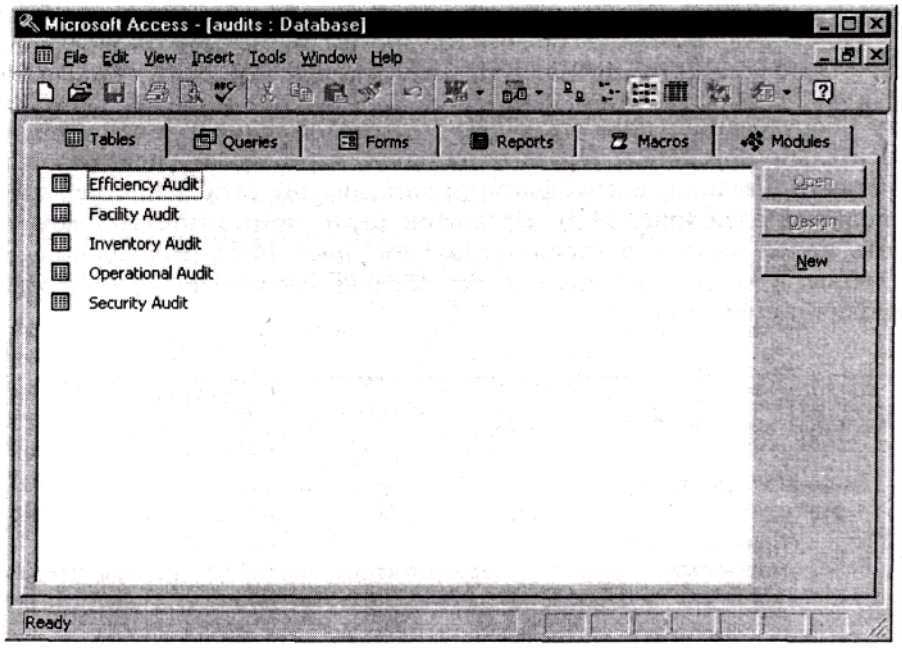


Рис. 14.1. База данных содержит одну или несколько таблиц, каждая из которых посвящена определенной теме

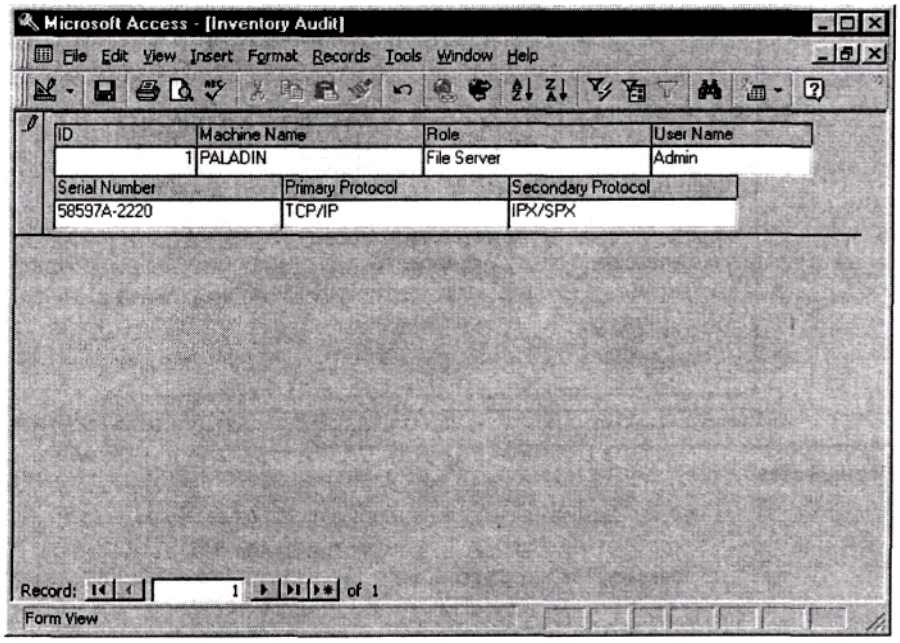


Рис. 14.2. База данных аудита инвентарных принадлежностей, созданная с помощью Access 97

Представление сети на физическом уровне

Фактически можно иметь несколько физических карт вашей сети в зависимости от ее размера и сложности. Физическая карта напоминает карту оборудования, показывающую местонахождение компонентов сети относительно друг друга. Поэтому на одной карте можно показать размещение сети в здании, идентифицируя каждый узел сети, например именами пользователей (рис. 14.3). На другой карте можно показать всю сеть, вплоть до ее выхода в глобальную сеть (рис. 14.4). Назначение карт различное: к каждой из них следует обращаться

для получения ответов на различные вопросы.

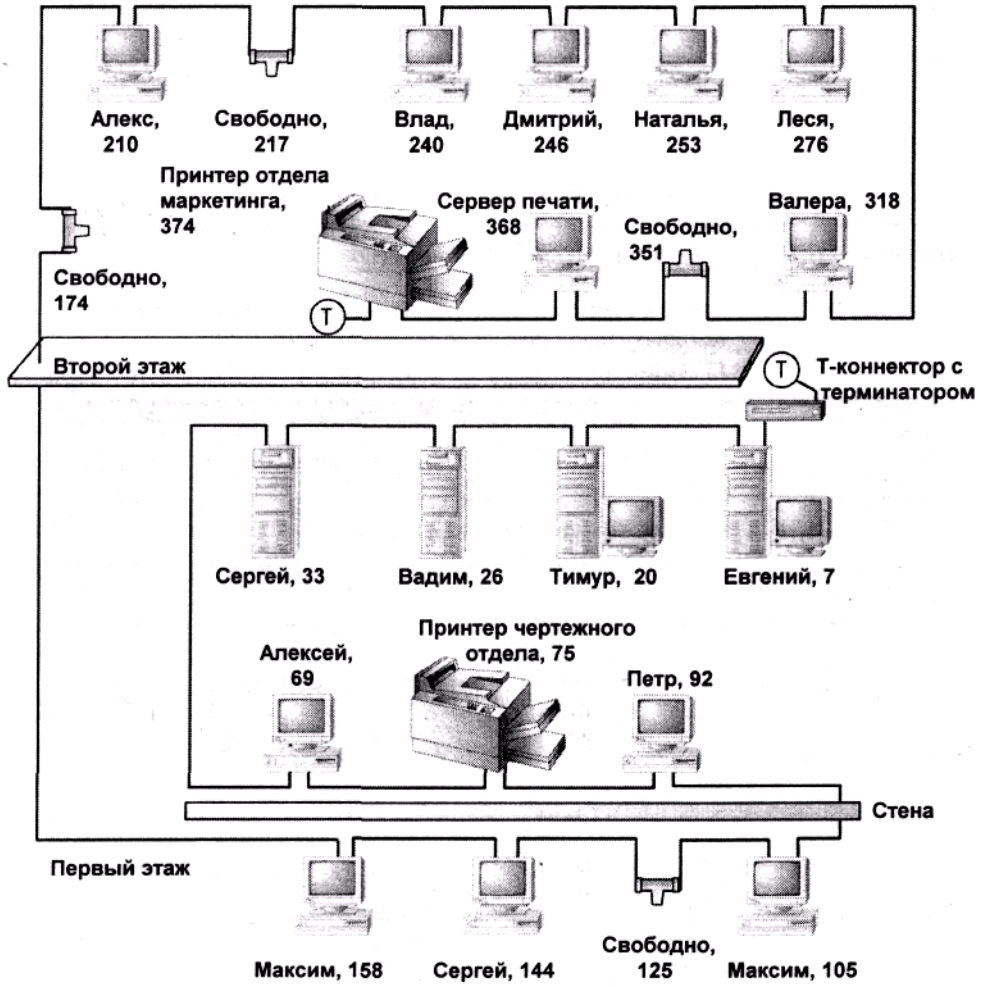


Рис. 14.3. Пример физической карты сети для двухэтажного здания

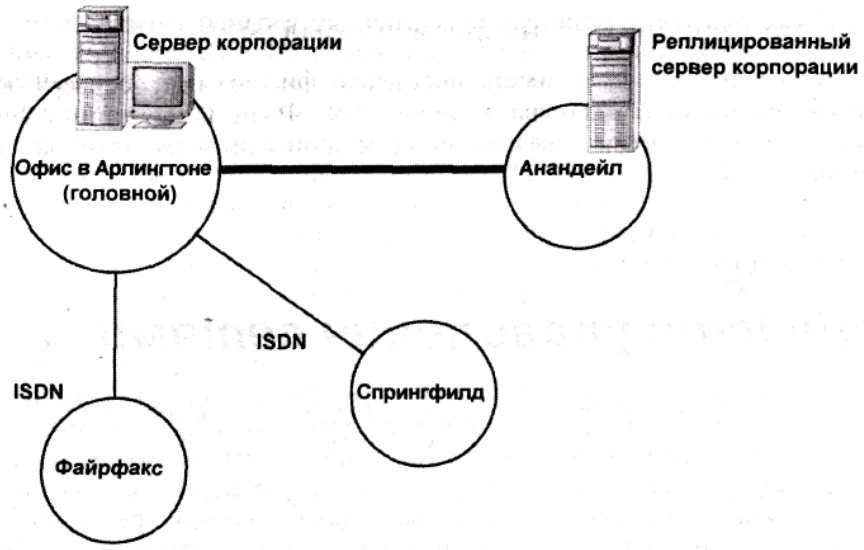


Рис. 14.4. Пример физической карты сети предприятия

Логическая схема сети

Физическая карта сети показывает размещение компонентов относительно друг друга. В отличие от нее логическая карта сети (logical network tap) показывает организацию сетевых ресурсов (рис. 14.5). Какие клиенты и к каким серверам имеют доступ? Какую информацию содержат те или иные серверы или группа серверов? Какие репликации выполняются в сети? Ответы на эти вопросы могут быть на физической карте, хотя и не всегда.

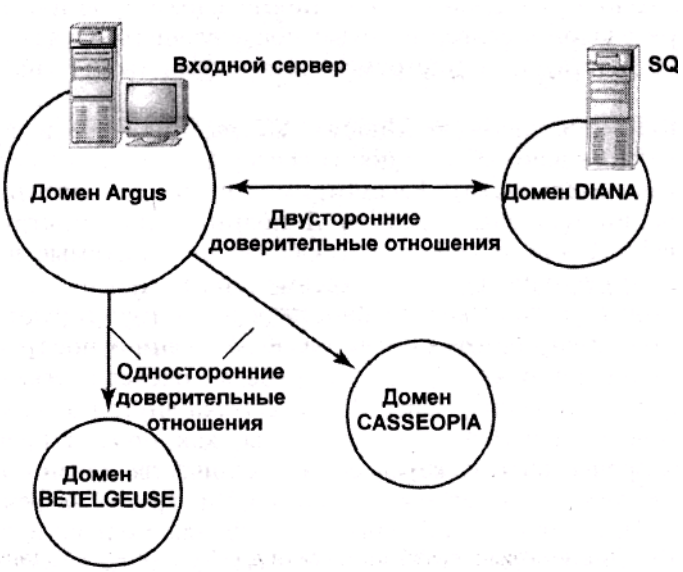


Рис. 14.5. Логическая карта структурной организации сети

И все же для демонстрации различных уровней сети во всех деталях может потребоваться несколько различных карт. Например, необходимо узнать, какие клиенты подключились к конкретному серверу входной аутентификации (authentication server) или какие базы данных реплицируются посредствами глобальной сети для контроля потоков сетевого трафика.

Обзор средств управления сетями

Теперь вы представляете, какую информацию о сети необходимо иметь под рукой. Однако вы не сможете получить всю нужную информацию, просто прогулявшись по зданию. Такой обход сети может оказаться физически невозможен, и в любом случае не вся информация выявляется так просто. Читайте дальше, и вы узнаете больше о тех средствах, которые можно использовать для сбора информации о вашей сети, чтобы далее заставить ее делать именно то, что вам нужно.

Средства для контроля работы сервера

Одним из ключевых условий успешной работы сети является производительная работа сервера. Если сервер не соответствует предъявляемым к нему требованиям, то даже при достаточной полосе пропускания соединительных линий производительность сети не будет высокой. Для отслеживания работы компонентов сервера и поступающих на него запросов, а также для наблюдения за текущими значениями параметров или регистрацией результатов

входов в сервер с целью последующего изучения можно использовать соответствующее инструментальное средство для наблюдения за сервером.

При использовании системы Windows NT вы получите в ее составе один из инструментов для наблюдения за сервером — Performance Monitor (Монитор производительности). Рассмотрим этот инструмент в качестве примера реализации подобных средств. Дополнительные инструментальные средства наблюдения за сервером (включая используемые в Windows NT) устроены если не точно так же, то весьма схоже.

На экране монитора производительности ресурсы группируются в виде объектов и счетчиков внутри этих объектов. К объектам относятся ресурсы основных категорий, таких как процессор, рабочие очереди сервера, физические диски, файл подкачки (paging file). Счетчики внутри этих категорий контролируют такие специфические величины, как номера прерываний, обрабатываемых процессором каждую секунду, количество клиентов, запросы которых были обслужены отдельным процессором, время, затраченное на чтение с диска, или процент используемого файла подкачки в данный момент времени. Некоторые счетчики подразделяются на копии (instance). Например, один из счетчиков для объекта Process (Процесс) измеряет процессорное время, отведенное каждому исполняемому процессу на выбранном компьютере. У этого счетчика имеются копии — это значит, что можно наблюдать или за суммарной процентной долей полного процессорного времени, используемого всеми процессами, или выбрать для наблюдения отдельные процессы.

Для организации наблюдения за системой с помощью монитора производительности следует выбрать наблюдаемый компьютер, найти интересующий объект и выбрать счетчик (или счетчики). Щелкните на кнопке Add (Добавить) и добавьте линию, с помощью которой на диаграмме будет отображаться выбранный счетчик. Как показано на рис. 14.6 линия каждого счетчика будет иметь отличающийся от других цвет, так что вы сможете без труда за ней проследить.

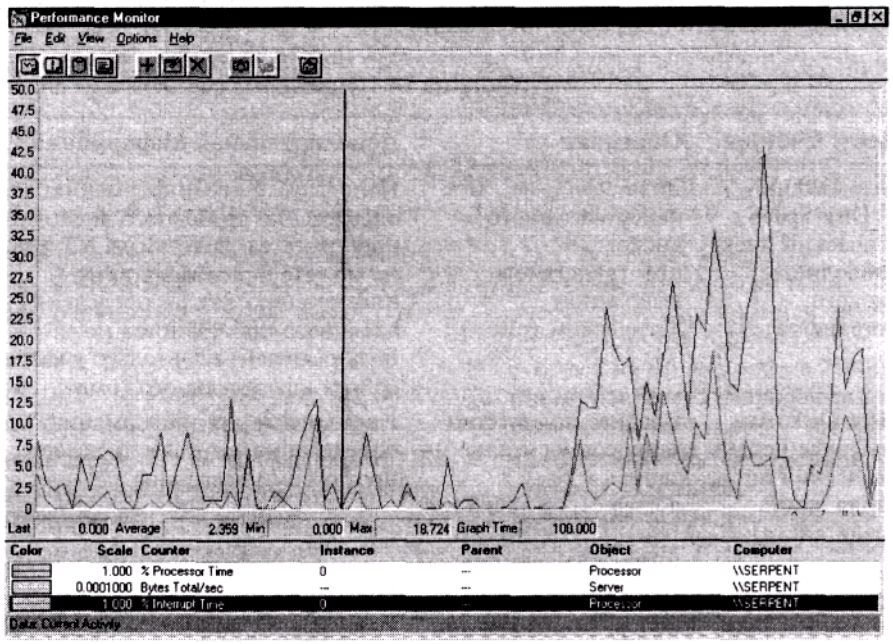


Рис. 14.6. Используйте монитор производительности Windows NT для построения диаграммы запросов к серверным ресурсам

Наблюдайте за производительностью сервера дистанционно, если это возможно. В противном случае монитор сам станет использовать ресурсы сервера, что приведет к искажению результатов, поскольку некоторая часть памяти и циклов процессора будет выделена для поддержки монитора.

Совет

Если вы должны запускать монитор производительности на наблюдаемом сервере, то обязательно следите за копией PERFMON счетчика Processor Time (Процессорное время) объекта Process. Это даст вам, по крайней мере, некоторое представление относительно того, как много процессорного времени выделяется монитору производительности.

Чтение выводимых монитором данных не вызывает затруднений. Трудности могут возникнуть в понимании скрытого смысла читаемой информации. Следует знать, как именно осуществляется взаимодействие различных частей сервера и какое оборудование задействовано для поддержки различных запросов к серверу. Как минимум, следует ознакомиться с описанием серверов, приведенных в гл. 8. Чтобы узнать о работе сервера как можно больше, следует иметь некоторое представление об архитектуре серверов. Вы не получите никакой полезной информации, наблюдая за ростом значения счетчика Threads (Потоки), если не будете знать, что такое поток, почему число потоков может расти и что означает такое поведение счетчика. Эта глава не может научить вас всему тому, что связано с наблюдением за сервером, но в табл. 14.1 описаны несколько основных счетчиков. Используя знания функций сервера, вы сможете идентифицировать и осмыслить показания других счетчиков.

Таблица 14.1. Некоторые счетчики и их описание

Объект: Счетчик	Описание	Дополнительная информация
Logical Disk: % Free Disk Space (Логический диск: % свободного дискового пространства)	Доля неиспользуемого дискового пространства на выбранном логическом томе	Используйте эту информацию для определения свободного дискового пространства. В Windows NT 4 вы не можете использовать эту информацию для распределения дискового пространства по пользователям, если только у каждого из них нет отдельного тома
Logical Disk: Avg Disk Queue Length (Логический диск: средняя длина очереди диска)	Среднее количество запросов на чтение и запись к тому логического диска в течение указанного интервала времени	Используйте эту информацию для определения загрузки диска на протяжении всего дня
Memory: % Committed Byte in Use (Память: % использования выделенных байтов)	Доля памяти, используемой тем или иным процессом в сравнении с той, что могла бы быть использована	Показывает процентную долю виртуальной памяти, используемой в определенный момент времени
Memory: Page Faults/Sec (Память: Ошибки страницы/С)	Частота обращения к данным в файле подкачки на диске вместо обращений к оперативной памяти	Некоторое количество ошибочных страниц предусматривается заранее, но большое количество означает недостаточный размер виртуальной памяти по сравнению с предъявляемыми запросами
Physical Disk: Avg Disk Queue Length (Физический диск: Средняя длина очереди диска)	Среднее количество запросов на чтение и запись к физическому диску в течение заданного интервала времени	Используйте эту информацию для определения нагрузки на диск в течение дня. В зависимости от этой информации вам может потребоваться возложить часть нагрузки на более быстрый диск
Physical Disk: Disk Transfer/sec (Физический диск: среднее время обращения, с)	Скорость чтения и записи данных на отдельный физический диск	Показывает скорость ответов выбранного диска на запросы пользователя
Processor: % Processor Time (Процессор: % нагрузки)	Показатель того, как часто процессор занят полезной работой, а не находится в простое	Показывает степень загрузки процессора. Загруженность процессора не обязательно означает нечто плохое, а отслеживание степени загрузки позволяет предотвратить появление "узких мест"
Server: Bytes Total/sec (Сервер: Всего байтов/с)	Количество байтов, передаваемых и получаемых каждую секунду	С его помощью можно проанализировать количество операций чтения и записи, чтобы посмотреть, как быстро сервер отвечает на запрос определенного типа и как много запросов данного типа поступает

Окончание табл. 14.1

Объект: Счётчик	Описание	Дополнительная информация
Server: Errors Logon (Сервер: Ошибки входа)	Неудавшиеся попытки входа на сервер	Высокое количество может означать попытку получения несанкционированного доступа путем угадывания пароля или с помощью специальных программ для его подбора
Server: File Directory Searches (Сервер: Число поисков каталога с файлом)	Количество процедур поиска файла, выполненных за выбранный интервал времени	Эта величина характеризует занятость сервера
Server Work Queues: Queue Length (Рабочие очереди сервера)	Текущее количество запросов, ожидающих получения процессорного времени. Если в системе установлено несколько процессоров, этот счетчик работает отдельно для каждого из них	Более четырех ожидающих запросов в каждый заданный момент времени может означать перегрузку процессора

Вам может потребоваться и другая информация, причем в достаточно большом объеме, средства получения которой не предусмотрены в мониторе производительности. Но приведенные сведения позволят вам почувствовать, какого типа информацию вы можете получить с помощью средств наблюдения за сервером.

В определенной степени тип информации, которая может представлять для вас наибольший интерес, зависит от роли отслеживаемого вами сервера. Например, наблюдение за дисковым пространством на файловом сервере будет более полезным, нежели контроль сервера приложений, а количество обслуженных CGI-запросов имеет значение только для Web-сервера. Однако некоторые ресурсы важны для серверов любых типов — циклы процессора, объекты, использующие память, полезная доля оперативной памяти или файла подкачки, а также количество запросов в очереди — все это примеры таких ресурсов.

В принципе, вы можете использовать столько счетчиков и в таком количестве объектов, сколько пожелаете. Однако поскольку с помощью инструментов наблюдения за сервером можно собрать очень большой объем данных, лучше всего сконцентрироваться на получении именно тех данных, которые важны для вас в текущий момент времени. Особенно важно сфокусировать свое внимание во время сбора информации. Сколько запросов в секунду обрабатывает ваш сервер в каждый данный момент рабочего дня? Как этот показатель изменяется на протяжении дня или месяца? Определите нормальные значения параметров и запишите их, чтобы при отклонениях вы могли идентифицировать изменения и обнаружить их источник.

Сетевые мониторы

В своей работе вы обязательно будете использовать программные средства, использующие протоколы управления сетью, для сбора информации о сети и иногда для отправки команд удаленным компьютерам. Это не просто средства пассивного наблюдения. Они могут быть использованы для уведомления ответственного лица о возникновении проблемы.

Сетевые мониторы состоят из двух частей: клиентной, расположенной на наблюдаемом устройстве, и серверной, расположенной на устройстве, выполняющем наблюдение и запись собранной информации. Взаимодействие клиентной и серверной частей зависит от протокола наблюдения. Несмотря на это, все программное обеспечение для наблюдения за сетью спро-

ектировано с одной целью — сбора информации о сети. Для выполнения такой работы может потребоваться:

- транспортный протокол сбора статистической информации;
- идентификация узлов сети;
- сбор данных о конфигурации программного обеспечения и оборудования;
- сбор статистической информации о производительности и загруженности каждого сервера Internet (host);
- запись статистической информации об использовании приложений;
- запись сообщений о событиях и ошибках.

Содержание собираемой информации зависит от элементов, за состоянием которых можно наблюдать и обслуживать отдельными программными продуктами для наблюдения/управления сетью. Каждый сервер Internet (host), допускающий управление такого типа, для каждого наблюдаемого элемента имеет текстовый файл, называемый административной базой данных (MIB — Management Information Base). Файл MIB содержит следующую информацию.

- Список наблюдаемых объектов.
- Синтаксис наблюдаемых объектов.
- Предоставляемый для наблюдения доступ (только для чтения, или же для чтения/записи).
- Статус (обязательный или нет) объектов.
- Описание объекта.

Короче, файл MIB содержит список наблюдаемых объектов системы и их характеристики. Комплект средств Windows NT Resource Kit содержит файл MIB (ведущий свою родословную от списка адресов SNMP), называемый TOASTER.MIB, который иллюстрирует синтаксис. Ниже приведен один из объектов файла MIB.

```
toasterDoneness OBJECT-TYPE
          SYNTAX INTEGER   (1..10)
          ACCESS read-write
          STATUS mandatory
          DESCRIPTION
                  "This variable controls how well done ensuring toast should
                  be on a scale of 1 to 10. Toast made at 10 is generally
                  considered unfit for human consumption; toast made at 1 is
                  lightly warmed.(Этот параметр указывает,  насколько хорошо
                  был сделан тост,  его значение лежит в диапазоне от 1 до 10.
                  Тост,  сделанный при параметре 10,  обычно считается не-
                  пригодным для употребления; 1 означает лишь легкий подогрев)
                  " := {toaster 4}
```

Таким образом, значение, ассоциированное с объектом toasterDoneness, указывает, насколько хорошо был приготовлен тост. Монитор может также оценить, попадает ли это значение в некоторый интервал (скажем, между 3 и 7 для хорошо сделанного тоста) и выдает предупреждение сетевому администратору при выходе величины за допустимые границы. Значение в скобках внизу ({toaster 4}) — номер объекта. Таким образом, toasterDoneness является четвертым типом объектов, определенным в файле MIB.

Примечание

Этот пример соответствует стандарту, называемому MIB-II. Для того чтобы за устройством можно было наблюдать или управлять им с помощью последней версии SNMP-списка, оно должно использовать этот формат для своих файлов MIB.

Для применения наиболее популярного метода сбора данных (когда вам требуется ин-

формация сразу о нескольких управляемых объектах), вы можете запросить ее у сетевого монитора. Монитор, в свою очередь, запрашивает информацию у сервера Internet (host), используя при этом имя объекта. Сервер производит поиск имени, определяет связанное с ним значение и возвращает монитору отчет.

Не все протоколы средств наблюдения за сетью используют одинаковые файлы MIB и даже не все протоколы одного типа работают с одинаковыми файлами MIB. Для того чтобы средство наблюдения соответствовало стандартному протоколу, при разработке средства следует придерживаться руководящих принципов сбора данных, указанных в стандарте протокола. Если в программном продукте для наблюдения используется, как минимум, один определенный MIB, то он должен быть согласован со стандартом. С практической точки зрения это значит, например, что не все использующие SNMP-список сетевые мониторы созданы одинаковыми (равными). Требуется тщательно проверять, какую именно информацию позволяет собирать тот или иной программный продукт.

Простой протокол сетевого управления (SNMP)

Простой протокол сетевого управления (SNMP — Simple Network Management Protocol) является примером события, часто встречающегося в мире сетей: появившееся как временная "затычка" средство становится стандартным, поскольку предназначенная ему на замену усовершенствованная технология несколько опоздала к тому времени, когда это средство стало доступным. Изначально протокол SNMP был спроектирован как простой, облегченный метод наблюдения за интрасетями, в которых используется протокол TCP/IP. Более совершенный протокол *CMIP (Common Management Information Protocol — общий протокол передачи управляющей информации)*, соответствующий модели OSI, предназначался в качестве замены SNMP, но этого так и не произошло по двум причинам. Первая: CMIP и в самом деле более мощный протокол, чем SNMP, и позволяет собирать информацию, которую SNMP собрать не может. Но такое расширение возможностей привело к недопустимой перегрузке ресурсов сети и сервера. Вторая: к тому времени, когда протокол CMIP стал пригодным для использования, протокол SNMP настолько широко распространился, что стоимость его замены стала превышать выгоду от применения протокола CMIP. Таким образом, SNMP стал самым распространенным стандартным протоколом для инструментов сетевого управления.

Протокол CMIP - претендент № 2

В гл. 6 была упомянута технология SMDS, служащая примером мощной технологии, вытесненной менее мощной Frame Relay, изначально предназначавшейся для временного заполнения определенной ниши до окончания разработки SMDS, Это довольно обычная история — то же самое случилось и со CMIP-протоколом.

Протокол CMIP задумывался как более мощное средство, призванное заменить протокол SNMP. CMIP поддерживает функции, которые в SNMP отсутствуют; он может работать на любой платформе (версия для взаимодействия только с TCP/IP называется CMOT). Он может предоставить такие средства управления, которые отсутствуют в SNMP. В сущности, он работает совершенно иначе, чем SNMP. Вместо опроса устройств для определения их статуса или получения о них какой-либо информации, CMIP ждет, пока устройства сами не предоставят отчеты диспетчеру CMIP.

По иронии судьбы, причиной отказа от CMIP стала его мощность. Он требует больше серверных ресурсов, чем может позволить большинство сетей. В конце 90-х гг. — все это уже история. По поводу протокола CMIP публикуется многообещающая информация: "Если CMIP поступит в коммерческое пользование, он будет- иметь огромное число заказчиков, поскольку над его разработкой продолжают работать все учебные институты". Однако кажется маловероятным, что CMIP сможет вскоре заменить SNMP. Протокол SNMP широко распространен и

пользуется признанием, чтобы его в данный момент можно было легко заменить, и хотя он не такой мощный, как CMIP, зато не так требователен к ресурсам.

Как работает протокол SNMP. При работе протокола SNMP используют файлы MIB подобно тому, как при переписи населения — опрос. Через регулярные промежутки времени (или по сигналу запроса) серверная часть SNMP запрашивает у устройства информацию о его статусе, используя данные из MIB-файла устройства. Когда агент получает такой запрос, он возвращает требуемые значения. Между клиентной и серверной частями монитора информация перемещается с помощью протокола UDP (User Datagram Protocol — протокол пользовательских дейтаграмм), являющегося компонентой транспортного уровня протокола TCP/IP. UDP — протокол без соединения (точнее без подтверждения). Это значит, что он позволяет передавать сообщения, не заботясь об их приеме, и поэтому не вносит большого вклада в сетевой трафик. Конечно, протокол SNMP или какое-либо другое средство наблюдения за сетью увеличивают сетевой трафик, но все они спроектированы так, чтобы это воздействие было минимальным. Устройства для наблюдения за сетью, которые требуют большого сетевого трафика (и, следовательно, "несут ответственность" за большую часть трафика), не особенно полезны.

Примечание

Хотя существует стандарт, регламентирующий применение SNMP в сетях с протоколом IPX/SPX (в котором для передачи сообщений применяется протокол IPX вместо UDP), но гораздо более вероятно, что вы столкнетесь с протоколом SNMP в сетях TCP/IP. Не все версии протокола SNMP поддерживают передачу сообщений посредством IPX-протокола.

Вспомните, что протоколы наблюдения за сетями содержат два компонента: диспетчер, расположенный на сервере, и агент — на управляемом устройстве (рис. 14.7). В этом простом примере диспетчер запрашивает у агента (возможно, исполняемого на файловом сервере) информацию о количестве поддерживаемых им соединений. Получив этот запрос, агент отыскивает на FTP-сервере данные и передает их диспетчеру.

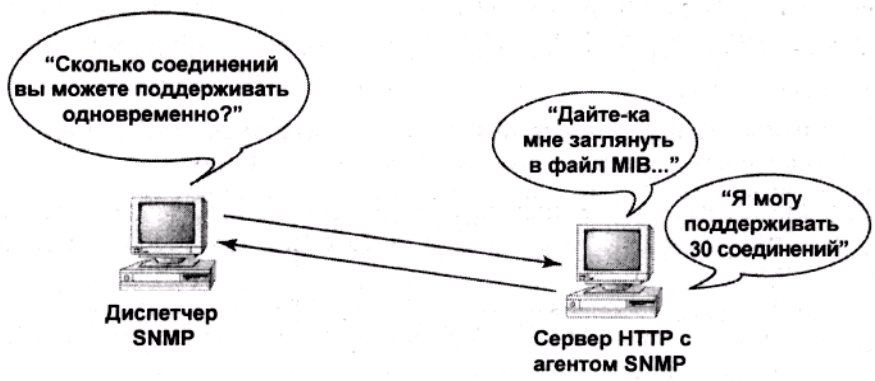


Рис. 14.7. Сетевое взаимодействие по протоколу SNMP между диспетчером и агентом

Не в каждом устройстве сети имеется агент SNMP. Он есть только в тех, за которыми необходимо наблюдать, и сконфигурированных для поддержки SNMP. Поддерживающие протокол SNMP устройства, например, маршрутизаторы или мосты, всегда снабжены агентами SNMP, но если вы хотите наблюдать за компьютером определенного (возможно, нестандартного) типа, вам следует самому установить агента. В NT это делается путем запуска средств SNMP как на наблюдаемом устройстве, так и на диспетчерском компьютере.

По умолчанию (и согласно рекомендациям стандарта) агенты SNMP конфигурируются следующим образом: для приема сообщений назначается порт 161, для пакетов перехода (traps)

- порт 162. Если вам требуется установить на отдельном компьютере несколько агентов SNMP, вы можете изменить назначенный порт. В NT, например, информация о назначенных портах хранится в файле SERVICES (файл без расширения; но вы можете открыть этот файл с помощью редактора Notepad), который находится в папке System32\Drivers\Etc. Поищите там, например, такие записи:

```
snmp        161/udp     snmp
snmp-trap   162/udp     snmp
```

Первый столбец описывает средство обслуживания, для которого предназначен порт, второй — задает номер порта, третий — указывает протокол для передачи информации, четвертый — определяет псевдоним указанного средства.

Предупреждение

Это средство не имеет "защиты от дурака". Редактируйте файл SERVICE (или иным образом изменяйте конфигурацию какого-либо другого порта), только если вы абсолютно уверены в том, что вы делаете, и твердо знаете, что не измените установки других портов устройства.

Агент SNMP ждет дейтаграммы от диспетчера SNMP с запросом информации. Когда агент получает такое сообщение, то выполняет одну из указанных ниже операций:

`get` — отыскивает указанный параметр управляемого объекта;

`get next` — отыскивает следующий параметр в файле MIB;

`set` — изменяет параметр управляемого объекта, пользуясь привилегией на чтение/запись.

Когда диспетчер SNMP получает от агента данные, он может либо просто отобразить их, либо сохранить в базе данных для дальнейшего использования.

Операции `get` и `set` выполняют только в ответ на запрос от диспетчера SNMP. Без запроса агент SNMP посылает сообщение только в двух случаях: когда узел останавливается или запускается, или когда значения некоторых контролируемых параметров выходят за пределы допуска и требуется передать сигнал тревоги. Эти сообщения называют *пакетами переходов (traps)*. Они отправляются по IP- и IPX-адресам или по адресу сервера Internet (host), указанному вами во время установки средств обслуживания SNMP на данном компьютере.

Сетевое взаимодействие по протоколу SNMP. Система защиты SNMP-протокола базируется на концепции среды (communities), представляющей собой логическую структуру SNMP-машин, объединенных под общим именем, аналогично рабочей группе. Подобно рабочей группе, члены среды часто физически расположены близко друг от друга, но это не обязательное условие. По сути дела, имя среды — пароль и должно трактоваться только таким образом.

Лишь те агенты и диспетчеры, которые входят в одну среду, могут общаться друг с другом. Когда монитор посылает агенту сообщение с запросом на получение информации, имя среды является составной частью сообщения. Когда он принимает сообщение, то проверяет корректность полученного имени среды. В случае несовпадения агент отбрасывает сообщение и, при необходимости, может зарегистрировать факт неудавшейся аутентификации. Только в случае, если агент и диспетчер используют одинаковое имя среды, сообщение будет обрабатываться.

По умолчанию все серверы NT, поддерживающие SNMP-протокол, изначально являются частью открытой (public) среды. Для дополнительной безопасности вы можете удалить имя среды или создать другую среду. Машина SNMP — агент или диспетчер — может быть членом одновременно нескольких сред. Если диспетчер SNMP не входит в состав ни одной

среды, он уподобляется устройству, не имеющему защитного пароля, и любой клиент SNMP может взаимодействовать с диспетчером независимо от того, членом какой именно среды является клиент.

Удаленное наблюдение (RMON)

На протяжении всей истории сетей, помимо средств наблюдения за сетью, предоставляемых протоколом SNMP, применялись также и аппа-ратно реализованные устройства удаленного наблюдения, например, сетевые мониторы и сетевые зонды (probe). Обычно (но не всегда) эти устройства представляют собой автономные инструментальные средства для решения задачи сбора сетевых данных, и они должны быть установлены в каждом сегменте маршрутизированной сети.

RMON (Remote Monitoring — удаленное наблюдение) — средство работы с оборудованием, предназначенным для выполнения сложных функций управления сетью. RMON — это протокол для сбора информации обо всей сети из единственного узла, применение которого позволяет отказаться от услуг специалиста, непосредственно наблюдающего за объектом, который подозревается в неисправности, и анализирует сетевые данные. Вместо этого центрального узла можно активировать удаленный монитор и поручить ему направлять информацию об определенном сегменте на центральную консоль. Единственное ограничение здесь то же самое, что и в случае применения протокола SNMP: наблюдаемое устройство должно иметь установленный агент RMON.

Хотя в обоих протоколах RMON и SNMP используются файлы MIB, это вовсе не одна и та же вещь. Оба они — средства управления сетями, но RMON обеспечивает поддержку расширенного набора файлов MIB, позволяющих собирать больше информации, чем SNMP. Основная функция SNMP заключается в получении подтверждения о том, что все части сети работают нормально. RMON предназначен для большего — он фактически является сетевым анализатором, используемым для измерения трафика данных в определенном сегменте локальной сети с целью определения его структуры и причины появления сколько-нибудь существенных узких мест. В определенных случаях RMON может использоваться не только для чтения данных, но и для записи, в зависимости от того, имеет ли какой-либо смысл задание значений параметров отдельного объекта. Как и при использовании протокола SNMP вам не следует наблюдать за процессом сбора данных в реальном масштабе времени. Инструментальные средства RMON позволяют подавать сигнал тревоги при выходе значений некоторых параметров за предварительно установленные допустимые границы или записывать данные в специальный журнал для последующего просмотра.

Первая версия протокола RMON позволяла собирать информацию только на канальном уровне. Но в версии RMON2, стандартизованной в июне 1997 г., предусмотрен сбор информации уже на сетевом уровне, вплоть до уровня портов, если это необходимо. RMON2 также поддерживает работу с некоторыми (специфическими для глобальных сетей) типами данных и позволяет идентифицировать ситуации, возникшие из-за каких-либо проблем на сетевом уровне, например, обрыва кабеля. RMON не фиксирует ошибки в пакетах на канальном уровне, поскольку данные из MIB-файла позволяют идентифицировать их только путем "разборки" кадра и его последующего чтения. Если на канальном уровне имеются ошибки, объем получаемой полезной информации будет относительно невелик. Однако на сетевом и вышележащих уровнях RMON может идентифицировать ошибки протокола и сообщать о них.

Данные, собираемые с помощью RMON, могут быть получены от одного из следующих источников.

Каталог протокола. Список имеющихся протоколов, которые удаленный монитор в состоянии отслеживать.

Распространенность протокола. Процентная доля пакетов, созданных в сегменте с помощью каждого из протоколов.

Установление соответствия адресов. Списки установленного соответствия адресов канального уровня адресам сетевого вместе с информацией о том, где это соответствие отслеживалось в последний раз.

Сервер Internet (host) сетевого уровня. Управляет величиной трафика между каждой парой сетевых адресов, определенных с помощью зонда (probe).

Матрица сетевого уровня. Подсчитывает величину трафика между каждой парой сетевых адресов, определенных с помощью исследования.

Сервер Internet (host) прикладного уровня. Управляет величиной трафика между каждой парой сетевых адресов, определенных с помощью исследования, распределяя результаты в соответствии с протоколом.

Матрица прикладного уровня. Подсчитывает величину трафика между каждой парой сетевых адресов, определенных с помощью исследования, распределяя результаты в соответствии с протоколом.

Примечание

"Прикладной уровень" в стандарте RMON не обязательно относится к протоколу, функционирующему на 7-м уровне модели OSI. Это может быть любой протокол, функционирующий на уровнях выше сетевого. Поэтому он включает протоколы транспортного, сеансового, представления данных или прикладного уровней.

Предыстория пользователя. Собирает данные по каждому пользователю сети.

Конфигурация зонда. Управляет способом, с помощью которого средства удаленного наблюдения могут быть запрограммированы с главной консоли.

Совместимые с RMON устройства не обязаны поддерживать обработку всех этих категорий данных, но если уж они поддерживают какую-либо категорию, то должны делать это полностью. Совместимое с RMON устройство может и не предоставлять некоторую часть информации о сервере Internet (host) на сетевом уровне из всего определенного в стандарте набора. К тому же некоторые группы зависят от других групп. Также совместимые с RMON устройства не могут использовать файлы MIB, связанные с матрицей прикладного уровня, если они не применяют матрицу сетевого уровня. Вы не сможете подсчитать трафик между узлами в соответствии с протоколом, если не в состоянии подсчитать трафик между узлами, независимо от транспортного протокола.

RMON важен не только потому, что позволяет собирать разнообразные данные, но также и потому, что обеспечивает непрерывный процесс сбора данных, независимо от того, функционирует ли в данный момент времени соединение между средствами удаленного наблюдения и главной консолью. Такой непрерывный поток собираемых данных поддерживает систему в состоянии, максимально соответствующем текущему моменту.

Например, вы не можете гарантировать, что удаленно управляемое устройство будет всегда соединено с главной консолью наблюдения. В случае прерывания такого соединения как по причине сбоя, так и вследствие запланированного отключения (что особенно вероятно, если монитор и главная консоль отделены друг от друга глобальной сетью WAN), будет наблюдаться разрыв связи между главной консолью и наблюдаемым устройством. Но использование файлов MIB для сбора данных означает, что удаленная система может быть сконфигурирована для сбора своих данных даже в случае, если она не находится в данный момент в контакте с главной консолью.

Примечание

Поскольку состояние сети можно отслеживать из разных мест, RMON поддерживает средства передачи данных на несколько консолей.

Протокол RMON можно использовать для осуществления непрерывной диагностики неисправностей, сбора информации, не отслеживаемой в данный момент, с целью ее последующего использования. Даже если сеть начинает отказывать, удаленный монитор будет записывать все параметры состояния системы, которые привели к возникновению проблемы — вплоть до момента полного прекращения работы сети. Когда появится такая возможность, с главной консоли можно будет просмотреть эту информацию для идентификации условий, приведших к сбою в работе сети. Поддерживающие RMON устройства могут также быть запрограммированы для записи определенных параметров системы. Устройства будут постоянно собирать информацию. Когда значения записываемых данных превысят заданные границы, монитор может распознать проблему и уведомить об этом главную консоль. Все эти данные весьма полезны, поскольку облегчают работу сетевого администратора. Чем больше данных вы можете получить, тем легче будет изолировать проблему в случае, когда сервер Internet (host), генерирующий большее число ошибок трафика, чем какой-либо другой сервер, пришлет последнее сообщение и остановит работу части сети.

Единственным недостатком RMON являются проблемы совместимости с другими устройствами. RMON1 не полностью согласован, поскольку отдельные производители добавляют различные новые средства к протоколу. Эти средства предоставляют расширенные возможности получения информации с помощью протокола, однако делают несовместимыми между собой различные реализации RMON. Перед покупкой устройств RMON удостоверьтесь, совместимы ли они друг с другом и можно ли контролировать их состояние с помощью ваших средств наблюдения.

Другие средства наблюдения за сетью

А что если вы не используете в своей сети протоколы SNMP или RMON? Это не такая уж большая беда — есть и другие возможности. Вы можете выбрать себе инструмент из поистине неисчерпаемого множества средств управления. Два описываемых далее средства предназначены для решения важных задач: отслеживание содержимого пакетов плюс выявление и определение местонахождения разрывов кабелей.

Анализаторы

Анализатор (sniffer) (в сетях TCP/IP его также называют *анализатором пакетов (packet sniffer))* — это компьютер или устройство, которое отслеживает данные, перемещающиеся по сети, путем перехвата пакетов, которые посылаются не только к ним самим. Такое функционирование называют работой в *смешанном режиме (promiscuous mode)*.

Примечание

Вы можете запускать программу-анализатор не в смешанном режиме, но в этом случае вы будете способны только наблюдать за данными, посылаемыми в и из машины, на которой запущен анализатор.

Анализаторы являются весьма популярными инструментами'взлома, поскольку они способны читать содержимое закрытых пакетов. Они могут также использоваться на законных основаниях для анализа данных сетевого трафика, в том числе различных типов широковещательной передачи, пересылаемой через сеть, для определения компьютера, пославшего данные, и по какому адресу, и т.д. Это та самая информация, которая нужна для эффективного руководства и проверки функционирования сети. Вам не требуется читать всю информацию, поэтому вы можете устанавливать фильтры для захвата только того трафика, который вы хотите

увидеть.

Короче говоря, анализаторы один из методов отслеживания трафика, если ваша сеть не поддерживает RMON. Приложение Network Monitor (Сетевой монитор) фирмы Microsoft, входящее в состав Windows NT, является примером коммерческого анализатора. Имеются и другие анализаторы, как коммерческие, так и доступные на сетевых узлах с различной степенью легитимности.

Доменные рефлектометры

Доменные *рефлектометры (TDR — Time Domain Reflectometer)* функционируют подобно локатору и позволяют вам определить все "узкие места" в сети. Устройство выполняет широковещательную передачу сигнала, называемого *зондирующим импульсным сигналом (fast rize time pulse)*, распространяемым по сети через регулярные интервалы, и ждет отраженного сигнала. Промежуток времени, прошедший до момента получения отраженного импульса, записывается и отображается в виде функции длины кабеля. Допустим, по результатам аудита оборудования вы знаете, что данный кабель имеет длину 20 футов (6 м), а результаты теста TDR покажут длину кабеля 15 футов. Это позволит вам определить наличие разрыва кабеля на отметке 15 футов. Устройства TDR ранее использовались только для проволочных соединений (коаксиальных кабелей и типа "витая пара"), но теперь они стали доступными также и для оптоволоконных сетей (рис. 14.8).

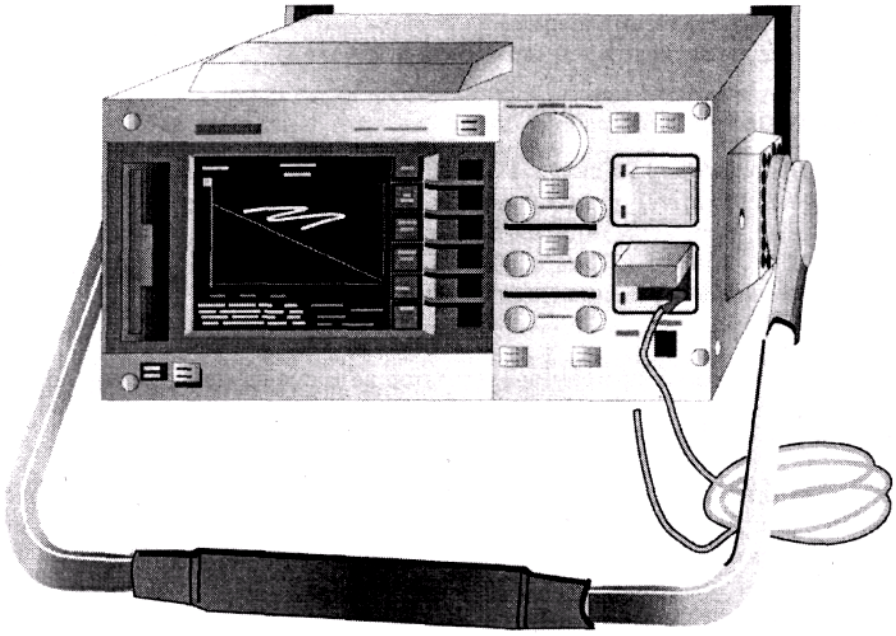


Рис. 14.8. Доменные рефлектометры (TDR) посылают сигналы для тестирования сети

Устройства TDR, мягко говоря, недешевы: TDR для проводных кабелей стоят несколько тысяч долларрв, а для оптоволоконных — 20 000 $ и выше. Это может заставить вас подумать о применении других методов выявления проблем с кабелями (см. следующую вставку), если только вы не работаете с крупной сетью, что позволит оправдать такие расходы.

Ping - дешевый способ выявления разрывов сети

Если вы используете в своей сети протокол TCP/IP, вам не стоит начинать поиск неисправностей в сетевых связях с применения устройства TDR. Сначала попробуйте использовать всегда доступный программный кабельный детектор, управляемый с помощью

клавиатуры. В наборе средств TCP/IP имеется диагностический инструмент "Ping", который просто посылает пакеты по указанным адресам и ждет ответов, подтверждающих прием пакетов в пунктах назначения. Если вы не можете подсоединиться к какому-либо адресу, попытайтесь использовать указанную ниже процедуру для сужения местонахождения неисправности.

1. В компьютере, который не может подсоединиться к другому компьютеру, введите ping 127.0.0.1 для отправки сообщения самому себе. Если эта процедура сработает, значит, компьютер подключен к сети и сетевая плата функционирует нормально.
2. Выполните тест Ping для стандартного шлюза вашего сегмента. Если это сработает, значит, проблема лежит вне сегмента.
3. Запустите тест Ping для сервера DNS. Если сработает, значит, проблема заключается не в определении имен.
4. Выполните тест Ping для сервера Internet (host) в другом сегменте. Если сработает, значит, проблема не связана с протоколом TCP/IP.

И *только* после выявления вызвавшего несрабатывание сегмента воспользуйтесь устройством TDR для нахождения обрыва, если вы подозреваете его наличие, но не можете обнаружить.

Тест Ping может выполнять и другие диагностические функции, например, показывать время, затрачиваемое пакетом на прохождение определенного расстояния, но эти возможности зависят от конкретной реализации средств протокола TCP/IP. Поэкспериментируйте с ними для определения существующих возможностей. Простейший Ping проще в эксплуатации (и дешевле) приобретения специализированных аппаратных средств для определения местонахождения разрывов кабеля.

Снижение расходов на администрирование

Как было указано в гл. 12, снижение общей стоимости содержания сети является весьма актуальной задачей. Там же говорилось о том, что наибольшие расходы на содержание сети приходятся не на стоимость оборудования, а на стоимость управления ею.

В качестве примера соотношения этих стоимостей друг с другом рассмотрим такой случай из жизни. У одной из моих знакомых по имени Джоанна (Joanne) есть родители, которые никогда не работали с компьютером (ее отец — ныне вышедший на пенсию дантист, а мать — артистка и домохозяйка.) В прошлом году на Рождество Джоанна подарила им факсимильный аппарат, чтобы облегчить отправку писем, но в этом году поменяла этот способ общения. После покупки нового компьютера она отдала родителям свой старый, чтобы они могли использовать электронную почту и ICQ (приложение для переговоров через Web и передачи почтовых сообщений).

После этого Джоанна стала тратить несколько часов в месяц на настройку компьютера по телефону. Это определенно улучшило семейные связи или, во всяком случае, усилило их — но в это же время значительно увеличило счета за междугороднюю связь и ее раздражительность. Ее раздражали родители, которые что бы ни делали с компьютером, так тут же его и ломали, а затем обращались к дочери за помощью. Короче говоря, компьютеризация общения не привела к ожидаемому эффекту. Предполагалось, что она сделает жизнь легче, но вместо этого сделала жизнь тяжелее.

Реально Джоанна могла выбрать одну из двух возможностей: продолжать удаленную

техническую поддержку или же установить программное обеспечение удаленного управления на свой и родительский компьютеры и управлять их компьютером на расстоянии. Последняя идея является примером использования средств *нулевого администрирования (zero administration)*.

Примечание

> Novell называет эти средства "организацией сети с нулевыми усилиями" (zero effort networking), но слово "администрирование" кажется более содержательным, поэтому мы будем использовать терминологию Microsoft даже при описании средств фирмы Novell. Оба названия звучат не слишком оптимистично (нулевое администрирование? Я думаю, вряд ли это возможно), но, по крайней мере, указывают на попытку уменьшить время на поддержку клиентного компьютера в работоспособном состоянии.

Нулевое администрирование представляет собой не одну уникальную концепцию, а целый набор инструментов и средств конфигурирования, снижающих расходы на администрирование. Суть идеи состоит в передаче управления ПК от пользователя к администратору с целью:

- уменьшить количество запросов на предоставление помощи из-за ошибок пользователя;
- централизовать загрузку приложений или сделать приложения доступными из любого узла сети;
- разрешить администратору управлять клиентными компьютерами удаленно, загружать требуемое программное обеспечение или перезагружать их в случае необходимости.

Технические средства нулевого администрирования обычно применяются в серверных операционных системах типа NetWare или Windows NT. Свойства программных продуктов, допускающих применение этих средств, зависят от операционной системы. Вообще, технология нулевого администрирования будет обеспечивать управление тем, что пользователь может и не может делать в операционной системе, включая указание на то, какие программы пользователь может выполнять: установку приложений из централизованного источника, удаленную инвентаризацию программного и аппаратного обеспечения, операции удаленной диагностики.

В нулевом администрировании имеется важная особенность, требующая осторожного обращения: для выполнения этой работы на стороне клиента сначала следует получить его права на серверной стороне. По этой причине все эти средства не выполняют настоящего *нулевого* администрирования: чем более "неинтеллектуальны" ваши клиенты, тем более "интеллектуальным" должен быть ваш сервер. Поэтому при конфигурировании серверной стороны с помощью средств нулевого администрирования соблюдайте особую осторожность в работе и тщательно все проверьте, прежде чем применить тот или иной программный продукт.

Продукт Z.E.N. works фирмы Novell

Предлагаемые фирмой Novell средства с нулевыми усилиями по администрированию называются средствами ZEN (Zero Effort Networking — организация сети с нулевыми усилиями) или, используя название соответствующего продукта, Z.E.N.works. Впервые они были предложены в мае 1998г. и представляют собой набор инструментов для передачи основной части работы по администрированию с клиентной машины на сервер. Клиентные компьютеры могут быть сконфигурированы автоматически с помощью новых и обновленных старых приложений, загружаемых клиентами. Эти приложения распространяются по сети, так что они вовсе не обязательно должны быть инсталлированы на единственном сервере. Вместо этого, когда клиент попытается обратиться к приложению, будет задействован ближайший к клиенту сервер. Кроме того, все пользовательские установки, процедуры и права системы защиты поддерживаются средствами обслуживания каталога именно для того, чтобы они были распределены по

сети, а не хранились в одном-единственном месте.

Пока все эти средства весьма похожи на предлагаемые Microsoft средства ZAW (описываемые ниже). В настоящее время они существенно отличаются лишь добавкой, привнесенной в ноябре 1998 г. в Z.E.N.works. Версия 1.1 этого средства содержит поддержку режима удаленной диагностики аппаратного и программного обеспечения для решения проблемы 2000 года.

Продукт ZAWфирмы Microsoft

Если вы не знакомы в достаточной степени с литературой по маркетингу фирмы Microsoft, то можете подумать, что продукт ZAW (Zero Administration Windows — нулевое администрирование Windows) является новым средством следующего поколения NT. Как раз наоборот. ZAW был частью NT, пока не была реализована версия NT 4. Немного позже эти средства превратились в сервер управления системами SMS (System Management Server), предназначенный для поддержки системных правил и профилей пользователя, а летом 1997г. — в комплект инструментов нулевого администрирования ZAK (Zero Administration Kit). Многие не видят смысла в использовании именно таких средств операционной системы, но это не вполне справедливо. Приведенные ниже сведения не являются руководством по использованию Microsoft ZAW, но содержат суть идеи, заложенной в эти инструментальные средства, которые можно использовать для уменьшения времени и усилий, требуемых для администрирования сети.

Правила и профили

Правила и профили являются ответами на один вопрос: как следует организовать согласованную поддержку пользовательского интерфейса? При неверном конфигурировании компьютеров возникает множество проблем с отображением информации у пользователя, параметрами оборудования, установленным программным обеспечением или с другими параметрами конфигурации. Поэтому, если хотите предохранить компьютеры от некорректного конфигурирования, вы должны заблокировать возможность конфигурирования в них чего бы то ни было пользователям, или же не позволять внесенным изменениям становиться постоянными.

Примечание

Профили могут быть заданы или на клиентном компьютере (подразумевается, что в клиентном компьютере установлен жесткий диск), или загружены с сервера при входе пользователя в сеть. Правила всегда помещаются на сервер - они просто не могут быть использованы в одноранговой сети. Этим сервером может быть как сервер NT, так и сервер NetWare - в зависимости от типа сети.

Профили пользователя. Профили содержат набор пользовательских опций (установок), таких как параметры приложений, цветовые палитры, хранители экрана и тому подобное. В компьютерах, работающих под управлением Windows 95, профили являются набором данных, хранимых в файле USER.DAT, используемом системным реестром (Registry) — центральной базе данных всей информации о конфигурации системы. Пользовательская информация не может быть загружена до тех пор, пока кто-либо не войдет в компьютер. По умолчанию профили всех пользователей одного компьютера в Windows 95 одинаковы. Итак, пусть пользователь Джо (Joe) войдет в компьютер, изменит цветовую схему со стандартной (Windows Default) на Storm и выйдет. Когда в этот же компьютер войдет Том (Tammy), то увидит вместо стандартной цветовой схемы Windows Default схему Storm. Тем не менее, если дать Тому возможность изменить цветовую схему, то изменения, внесенные Джо, будут потеряны.

Такой способ работы является стандартным: изменения в цветовой схеме сохраняются в общем файле USER.DAT, и когда кто-либо входит в компьютер, то загружается именно этот файл. Если же вы разрешите применение пользовательских профилей, то для каждого пользователя, вошедшего в компьютер, будет подготовлена пользовательская версия файла USER.DAT. Когда Джо поменяет цветовую схему, то эти изменения будут сохранены не в общем файле конфигурации, а в его персональном файле (изменения конфигурации системы, сделанные одним пользователем, не воздействуют на установки других). В сущности, пользовательские профили ограничивают ущерб, который один человек может нанести компьютеру, используемому многими людьми.

Примечание

Изменение профилей пользователя выполняется при его выходе из системы.

Для радикального ограничения воздействий на компьютер любого пользователя следует обязательно использовать профиль для каждого из них, получаемый путем переименования файла USER.DAT в USER.MAN. Он предоставляет системе общедоступный набор пользовательских параметров. При этом вы не сможете создать несколько обязательных профилей пользователя для одной машины. Однако эти параметры доступны в режиме "Только для чтения". Если Джо изменит цветовую схему в обязательном пользовательском профиле и затем выйдет из системы, эти изменения не появятся при входе в систему Тома. Так и Том может изменять свою систему для текущего сеанса работы, но изменения не сохранятся при его выходе.

Профили пользователя фактически представляют собой низкоуровневый инструмент ZAW и применяются только по отношению к полному набору параметров пользователя. Они не содержат параметры, "привязанные" к компьютеру, и не ограничивают доступ к какому-либо инструменту конфигурирования, например, к панели управления. Однако они уменьшают расходы на поддержку функционирования сети, неизбежные в случае, когда один пользователь приводит в беспорядок параметры, установленные другим пользователем. Если же вы хотите применить более тонкие средства управления, то вам необходимо использовать системные правила, к описанию которых мы и приступаем.

Системные правила. Позволяют при управлении рабочим столом продвинуться на шаг дальше. Вместо предоставления или отмены разрешений на изменение набора параметров пользователя, они воздействуют на определенные компоненты пользовательского интерфейса. К тому же системные правила могут быть использованы для определения способа конфигурирования самого компьютера. Параметры правил сохраняются на центральном сервере в файлах с расширением .pol и могут быть загружены клиентом при входе в систему.

Конфигурирование уровней пользовательского доступа к любым, в том числе весьма тонким, деталям системной конфигурации, может потребовать серьезных усилий, поэтому системные правила их не регламентируют. Вместо этого вы можете явно разрешить или запретить доступ к средствам, вызывающим у вас особое беспокойство, а остальную их часть оставить доступными для определения параметров пользователя. Для того чтобы системные правила работали, необходимо разрешить использование профилей пользователя. Например, вы можете установить системные правила, запрещающие совместное использование файлов, но разрешающие или запрещающие совместное использование принтеров (по выбору пользователя).

Сервер управления системами (SMS)

Правила и профили предназначены для блокирования параметров конфигурации с целью уменьшения вероятности проникновения в них ошибок пользователя. Сервер управления системами SMS является более прогрессивным средством администрирования, способным эффективно контролировать содержимое каждого клиентного компьютера. Используя сервер SMS, вы можете проводить удаленную инвентаризацию программного и аппаратного обеспе-

чения, устанавливать приложения или даже операционную систему, а также перезагружать клиентный компьютер с консоли SMS.

Комплект инструментов нулевого администрирования (ZAK)

Комплект инструментов нулевого администрирования (ZAK - Zero Administration Kit) представляет собой надстройку Windows NT, доступную для загрузки с Web-узла фирмы Microsoft. Эти средства расширяют идею, заложенную в концепцию описанных выше правил и профилей, и предназначены для предоставления стандартного доступа (двух типов) к клиента ым компьютерам: станцию для задач и станцию для приложений. Комплект ZAK устанавливается на клиентной машине (которая должна работать под управлением Windows NT 4 Workstation или Windows 95/98) в одной из двух указанных конфигураций.

Различие между этими конфигурациями заключается в количестве приложений, к которым пользователь может получить доступ (конфигурирование системы не имеет к этому отношения). Режим *TaskSheduler (Планировщик заданий)* предназначен для работы пользователей с проблемно-ориентированными средами. Таким пользователям, как правило, требуется доступ всего к одному приложению (например, к системе управления базой данных). Когда вы загружаете компьютер, сконфигурированный таким образом, он загружается прямо в Internet Explorer или любое другое предварительно указанное приложение. Рабочий стол будет полностью заблокирован: пользователи не смогут использовать кнопку Start (Пуск), приложение Task Manager (Диспетчер заданий), Control Panel (Панель управления) или Explorer (Проводник Windows). Режим *AppStation (Станция приложений)* предназначен для тех пользователей, которые работают с тремя-четырьмя офисными приложениями, но не хотят (или не могут) конфигурировать систему или устанавливать новые приложения. При загрузке клиентного компьютера с помощью такого режима он сразу же попадает в ограниченные администратором средства пользовательского интерфейса, предоставляющие доступ только к требуемым приложениям. Приложение Диспетчер заданий (Task Manager), Панель управления (Control Panel) и Проводник (Explorer) при этом недоступны. Приложения выполняются на сервере, а не на клиентной машине.

Новые средства ZAW

Некоторые функциональные средства ZAW уже реализованы в NT4 или в комплекте ZAK, а появление новых средств связано уже со следующим поколением NT: Windows 2000 Server. Компоненты, имеющие отношение к управлению сетями и не представленные в предыдущих версиях операционной системы, содержат следующие функции:

- автоматическое обновление системы и установка приложений с помощью технологии IntelliMirror;
- унифицированный интерфейс консоли управления Microsoft (MMC — Microsoft Management Console).

Конечно, Windows 2000 содержит средства поддержки и для доступных в данное время средств ZAW. Правила и профили предназначены для облегчения работы по блокированию различных компонентов системы. Установки станции задач (ZAK TaskStation) и станции приложений (ZAK AppStation) будут доступными в Win2K для всех, кто не установил ZAK. Сервер SMS 2 все еще будет поддерживать удаленное управление.

Автоматическое обновление и установка. Автоматическое обновление и установка базируются на технологии IntelliMirror, в которой предусмотрена загрузка данных клиенту без

всяких запросов с его стороны с использованием предварительно заданного множества параметров. Именно так работает броузер каналов. Цель применения такого рода средств для автоматизации обновления и установки приложений очевидна. Пользователь не должен знать, как выполняется установка. Администратор не должен входить в клиентный компьютер для выполнения установки.

Когда пользователи входят в сеть Windows 2000, центральный сервер программ определяет версию клиентной операционной системы и с помощью предварительно установленных разрешений пользователя и/или администратора загружает все программы обновления на рабочий стол клиента.

Консоль управления Microsoft (MMC — Microsoft Management Console). Сама по себе не является инструментом, но предоставляет средства внешнего интерфейса для базового комплекта инструментов NT и сменных комплектов инструментов (snap-ins) различных производителей. Они предназначены для обеспечения централизованного управления сетью взамен нынешней системы, в которой сначала делается что-то одно и закрывается соответствующее управляющее приложение. Затем делается что-то другое и снова закрывается это управляющее приложение. А затем делается что-то третье и, наконец, закрывается и это управляющее приложение. Хотя такая унифицированная консоль, как представляется, не лишена недостатков, она экономит время на получение доступа к инструментам из централизованного источника.

Дополнительное программное обеспечение

Последнее замечание относительно ZAW касается не только приложений. Одна из частей проекта ZAW посвящена созданию более простых в управлении компьютеров. Его авторы отказались от сложных проектов оборудования и предусмотрели взаимозаменяемость компьютерных устройств.

Большая часть теоретического фундамента ZAW относится к тонким клиентным системам, в которых функции клиентных ПК могут быть не просто низведены до уровня терминалов, но могут и на самом деле представлять собой терминалы. Устройства Net PC почти что "выбросили" из себя компьютер. Они не имеют жесткого диска, а их корпус опечатан (это, вероятно, не очень хорошее решение, поскольку усложняет их модернизацию). Предполагается, что вам следует забыть об этом устройстве после его включения, или же заменить его другим клиентным компьютером в случае поломки.

Технология PnP (Plug and Play — Подключи и Работай) представляет собой другую часть проекта ZAW, поскольку она уменьшает время на установку оборудования. Соответствующим образом спроектированное устройство PnP автоматически распознается при загрузке системы, что значительно проще возни с адресами ввода/вывода и установками прерываний. Мониторы стандарта DD2 и видеоплаты могут конфигурироваться автоматически для установки оптимальных параметров отображения, так что вам не придется об этом беспокоиться.

Средства диагностики неисправностей

В хорошо ли, плохо ли документированной, в удаленно управляемой или нет, но рано или поздно в какой-то части локальной сети произойдет сбой. Часто наиболее сложной частью работы с локальной сетью является не само восстановление работоспособности, а выявление и определение компонента, вызвавшего нарушение. С этой точки зрения от вас требуется:

- знать свою сеть и все относящиеся к ней данные;
- уметь локализовать неисправности, возникающие в сети;
- иметь доступ к данным отчетов по ранее возникавшим неисправностям, чтобы вам не пришлось повторно решать одни и те же задачи.

Читайте дальше, чтобы познакомиться с информацией по выявлению неисправностей в сети и их исправлению.

Web могущественнее, чем TDR

Наилучшим инструментом в вашем арсенале средств диагностики неисправностей должна быть не дорогостоящая аппаратура, а *информация.*В этой главе много места отводится описанию методов сбора информации о вашей сети и данных. Если по мере чтения книги вы следовали предлагаемым здесь советам (вряд ли так получалось всегда, но, быть может, вы все же пытались собрать некоторые данные о сети), то сейчас у вас должна быть информация о поведении сети, ее структуре, организации ресурсов и т.п.

Источники диагностической информации

Ваша сеть сама по себе может предоставить вам только часть требуемых данных. Эти данные расскажут о характерных особенностях вашей сети, структуре трафика, оборудовании и т.д. Другую часть информации предоставят внешние данные. Следует знать, что происходит в вашей сети, а также вам необходимо определить характеристики аппаратных и программных средств, которые должны работать в сети совместно.

Текущая поддержка. Наиболее актуальную информацию по интересующим вас операционным системам и оборудованию, вероятно, можно найти в бюллетенях с перечнями отдельных вопросов. Используя такую книгу в качестве онлайнового руководства, можно получить некоторые советы, а также просмотреть и другие бюллетени.

Предупреждение

Учтите, что все прочитанное в переговорной комнате, онлайновом форуме и пользовательском списке рассылки отнюдь не обязательно соответствует действительности. Некоторые их авторы и в самом деле являются опытными специалистами, но вы не должны заранее считать всех, кто ответил на ваш вопрос, экспертами.

Другими источниками текущей информации являются бюллетени, выпускаемые производителями продуктов, которые или рассылаются по электронной почте, или находятся на Web-узлах компаний.

Примечание

Не совсем актуальным, но значительно более упорядоченным источником информации является ежемесячная подписка на компакт-диски, например, TechNet фирмы Microsoft, содержащие "Белую книгу" в виде поисковой базы данных, информацию по исправлению повреждений и другие технические данные.

Кое-кто находит также полезными группы новостей, но соотношение полезная/бесполезная в группах новостей самое низкое. Одна половина трафика групп технических новостей состоит из тематических заголовков типа "Делай деньги сейчас!". Другая половина — обычно не упорядочена и не обязательно имеет отношение к основной теме. Существуют различные онлайновые хранилища информации, совместно используемые профессионалами.

Просмотрите упомянутый список рассылки, дискуссионные форумы или переговорные комнаты, присоединенные к Web-узлу (рис. 14.9).

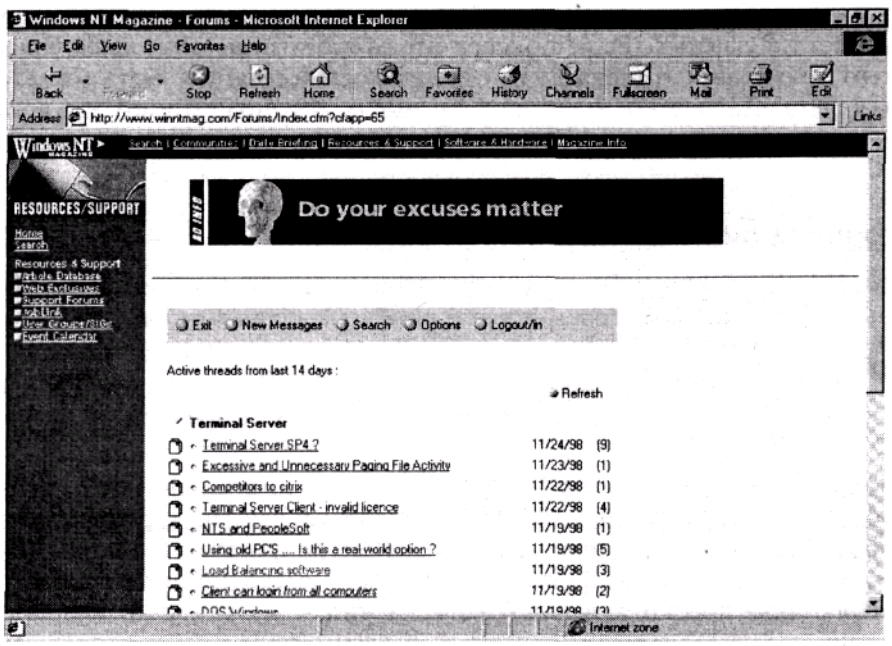


Рис. 14.9. Откажитесь от бесполезной информации в группах новостей форумов Web

Сбор справочной информации. Самая актуальная информация не всегда популярна. Для более глубокого ознакомления читайте отраслевые издания. Еженедельные выпуски приносят новости или отдельные мнения, технические же детали обычно приберегают для месячных изданий. Хотя журналы не так оперативны, как рассылаемые по электронной почте бюллетени, но они содержат справочную информацию, которой нет в списках рассылки или в других местах хранения информации. Журналы могут быть прекрасными учебными пособиями, советами по отдельным проблемам и рекомендациями по применению нового оборудования. Читайте также отраслевые издания с обзорами по конкретной продукции. Обзоры могут содержать комментарии по неисправностям, с которыми пользователь встретился при работе с этим продуктом, и методы поиска неисправностей.

Книги вряд ли предоставят вам ультрасовременную информацию по сравнению с бюллетенями или журналами, поскольку на их публикацию требуется время. Однако они могут быть прекрасным руководством по уже известным (и изученным) проблемам и источником справочной информации, который поможет вам решить собственную проблему или же подаст идеи для поиска дополнительной информации.

Поддержание знаний на современном уровне

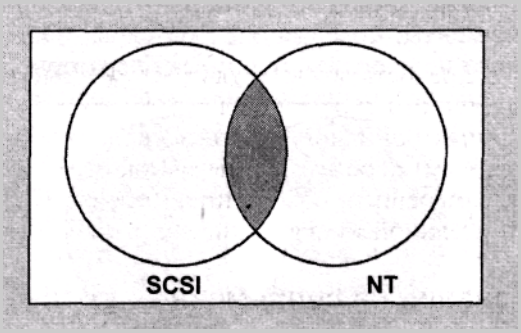
Всякий, кто попытается сориентироваться в водопаде информации по новым технологиям, вероятно, может немного испугаться, подумав "Я никогда не смогу полностью познакомиться со всем этим!". И он будет прав. Нет никого, кто был бы экспертом по всем вопросам. Самое большее, на что мы можем рассчитывать, так это на то, что станем достаточно образованными специалистами, знающими, где можно найти ответы на поставленные вопросы.
Вы можете более эффективно управлять потоком информации, используя различные тактики. Во-первых, подберите себе источники, которые помогут вам в наибольшей степени, и постарайтесь как можно лучше ознакомиться с их содержимым. Ведь если какая-либо информация была напечатана, это вовсе не означает, что она полезна для вас или требуется вам для дела. Microsoft, например, в течение года выпустила сотни статей с базами знаний, посвященными известным проблемам. Большинство из нас не нашло нужным прочитать 90 процентов этих

статей, поскольку все они применимы только для отдельной модели сетевой платы или для неиспользуемых нами приложений. Ищите статьи, которые содержат только интересующие вас ключевые слова (см. следующую вставку).

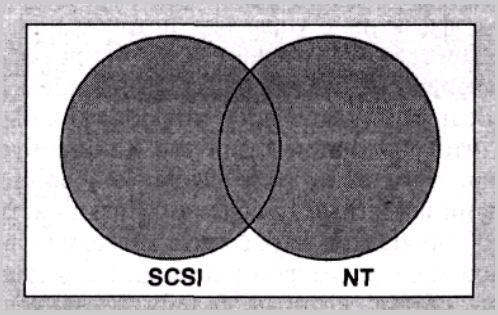
Советы по онлайновому поиску

При сортировке онлайновых изданий лучше всего ознакомиться с уже имеющимися средствами поиска в базах данных. Многие основные механизмы поиска по узлам сети и в Web содержат средства поддержки логических операций (Boolean coding), которые впервые появились в булевой алгебре, созданной в девятнадцатом веке английским математиком Джорджем Булем (George Boole). Они облегчают объединение различных ключевых слов, необходимых для точного указания интересующего вас документа.

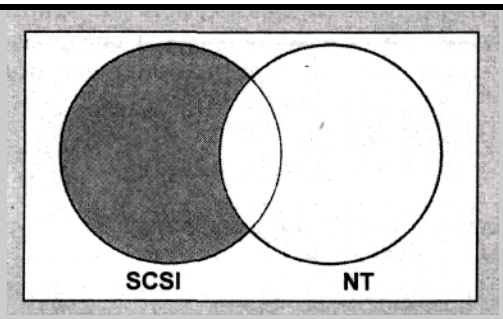
Для поиска документов, содержащих все слова, по которым вы производите поиск, но не какую-то их часть или в каком либо отношении с другими словами, используйте оператор AND, Например, запрос SCSI AND NT возвратит документы, включающие оба слова (наличие "AND" обычно подразумевается по умолчанию). Это значит, что если в окно механизма поиска со средствами работы с логическими операторами вы введете SCSI NT, то компьютер будет искать документы, содержащие оба слова.



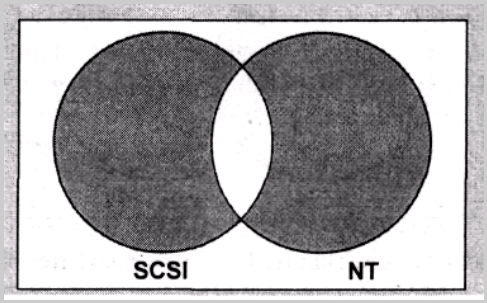
Для поиска документов с любым из интересующих вас словом используйте оператор OR. Например, поиск по запросу SCSI OR NT возвратит все документы, содержащие хотя бы одно из этих слов. Этот оператор используется реже, поскольку обычно возвращает слишком много ответной информации.



Пусть вам требуется найти документ, не содержащий отдельных слов. Например, если вам нужно найти все документы, в которых есть термин SCSI, и нет термина NT, вы должны использовать оператор NOT, например, так: SCSI NOT NT. Оператор NOT полезен для сужения области поиска, если вы считаете, что она может быть обширной.



Для нахождения документа, содержащего одно или другое слово, но не оба вместе, используйте оператор XOR. Например, запрос SCSI XOR NT возвратит все документы, в которых есть какое-либо из этих слов, но нет этих слов вместе. Оператор XOR напоминает оператор OR, но позволяет исключить все документы, содержащие оба слова. Обычно он расширяет диапазон поиска, если не используются иные операторы.



Логические механизмы поиска могут поддерживать два дополнительных оператора, не входящих в состав операторов булевой алгебры: NEAR и кавычки. Оператор NEAR работает аналогично оператору AND, за исключением того, что он производит поиск экземпляров слов, находящихся в тексте друг от друга на некотором расстоянии. Например, запрос SCSI NEAR NT должен возвращать список всех документов, в которых SCSI и NT находятся друг от друга на расстоянии не более восьми слов, игнорируя все документы, в которых появляются оба слова, но на большем расстоянии друг от друга.

Кавычки используются для определения строки поиска, состоящей из нескольких слов. Большинство механизмов при выполнении поиска по строке Windows NT возвратит все документы с Windows и NT — не только экземпляры, содержащие "Windows NT", но и фразы типа "Windows 3.1 is a predecessor of NT" (Windows 3.1 является предшественником NT). Если вы хотите, чтобы механизмы поиска возвращали только документы, в которых оба эти слова появлялись точно такими, как в строке, необходимо использовать кавычки вокруг этой строки, например, "Windows NT".

Операторы в этих примерах очень просты. В каждом из них используется всего два слова и один операнд. Однако запросы могут состоять из нескольких слов и множества операторов, если это необходимо. Например, запрос SCSI AND NT NOT network будет возвращать все документы, содержащие слова SCSI и NT, но не слово "network".

Во-вторых, общайтесь друг с другом с целью обмена информацией. Очень полезно использовать списки адресов и онлайновых форумов — ведь если вы чего-то не знаете, то другие могут это знать. Вы можете вернуть оказанную вам любезность, когда кто-либо спросит у вас нечто, прозвучавшее для вас пустяковым вопросом, но ставшее причиной двухдневного кошмара для спросившего.

Исправления и обновления

Как вы относитесь к обновлению не только вашего электронного "мозга", но и программного обеспечения? Не бывает программного обеспечения — драйверов, приложений или операционных систем — которое можно считать "готовым". Производители часто предоставляют исправления или усовершенствования для своих продуктов в виде новых драйверов и оперативных исправлений (hotfix) для решения какой-либо конкретной проблемы, или же в виде служебных пакетов (Service Pack), предназначенных для решения нескольких проблем, которые могут содержать некоторые дополнительные средства, не входящие в исходный продукт. Знакомство с этими обновлениями является основным способом поддержки знаний об оборудовании и программах на современном уровне. Большая часть обновлений доступна на Web- или FTP-узлах соответствующих производителей или на подписных компакт-дисках, например, TechNet.

Вам следует ознакомиться со всеми этими обновлениями, но вовсе не обязательно тотчас же их устанавливать. Во-первых, не вносите исправления,
если у вас нет достаточного опыта в решении тех проблем, которые эти исправления должны откорректировать.

Во-вторых, если вы решили внести оперативное исправление или установить служебный пакет, сначала удостоверьтесь, что это обновление не приведет к усугублению проблемы и вы сможете восстановить состояние системы, существовавшее до обновления, если это понадобится. (Всякий, кто помнит имеющий дурную репутацию служебный пакет Service Pack 2 для Windows NT 4, поймет, почему это важно. В двух словах эта длинная история сводится к описанию тяжелого труда многих людей по восстановлению резервных копий их систем после установки SP2, поскольку это обновление испортило все текущие установки.) Следует очень внимательно следить за системой в течение одной-двух недель после обновления. Познакомьтесь с мнениями других пользователей, приведенными в бюллетенях производителей, о возникающих при этом проблемах или послушайте, что говорят производители, когда им звонят по телефону и сообщают о какой-то проблеме. Если можно, самостоятельно протестируйте результирующую программу на компьютере, которая может быть повреждена без дополнительного вреда для окружающих. В общем, делайте все, что только можно, чтобы обновление было вам полезным.

Даже если программы обновления не нанесут вреда, иногда они не представляют собой завершенного продукта и не полностью устраняют проблемы, для решения которых предназначены, и похожи на типичную программу, сопровождаемую таким "советом": "Фирма Microsoft настоятельно рекомендует всем заинтересованным заказчикам, включая тех, кто загрузил исходное исправление перед 18 ноября, загрузить и установить обновленное исправление для защиты своих компьютеров".

Очевидно, можно найти себе лучшее занятие, чем дважды загружать и устанавливать исправления для одной и той же программы на свою систему. Если вы хотите использовать все функциональные возможности данного обновления программного обеспечения, то установите его немедленно. В противном случае подождите с установкой, как минимум, несколько дней. Несмотря ни на что, создайте резервную копию всех данных и информации о конфигурации системы перед установкой какого-либо обновления. При этом в случае какой-либо аварии вы сможете, по крайней мере, восстановить работоспособность системы в прежней конфигурации.

Обращение в службу поддержки

Залогом успешной диагностики неисправностей является справочная информация, помогающая вам отслеживать неисправности, и содержащая рецепты для их поиска. Если ее нет, вам ничто не сможет помочь, и придется потратить большее количество времени на получение данных о неисправности, нежели на ее устранение. В этом разделе рассматривается важность документирования обращений в службу поддержки и описываются два способа ус-

пешного решения этой задачи.

Одним из наибольших благодеяний, которые вы можете сделать для себя — это завести журнал аварийных вызовов, нарушений работоспособности и их устранения. Частично поводом для этого служит инстинкт самосохранения: отслеживание вызовов документально фиксирует ваш вклад в работу организации. Также это неплохой повод продемонстрировать необходимость приобретения дополнительного оборудования или приема на работу персонала, или же возможность наглядно доказать, что сделанные изменения привели к разрушению сети. Если вы будете в состоянии документально показать, что количество обращений в службу поддержки "взлетело до небес" после того, как в одной части сети были сделаны изменения, то вы сможете предотвратить распространение этих изменений по всей остальной части сети до их отменены.

Другой повод заключается в предупреждении или устранении нарушений проблем путем отслеживания уже замеченных. Это может касаться отдельных индивидуумов ("Мистер X звонил нам по причине отсутствия доступа к принтеру") или отдельных ситуаций ("Мы можем ожидать вызовов по поводу файлов, называемых 'Ť', от всех пользователей WordPerfect"). Справочная информация такого сорта может быть полезна при обучении новых специалистов службы поддержки или сетевых администраторов.

Итак, вам требуется записывать на бумаге или (как это делаю я) в файле все обращения в службы поддержки. Отчет о каждой неисправности должен содержать следующую информацию.

- Идентификационный номер (ID) отчета о неисправности.
- Предварительная информация.
    - Кто сообщил о возникновении неисправности?
    - Когда поступило сообщение о неисправности?
    - Каким образом поступило сообщение (электронная почта, телефон, устно)?
    - Связано ли это с предыдущими аварийными вызовами?
    - Откуда было отправлено сообщение о неисправности?
    - Какова специфика жалобы?
    - Воспроизводима ли такая неисправность? Способен ли ваш клиент/сотрудник воспроизвести ситуацию у вас перед глазами?
    - Когда это впервые проявилось?
    - Что необычное происходило непосредственно перед и сразу после появления неисправности?
    - Случается ли это периодически? С какой периодичностью?
- Информация об узле сети.
    - Комментарии по поводу окружающей ПК среды: электропитание, температура, другие.
    - Результаты обследования неисправности.
    - Действия, производившиеся на узле.
- Информация о проведенных ремонтах ПК (если таковые выполнялись).
    - Даты выполнения ремонтов?
    - Какие работы были выполнены?
    - Каковы результаты проведенных работ?
    - Был ли компьютер возвращен клиенту/сотруднику? Когда?
- Итоговая информация/ключевые слова.
    - Связана ли эта проблема с оборудованием или программным обеспечением, и/или

с пользователем?

- Если с программным обеспечением, то с каким именно пакетом (пакетами)?
- Если с оборудованием, то с каким именно устройством (устройствами)?

Совет

Для решения типичных проблем предусмотрите создание системы FAQ, сообщения которой пользователь сможет просматривать перед началом работы. Эти средства могут быть использованы персоналом службы поддержки, особенно новыми сотрудниками.

Разделяй и властвуй

Итак, вы получили нужную информацию по состоянию сети и уверены, что используете современную технологию. Вы разработали базу данных известных вам сведений. Что же осталось?

Ну что ж, теперь самое время начать устранять неисправность в сети.

Нашел причину неисправности - исправь ее

Принцип разделения и властвования включает в себя два аспекта. Первый, достаточно очевидный, состоит в выявлении места неисправности. Находится ли она в сети? Где? В каком сегменте? Или неисправность возникла на сервере, скажем, в его памяти, в процессоре, в жестком диске? Вторым, менее очевидным, аспектом является определение неисправности. У вас больше шансов обнаружить ее, если кто-либо сообщит вам о ней, нежели в ходе обычной проверки. После получения такого сообщение ваша работа будет заключаться в детализации полученной информации, чтобы вы могли изолировать реально возникшее нарушение работоспособности.

Вы не уловили разницы между этими двумя задачами? Например, если Джесси (Jesse) обратится к вам и сообщит, что она не может получить свою электронную почту, фактически вы не будете знать, где именно возникла проблема. Без дополнительной информации вы не сможете определить, что же случилось — то ли Джесси не может получить доступ к сети, то ли не может войти в почтовый сервер, то ли не может найти почтовое клиентное приложение, или (что бывает с несобранными людьми) она просто не может загрузить свой компьютер.

Когда вы услышите звонок и снимете трубку, сначала постарайтесь добыть побольше информации о случившемся, а затем последовательно обойдите весь офис, пытаясь отследить, насколько это возможно, источник проблемы. Это нетрудно сделать, а результаты будут весьма продуктивными.

В заключение дадим вам пару советов по сбору информации: если вы не знаете, в чем состоит проблема и как ее можно решить, не советуем вам что-либо делать и высказывать "конфиденциальные" предположения. ' Во-первых, это будет раздражать пользователей, если ваш совет не приведет к успеху, поскольку они должны будут повторить свой вызов. Один ответ: "Я пока не знаю, в чем тут дело, и позвоню вам через час после изучения проблемы", — стоит дороже шести советов типа: "Проблема заключается в X — делайте Y. Не получилось? Не работает? Попытайтесь сделать Z. Тоже не работает? Попытайтесь сделать A". Ведь если вы и в самом деле ответите на вопрос, первый из указанных выше ответов сохранит конфиденциальность. А второй — нарушит ее.

Во-вторых, если вы составляете предварительный отчет о возникшей проблеме, то перенесите свои усилия с решения проблемы в сторону обеспечения своих прав. Неважно, были ли вы правы с самого начала, или нет — пользователи простят ошибки, если вы все-таки сможете исправить проблему.

Выявление затруднений

Ну, хорошо, вы составили более детальное описание ситуации. Теперь следует отследить причину ее возникновения. Спросите себя:

- Кто страдает от этой неисправности? Один человек, рабочая группа, домен, сегмент или вся сеть?
- Какие действия привели к возникновению нарушения? Что пользователь пытался сделать, и из-за чего возникло нарушение? Возникает эта ситуация лишь при одном-единственном сочетании обстоятельств или проявляется в различное время? Прослеживается ли здесь какая-либо тенденция?
- Возникала ли эта неисправность ранее? Что было ее причиной, как она была разрешена?
- Какое различие между вчерашним днем (или каким-то другим, когда нарушения еще не было) и сегодняшним (или тем, в который неисправность возникла).

Короче говоря, вы должны подумать, выявить тенденции и найти примеры подобных случаев.

Подготовка к изменениям

Даже оптимально управляемая и максимально свободная от аварий сеть, в конце концов, должна подвергнуться изменениям. Со временем появляются новое оборудование, новые приложения или новые версии уже существующих приложений, да и сами компании претерпевают изменения. Рано или поздно вы будете вынуждены делать большие или маленькие изменения в сети. Ваша задача состоит в максимально возможном упрощении этой работы. Для этого вы должны слить воедино все свое техническое мастерство с тактичностью дипломата. Однако заметим, что работа дипломата состоит отнюдь не в хождении вокруг да около, а, наоборот, в умении идти своим путем, чтобы другие участники процесса общения относились к этому с пониманием.

В дальнейшем описании некоторая часть сеансов сетевого планирования отделена от других, и, начиная с описания переходов на новое оборудование или программное обеспечение, изложение будет более подробным. Переход на новое оборудование или программное обеспечение почти всегда выполняется одинаково.

1. Определяются требования к новой системе.
2. Планируются компоновки (аппаратная или программная).
3. Тестируется новая система, и устраняются возникшие нарушения работоспособности.
4. Реализуется новая система.
5. Осуществляется обратная связь с пользователями.

Рассмотрим все эти вопросы более детально.

Анализ требований к системе

Первым шагом при планировании изменений сети должно быть определение новых средств решения текущих и будущих задач. Необходимо отыскать новую технологию или продукт, которые смогут принести пользу системе. Как мне представляется, наиболее правильный подход заключается в использовании принципа: "Как бы нам облегчить себе жизнь?",

— вместо: "Это что-то новенькое. Как бы нам включить это средство в сеть?".

Подготовка с помощью регулярных совещаний

С целью выполнения анализа многие компании, особенно крупные, проводят регулярные совещания в сети. В процессе этих совещаний они оценивают сетевую производительность, удовлетворенность пользователей работой системы и т.п. Если стала доступной новая технология, то, значит, пора кратко сообщить об этом сотрудникам. На таких совещаниях должен присутствовать не только управленческий персонал (MIS staff) — это совещания управляющих с участием пользователей и обслуживающего персонала, вносящих предложения о том, что им требуется и что для этого можно сделать. Точное число участников зависит, конечно, от размеров компании. В одной компании в совещании могут участвовать 8—10 человек (надеемся, у вас их будет не больше, иначе вы ничего толком не сможете сделать). В другой — вы встретите трех, каждый из которых является "единым во многих лицах" специалистом. Как бы то ни было, на совещаниях должны быть представители:

- сетевых администраторов;
- администрации здания;
- группы обслуживания оборудования;
- группы поддержки программного обеспечения;
- персонала поддержки сети;
- пользователей.

Совет

Чем меньше число участников сетевых совещаний, тем более вероятно, что вам удастся сделать что-нибудь полезное. Если некоторые участники нужны лишь "постольку поскольку", предоставьте им возможность выступить в качестве гостей и сделать доклад по вопросам, относящимся к их компетенции.

Описанные выше обращения в службы поддержки, отслеживаемые вами, являются одним из источников информации о пользовательских требованиях. Если вы зафиксировали множество звонков по поводу отдельного текстового процессора, а по вашим данным имеется новая версия сервисного пакета, исправляющая недостатки текущей версии, значит, настало время приобрести новую версию текстового процессора. Или, если вы получаете множество нареканий на плохую реакцию системы при запуске программ под Windows в режиме эмуляции, то вам следует поменять операционную систему на ту, которая поддерживает уже используемые приложения.

Другим потенциальным источником информации являются отзывы пользователей о работе системы и список их потребностей. Это одна из причин, по которой необходим представитель пользователей. Такой человек не всегда является представителем всех пользователей, но мнение людей, использующих сеть, о тех средствах, которые могут облегчить им жизнь, вероятно, имеет большое значение даже в том случае, если их взгляды будут не очень четко сформулированы.

Предложите пользователям ввести данные

Если вы планируете внести большие изменения, о них следует рассказать пользователям сети, чтобы узнать, какие приложения им нужны для выполнения своей работы и какая необходима образовательная подготовка. Ниже приведен пример списка вопросов, используемого для опроса, проведенного накануне перехода правительственной организации с рабочих станций UNIX на Windows NT.

1. Поскольку мы собираемся покупать инструментальные средства MS Office Suite, отметьте все перечисленные ниже приложения, которые вам понадобятся при переходе на новую систему NT. Если возможно, перечислите версии, которые вы используете в настоящее время.

   Applix Mail;
   Applix Spreadsheet;
   Applix Word;
   Corel Draw;
   Corel Presentation;
   Frame Maker;
   PhotoShop;
   WordPerfect.

Примечание

Это всего лишь пример. Конкретные пункты этого списка не имеют значения. Здесь вы должны главным образом постараться получить ответ на вопрос: "Если ваш компьютер завтра исчезнет, какие приложения потребуется восстановить, чтобы вы могли продолжать работу?"

2. Требуется ли вам программное обеспечение, не приведенное в списке п. 1 ?
3. Нужен ли вам какой-либо макрос для конвертирования старых файлов?
4. Требуют ли ваши заказчики сохранения файлов в определенном формате?
5. Какие средства интерфейса с базой данных вам необходимы для перехода на новую операционную систему?
6. Какая подготовка вам потребуется? Укажите, пожалуйста, ваш уровень знаний по данному вопросу.
7. Имеются ли у вас какие-либо дополнительные комментарии или замечания относительно перехода?

Когда вы будете приглашать пользователей ввести данные, помните о следующем. Во-первых, то, что кто-то затребовал определенные средства, вовсе не означает, что их следует предоставить. В данном частном примере пара пользователей из одного подразделения захотели получить программное обеспечение для моделирования трехмерной графики. Они не имели его на момент обследования, и характер их работы не предусматривал каких-либо задач, требующих программного обеспечения для моделирования трехмерной графики. Но они потребовали его, поскольку знали, как его можно использовать (данный запрос был отвергнут).

Во-вторых, это связано с первым: введенная пользователем информация носит исключительно рекомендательный характер, так что и вы (человек, проводящий опрос), и пользователь должны это понимать. Каждый раз при изменении части сети вы будете как приобретать какие-то преимущества, так и терять некоторые из них. Если вы попытаетесь придерживаться нереального замысла, позволяющего пользователям диктовать основные принципы организации сети, то добьетесь лишь появления множества обиженных, так как сеть или приложение не будут нормально работать. Помните: достижение состояния работоспособности и эффективной управляемости сети являются итогом работы всей команды. Хотя вы и вносите изменения, облегчающие жизнь всем пользователям, за принятые решения отвечаете только вы. Иногда требуется принимать компромиссные решения, ухудшая одни параметры за счет других.

Планирование инфраструктуры сети

После того как вы выяснили запросы пользователей сети, и у вас появились какие-то идеи относительно технологии, которая может удовлетворить этим требованиям, приходит время складывать воедино все компоненты сетевой инфраструктуры. Для этого необходимо

ответить на несколько вопросов, которые могут меняться в зависимости от природы выполняемых в сети изменений, но чаще всего вопросы выглядят следующим образом.

- Работа каких приложений должна поддерживаться в сети?
- Кому необходим доступ к этим приложениям?
- Какие возможности управления своими компьютерами могут (должны) получить пользователи?
- В какой степени должны быть защищены данные?
- С какими другими сетями вам требуется организовать связь?
- Какое оборудование необходимо поддерживать? Какое должно быть заменено? Какое добавить?
- В каком направлении будет далее развиваться сеть? Можем ли мы определить свои потребности, нереальные сейчас, но доступные через год или два?

На основе ответов на эти вопросы вы можете выбрать оборудование и программное обеспечение, и их конфигурацию, обеспечивающую эти потребности. Если вы в состоянии быть в курсе всех технологических новинок ("Смотрите, про это приложение я недавно читал в отраслевом издании!"), то поиск инструментов, которые соответствуют вашим запросам и годятся для совместного использования, не будет слишком сложен и продолжителен. Для решения проблем, выходящих за рамки вашей компетенции, вам может потребоваться некоторое время на поиск самых последних предложений или прибегнуть к посторонней помощи.

Совет

Не забывайте о сетевом взаимодействии, когда планируете инфраструктуру своей сети. Львиная доля проблем возникает из-за того, что "эта часть сети не взаимодействует с другой". Сэкономьте себе время и определите части сети, которые могут взаимодействовать друг с другом или это можно сделать в будущем.

Одна из задач планирования инфраструктуры — обучение клиентов работе с новыми компонентами сети. Это не всегда необходимо — если вы установите новую серверную операционную систему, то пользовательский интерфейс может вообще не измениться. Однако если каких-либо пользователей необходимо обучать работе с новыми приложениям, сейчас для этого самое время.

Тестирование компонентов

Итак, вы уже подобрали компоненты для своей сети и даже знаете, как сложить их вместе. Установите же их! Изменения будут сделаны, и вы спокойно начнете работать с завтрашнего утра!

Но, быть может, лучше сначала удостовериться, что эти изменения работоспособны, перед тем как вносить их в уже функционирующую сеть?

Успешная установка — это протестированная установка. Характер тестирования зависит от объема сделанных изменений, ресурсов компании, которые могут быть отведены для тестирования, и, возможно, от опыта клиентов, но тестирование является обычной составной частью процесса модернизации сети. И для этого имеются веские основания. Если вы не протестируете изменения, то сможете лишь теоретически предполагать, что все работает нормально, и не будете знать, как это работает на самом деле.

Для проверки безопасности внесенных изменений в сети вы можете сначала выполнить их в лабораторных условиях, если у вас, конечно, имеются таковые. Лабораторное тестирование фактически и будет предварительным тестированием. Во время его выполнения вы сможете экспериментально выбрать наилучший способ установки изменений, попробовать различные конфигурации и, вообще, поработать с системой для достижения наибольшей производительности, не беспокоясь о том, что ваши действия скажутся на пользователях. Загрузку

данных можно сымитировать с помощью автоматических генераторов пакетов, так что можно будет легко определить, как ваша сеть работает в критических условиях, не привлекая для этого "живых" пользователей. Лабораторное тестирование также является подходящим случаем для обнаружения конфликтов при взаимодействии сетей, так что вы сможете разрешить их заранее, не причиняя беспокойства кому-либо, кроме персонала подразделения IS (Information Systems).

Совет

Вы можете подсоединить компьютеры лаборатории к основной сети, если объедините их в собственный сегмент, подключаемый с помощью повторителя, маршрутизатора или моста. В этом случае проблемы в лабораторной сети не будут воздействовать на остальную сеть, но вы сможете получить любую нужную вам информацию, доступную по сети.

Животные, живущие в зоопарке, не ведут себя как звери, живущие на воле. Лабораторная сеть не всегда ведет себя так, как "живая". Серьезным испытанием стабильности изменений является работа в производственных условиях, иначе вам трудно будет судить, как сеть поведет себя в пиковых ситуациях на протяжении рабочего дня. Вы сможете перейти в рабочий режим (не преодолевая одним прыжком всю дистанцию, разделяющую лабораторные испытания и реализацию этих изменений во всей сети) несколькими способами.

Если изменения фактически являются включением в сеть нового элемента (или если сеть сама только что создана), вы можете организовать тестовый узел. На тестовом узле эти изменения должны быть реализованы так же, как если бы они были внесены в сеть и использовались в обычном режиме. Результаты работы тестового узла могут быть зафиксированы и оценены. Если необходимо сделать какие-либо дополнительные изменения, вы можете внести их и опробовать на тестовом узле. После того как сеть будет готова и начнет работать на тестовом узле, вы можете распространить изменения на другие узлы.

Если тестирование отдельных узлов невозможно, вы можете ограничить область внесения изменений одним тестовым сегментом или тестовой группой в зависимости от того, имеет ли изменение логическую или физическую природу, или же обе сразу. К тому же, если внесенные локально изменения работают так, как ожидается, то вы можете распространить их по всей сети. Однако учтите, что такому тестированию подвергается только ограниченная часть всей сети, что позволяет вам найти и изолировать нарушения, когда они воздействуют еще на ограниченное количество пользователей.

Третий подход к тестированию состоит в постепенном наращивании изменений, т.е. в частичном добавлении изменений в сеть. Такой способ реализации может потребовать некоторых дополнительных усилий, но он позволяет изолировать компоненты сети, а не пользователей. В этом случае, если установленный компонент не работает, вы сможете легко выявить причину, поскольку новые элементы вводятся по одному за один раз, а не сразу всей группой.

Эти методы тестирования не исключают друг друга — вне всякого сомнения, их можно комбинировать. Можно придумать и свои, новые способы тестирования сети. Однако, независимо от используемого метода, принципы остаются неизменными: ограничение отрицательных последствий до тех пор, пока вы не удостоверитесь, что сеть работает так, как ожидалось. Значительно проще удалить неисправность в малом масштабе и затем реализовать такое изменение во всей сети, чем исправлять нарушение работоспособности всей крупной и сложной сети.

Реализация сети

Итак, наконец-то вы готовы применить (и сохранить) сделанные изменения. Если это возможно, завершите выполнение этой задачи или где-нибудь в стороне от большинства клиентов сети, или тогда, когда все они отсутствуют (предусмотрите достаточный резерв времени). Внесение изменений, как правило, занимает больше времени, чем мы предполагаем, и если вы будете ограничены во времени, то, скорее всего, начнете нервничать и пропускать отдельные действия, что может привести к возникновению новых проблем.

Даже если вы заранее протестировали все изменения, следует подождать некоторое время, чтобы "сгладились" все неисправности, которые не проявились до полномасштабной их реализации. Однако если вы протестировали все достаточно тщательно, то можете ожидать уменьшения количества неисправностей.

Выводы

Как уже было сказано, объединение компонентов сети в единое целое часто представляется сравнительно легкой задачей. Самое тяжелое время настанет, когда пользователям потребуется поработать с какими-то средствами, и вы должны будете или исправлять результаты работы, или вносить изменения.

Чтобы сделать работу по ремонту сети настолько легкой, насколько это возможно, вам следует задокументировать сеть до того момента, как она прекратит работу: изучите все компоненты вашей сети и ее схему так хорошо, как только сможете, с тем, чтобы в тот момент, когда что-то станет работать не так, вам было бы проще выявить источник нарушения. Дополнением к этому может быть блокирование пользовательских рабочих столов. Храните приложения централизованно и препятствуйте попыткам пользователей выполнить конфигурирование (возможно, ошибочное) своих компьютеров. Старайтесь проводить все инвентаризации и установки из одного центрального пункта, чтобы не пришлось слишком много бегать при выполнении этой работы. Суть такого подхода заключается в том, чтобы с помощью адекватной информации о своей сети и соответствующего уровня контроля над ней сделать работу по управлению сетью значительно проще, чем если бы она была свободной для всего и вся.

Управление, т.е. поддержка работающей сети в должном состоянии — это значительная часть одной общей задачи: облегчения жизни сетевых пользователей. В следующей главе расскажем о другом аспекте этой задачи — о защите данных.

Упражнение 14

Вы пытаетесь определить количество клиентов, использующих файловый сервер в будний день в послеполуденное время. Дополните эти пункты.

1. Какого типа аудит вы должны выполнить?
2. Какой инструмент, описанный в этой главе, поможет вам определить, сколько клиентных запросов ожидают обработки в данный момент времени?
3. Какой инструмент вы используете, чтобы определить клиентные компьютеры, которые связывались с вашим сервером?
4. Для идентификации компьютера в отдельном сегменте вы должны использовать_____сетевую карту.
5. Чем хороша идея удаленного запуска инструмента наблюдения за сервером?
6. Информационной базой для управления является_____файл.

    A. Текстовый
    B. Двоичный
    C. Читаемый с помощью компьютера
    D. Никакой из указанных

7. На каком протоколе без установки соединения базируется протокол SNMP?
8. Вы хотите наблюдать за трафиком IPX/SPX на одном из сегментов сети. Каким инструментом следует воспользоваться?

A. SNMP
B. CMIP
C. RMON
D. TDR

9. Ответьте: "Да" или "Нет". Для работы SNMP требуется поддержка протокола TCP/IP.
10. Какая технология нулевого администрирования в данный момент поддерживает проверку решения проблемы Y2K через сеть?
11. Какое из следующих средств ZAW не является внешней частью NT 4?

A. Системные правила
B. Конфигурация TaskStation
C. Контроль совместимости Y2K
D. Профили пользователей

12. Какие именно документы будут найдены в результате применения следующего логического оператора поиска: "NetWare 5" NEAR Zero Administration?
13. Напишите запрос, по которому будет возвращен список документов, содержащих ссылки на NT или NetWare, но не оба сразу.
14. Перечислите три способа тестирования изменений перед полной их реализацией.

Глава 15

Защита сетей

Что такое защита сетей? Ответ не такой простой, как может показаться, поскольку в понятие "защита" входит несколько элементов. Концепция защиты едина, но она состоит из трех составляющих, связанных, в основном, с защитой данных.

Во-первых, сеть следует защитить от несанкционированного доступа. Как предотвратить вход в сеть незарегистрированных пользователей, а законным пользователям не позволить просматривать данные, для них не предназначенные? Во-вторых, данные необходимо защитить от повреждений. Каким образом можно гарантировать, что данные не будут разрушены или, точнее, как восстановить их после повреждения?

Примечание

Защита от потерь данных рассматривается в гл. 16.

В-третьих, сетевые компьютеры необходимо защищать от вирусов. Вирусы могут быть как совершенно безобидными, так и деструктивными, однако сам факт наличия даже безвредных вирусов раздражает пользователей.

В этой главе рассматривается подготовка к созданию системы защиты и инструментальные средства, которые вы можете для этого использовать.

Предварительное планирование

На первом этапе защиты сети следует определить, от чего именно ее следует защищать, а также оценить примерную стоимость такой защиты. Определившись с этим, можно приступить к решению более тонких вопросов, связанных с разрешениями для пользователей и групп или политикой назначения паролей (password policies).

Не гоняйтесь за призраками

Хотя это и очевидно, стоит сказать: прежде чем разрабатывать систему защиты, подумайте о том, что, собственно говоря, вам угрожает. Так, например, некоторые подразделения Министерства обороны США занимаются анализом угрозы, иными словами, анализом всех возможных источников опасности, а также оценкой их значимости и вероятности проявления. Результаты анализа распадаются на две части: скажем, страна X рассматривается как меньшая угроза национальной безопасности США, чем страна Y, а Y не представляет большой опасности в краткосрочном плане, но может стать опасной в течение одного-двух десятилетий.

Анализ требований к системе защиты сети во многом подобен описанному: он тоже требует идентификации опасностей и оценки их серьезности. Например, служащий фирмы, отвечающий за архивирование, представляет собой некую опасность — он может украсть магнитные ленты с архивами и продать их промышленным шпионам. *Собирается ли* он сделать это? А если сделает, чем это грозит? Ответы на вопросы подобного рода позволяют представить степень опасности этого служащего. Оценив ее, можно предпринять соответствующие меры, предотвращающие кражу лент.

Для идентификации опасности и оценки ее серьезности можно использовать два подхода. Прежде всего, если у вас есть опыт в защите сетей, можно положиться на собственную интуицию. Это допустимо при работе с небольшими сетями, в которых защитой занимается

единственный служащий, однако не годится для крупных сетей, а также в том случае, если вы обязаны отчитываться за свои поступки.

Более строгий подход, который больше подходит людям, пытающимся найти решение в новой или очень сложной ситуации, заключается в систематической идентификации и индивидуальной оценке опасности каждого вида. Такой подход срабатывает безукоризненно, особенно если вы можете привлечь несколько служащих с разнообразными познаниями к "мозговому штурму", чтобы рассмотреть вопрос с разных точек зрения. Попросите каждого служащего письменно изложить вероятные источники опасности для системы защиты, которые они в состоянии предвидеть, затем сравните списки, удалите из них повторяющиеся или бессмысленные идеи. То, что у вас останется, и представляет собой конкретные виды опасностей, которые следует оценить и устранить.

Совет

Для более содержательного анализа опасностей рекомендуем постоянно просматривать бюллетени защиты (security bulletins), выпускаемые производителями сетевых компонентов. В них в общих чертах описываются возможные проблемы, а также методы их обхода или исправления.

Кого привлечь к работе

Стоит ли привлекать посторонних консультантов, специализирующихся на проблемах защиты, или положиться на собственных служащих, хорошо знающих ситуацию? Если вы наймете консультанта с большим опытом работы в разных фирмах и организациях, сравнимых с вашей, можно перенять его опыт. Разумеется, консультант не в состоянии единолично отвечать за полное конструирование системы защиты, однако его опыт может подсказать вам решения, до которых вы не смогли бы додуматься самостоятельно, либо найти опасность, которая заметна только постороннему взгляду.

С другой стороны, консультант по защите не знает вашу организацию так же хорошо, как ее служащие. Посторонний человек в меньшей степени доверяет фактам, которым трудно дать количественную оценку, но вам представляются крайне важными при оценке возможной опасности. Кроме того, он может вообще упустить из виду важные элементы, которые вам кажутся вполне очевидными (в результате долгой работы в своей фирме). С другой стороны, посторонний консультант может оказаться совершенно прав, игнорируя некоторые непредсказуемые элементы, вроде личных достоинств служащих, поскольку они совершенно субъективны.

Подводя итог, можно сказать, что опытный консультант по защите, который опирается как на ваши знания внутренних проблем, так и на собственную квалификацию, может оказаться весьма полезен. Неопытный консультант, который подходит к решению проблемы без учета специфики организации, не принесет никакой пользы в создании системы защиты (как и чего-либо вообще).

И последнее замечание об опасностях. Internet — великолепная среда для совместного использования информации. Но это также превосходная "фабрика слухов". Отнюдь не всякая угроза безопасности, о которой вы узнаете, реальна и не всегда ведет к повреждению системы защиты. Точно так же не стоит полагаться на всякий пакет, предлагаемый для исправления "прорех" вашей системы защиты, поскольку и сами пакеты не всегда надежны. Общеизвестные принципы сбора и анализа информации вполне эффективны, если на практике учитывают следующие особенности систем защиты.

- Принимают во внимание источник опасности для системы защиты.
- Если недостатки системы защиты незначительны, не бросайтесь немедленно вносить исправления. Подождите неделю, чтобы зафиксировать реакцию пользователей. Иногда эти исправления работают совсем не так, как рекламируются.

- Используйте пакеты с исправлениями, полученные только из надежных Web- или FTP-узлов: не стоит устанавливать какой-нибудь "пакет" только для того, чтобы убедиться, что это — "троянский конь", т.е. вирус, замаскированный под формально полезную программу.

В общем, защищайте вашу сеть и самого себя, при этом сохраняйте здоровую долю скептицизма.

Соразмеряйте защиту с ее стоимостью

Оказывается, в современном мире есть и такая штука — *слишком* защищенные сети! *Слишком* защищенные не в том смысле, что данные защищены лучше, чем это необходимо. Пользователи, очевидно, не слишком расстроятся, когда обнаружат, что меры защиты предотвращают утрату или искажение данных. (Хотя тех, кто только что получил в электронной форме выговор за плохую работу, не слишком огорчит пропажа *этого* документа.)

Нет, проблема заключается не в степени защиты, а в том, какой ценой она достигается. Цена выражается двояко. Меры защиты (по определению) вызывают некоторое раздражение как пользователей, так и администраторов, поскольку затрудняют доступ к данным. Пользователи должны помнить изменяемые пароли, а вы должны установить схемы шифрования, отсортировать права пользователей, сконфигурировать брандмауэры... Это серьезная работа, которая отнимает много времени. Второй фактор связан с первым. Установка системы защиты стоит денег, как с точки зрения стоимости собственно системы, так и оплаты труда специалистов по ее установке.

Вопрос не в том, что система защиты обходится дороже, чем она того заслуживает. Ваши данные — самое важное, что есть в компьютере или в сети, причем в отличие от всего остального их нечем заменить. Все данные следует защитить от потери, а часть данных — держать в тайне. И, тем не менее, следует выполнить небольшой расчет и сопоставить стоимость защиты со стоимостью защищаемых данных.

Проще всего сказать, что система защиты должна быть не дороже того, что она защищает. Какие же факторы определяют эту цену? Оценивая систему защиты, сопоставьте, насколько изменится каждый фактор, перечисленный в табл. 15.1, при использовании конкретной системы защиты по сравнению с отказом от нее.

Таблица 15.1. Анализ соотношения цена/эффективность применительно к системам защиты

Фактор	Цена	Эффективность
Производительность труда	Как изменится производительность после установки системы защиты?	Во что обойдется (учитывая затраты времени и оплату труда) воссоздание или замена утраченных или искаженных данных?
Административные расходы	Во что обойдется (учитывая затраты времени и оплату труда) первоначальная реализация системы?	Во что обойдется (учитывая затраты времени и оплату труда) восстановление и повторный запуск системы?
Объем сбыта	Насколько система защиты помешает вашему бизнесу?	Насколько улучшит работу фирмы установка системы защиты?
Законные обязательства	Какую ответственность мы принимаем на себя, реализуя данную систему?	Какую ответственность мы примем на себя, если не реализуем систему и данные будут утрачены либо искажены?

Стоимость страховки	Насколько система защиты изменит стоимость страховки?	Насколько система защиты изменит стоимость страховки?

Каждый фактор можно оценить суммой в долларах, которую затем следует проанализировать со всех сторон.

Уяснив, в чем заключается риск и что следует сделать для его предотвращения, можно познакомиться с деталями, описанными в оставшейся части главы.

Привлеките пользователей на свою сторону

Вы не сумеете защитить сеть, если начнете воевать с пользователями.

Система защиты сети относится скорее к сфере управления, а не к технологии. Само по себе блокирование системных средств не решает задачу защиты. Если система защиты слишком неудобна, пользователи сумеют обойти ее. Если же это будет слишком трудно, они начнут жаловаться. Большинство из них не ожидают некорректной работы системы защиты, и, следовательно, подготовка к этому вызывает раздражение.

Как же поступить в таком случае? Пользователям следует объяснить причины установки системы защиты. Это отнюдь не означает, что вы должны советоваться со всеми пользователями. Поступив таким образом, вы ухудшите систему защиты, поскольку для облегчения доступа придется пожертвовать защитой (или ее элементами). Вместо этого расскажите пользователям, почему не следует разглашать пароли, зачем нужно выходить из системы на время ленча и т.д. Помогите им понять, почему недопустимо приносить из дома дискеты и почему поступающие файлы необходимо всегда проверять на наличие вирусов. В общем, поясните людям, насколько полезна для них же самих система защиты. В противном случае вас ждет тяжелое сражение, которое вы проиграете просто из-за численного превосходства "противника".

Хуже всего, если на вас начнут смотреть, как на ужасное пугало, которое препятствует доступу к системе. А что если улучшить мнение о себе, заблокировав сеть прежде, чем пользователи получат к ней доступ? Затем вы будете постепенно деблокировать ее части, по мере того как пользователи будут требовать доступа к ним. И тогда, вместо того, чтобы выглядеть дядюшкой Скруджем (Scrooge — скряга (англ.)), запрещающим пользователям доступ, вы станете Санта Клаусом, *разрешающим* доступ к сети. Только не говорите кому-нибудь, что именно вы организовали начальную блокировку сети.

Защита от несанкционированного доступа

Хакеры, шмакеры.

Так, да не так.

Примечание

С технической точки зрения *хакер* (hacker) - это пользователь, который "общается" (hack) с компьютером, пытаясь лучше изучить систему. Вы сами можете попробовать сделать это. *Кракером* (cracker) называют пользователя, который прорывается в защищенную систему с целью кражи или искажения данных. В прессе эти термины часто путают, однако это отнюдь не одно и то же.

Легенды о взломах баз данных Пентагона и разрушении Web-узла газеты *New York Time*s — это часть их реальных "подвигов". Поэтому сети следует, безусловно, защищать от внешнего влияния. Однако вам, вероятно, гораздо реже придется сталкиваться с вредом, нанесенным скучающими или праздными злоумышленниками, проникающими в сеть, чем с каким-либо сообразительным пареньком, который сидит в подвале за компьютером, оснащенным модемом. Как правило, реальную угрозу защите сети представляют не пользователи, а лазейки в системе защиты. Заткните лазейки — и вы избавитесь от 99% нарушителей.

Итак, настало время подумать о методах допуска в сеть только зарегистрированных пользователей, ограничения их возможностей, а также отслеживания их входов в систему. Ну, а если вы — параноик, можно даже присматривать за тем, чем они там занимаются.

Идентификация пользователей

Для предотвращения доступа в сеть незарегистрированных пользователей прежде всего следует установить *учетную запись* (user account). Пока пользователь не введет достоверное имя и пароль, указанные в учетной записи, он не сможет войти в сеть. Например, в сетях Windows NT каждому пользователю назначают персональную учетную запись с внутренним защитным кодом (SID — Security Identifier), по которому операционная система однозначно идентифицирует пользователя. Исключения из этого правила обычно делают только для учетной записи Guest (гость), которая может использоваться кем угодно, кто знает ее пароль. Однако в ныне действующих сетях по этой учетной записи предоставляют весьма ограниченный доступ к системе.

Защитный код (SID) определяет, что может делать в сети данный пользователь. Например, когда кто-то пытается открыть файл, подсистема защиты (security subsystem) проверяет этот файл, сверяет личность пользователя со списком тех, кому разрешен доступ к файлу, а затем устанавливает тип доступа, который ему предоставлен.

Примечание

Тонкости работы средств организации разрешений на доступ зависят от операционной системы, установленной на сервере.

Конец маскарада

Одна из проблем доступа заключается не только в создании средств, принуждающих пользователей предъявлять "верительные грамоты" на право использовать сетевые ресурсы, но также и в гарантии того, что злоумышленник не подделает достоверную учетную запись и не присвоит себе личность пользователя — не *замаскируется* под пользователя. Одним словом, важно удостовериться, что учетные записи пользователя защищены, и никто не может замаскироваться под зарегистрированного пользователя.

С этой целью можно скрывать имена пользователей и защищать пароли.

Скрытие имен пользователей. Прежде всего, следует защитить имена и пароли пользователей. Идентификация пользователя выполняется сопоставлением его имени с конкретным паролем, а не просто назначением пароля. Если злоумышленник не знает имени учетной записи пользователя, он не сможет войти в систему, даже если узнает пароль.

Совет

Измените имена учетных записей, которым предоставлены особенно большие права, например, администраторов Windows NT.

Правила защиты паролей. Пароли следует защищать еще в большей степени, чем имена пользователей. При назначении пароля необходимо следовать некоторым общим пра-

вилам.

Примечание

Заставляя пользователей следовать этим правилам, ни в коем случае не полагайтесь на хорошие личные отношения. Любая правильно спроектированная NOS обеспечивает парольную защиту, контроль повторного использования (reuse cycles) пароля и т.п. Некоторые дополнительные типы программ позволят указывать пароли, которые невозможно применять.

Во-первых, регулярно заменяйте пароли. Это означает, что пароль действителен, скажем, в течение 30 дней, после чего отправляется в "Дом Престарелых Паролей". Кроме того, это означает, что вы обязаны установить правила повторного использования паролей, согласно которым нужно выжидать некоторый период времени, прежде чем можно будет использовать старый пароль. В противном случае половина пользователей будут снова и снова назначать один и тот же пароль, чтобы упростить себе вход в систему. Использование же устаревших паролей рискованно.

Пароли должны быть трудны для отгадывания. Поэтому короткие и благозвучные пароли неприемлемы; кроме того, установите для паролей некую минимальную длину (Microsoft рекомендует не менее 11 символов) и не позволяйте людям использовать ни одно из следующих слов.

- Имя пользователя, его супруги (супруга) либо имена детей.
- Дату рождения.
- Название любимой спортивной команды.
- Слова, так или иначе связанные с работой пользователя.
- Имена домашних животных.

Совет

Немедленно заменяйте все используемые стандартные пароли. Списки стандартных паролей для конкретного оборудования (в том числе пароли BIOS, которые вы можете назначить для компьютера) можно без труда получить в онлайновом режиме (online).

Чтобы затруднить угадывание паролей, вы можете записать их в необычной форме. Например, записывайте пароль задом наперед, придумывайте бессмысленные слова либо вставляйте в них произвольные символы, например, mort$ician (mortician — гробовщик). Кроме того, если ваша NOS и система идентификации способны различать регистры символов паролей, используйте в пароле произвольные регистры букв, скажем, FrOggiE. Наиболее защищенные пароли создаются генератором случайных паролей (random password generator). К сожалению, такие пароли не нравятся пользователям — например, JO%de)(Iwi832 — их трудно запомнить и точно ввести.

Наконец, последнее правило защиты пароля гласит: *никогда не записывайте пароль*. Все наши уловки затрудняют людям корректный ввод их собственных паролей (они имеют обыкновение записывать пароли и приклеивать липучкой к монитору или под клавиатурой). Отбейте у них всякую охоту делать это.

Реализовать данные рекомендации нелегко, особенно потому, что иногда они противоречат друг другу. Нелегко придумывать через каждые 30 дней новое слово из 10 букв. Однако если следовать приведенным рекомендациям, угадать пароль для вашей сети будет весьма нелегко.

Итак, теперь я в безопасности, правда? Пароль, назначенный надлежащим образом, затрудняет *случайный* доступ по вашей учетной записи. Однако он не может предотвратить *намеренную* попытку прорыва в систему и вы по-прежнему не должны допускать посторонних в сеть.

Пароли, которые трудно угадать людям, уязвимы, тем не менее, со стороны *словарной атаки* (dictionary attack), когда специальная программа вводит случайные комбинации симво-

лов в экран входного диалога (login screen), пока одна из них не совпадет с подлинным паролем.

Кроме того, пароли, пересылаемые по сети, могут перехватывать программы-анализаторы (sniffers). Если пароли представляют собой простой текст, оператор программы-анализатора без малейшего труда их перехватит. (Простой текст незашифрован. Подробнее о том, что это значит, вы узнаете в разделе "Шифрование данных".) Если пароли зашифрованы, они, разумеется, тоже потенциально опасны при перехвате, поскольку средства взлома паролей общедоступны (см. ниже).

Идеалы L0pht

Организация, называемая L0pth (да, именно нуль) создала множество инструментов, для испытания средств защиты продуктов в тяжелых режимах. В частности, один из них, называемый L0phtcrack, предназначен для оценки уязвимости шифрования паролей Windows NT.

Суть дела в следующем: Windows NT поддерживает два метода выполнения вызовов/откликов (challenge/response techniques): NTML2 и LM (систему вызова/отклика LAN Manager). Средства идентификации паролей LM весьма уязвимы с точки зрения дешифрования. Проблема заключается в способе, которым намеренно зашумленные (т.е. зашифрованные) пароли разбиваются на части и идентифицируются. Система идентификации LM позволяет при взломе разделять пароли на блоки размером в семь байт. Напротив, система идентификации NTLM намного устойчивее к взлому. Никакой пароль не устоит перед грубыми силовыми методами, однако для взлома системы вызова/отклика NTLM требуется намного больше времени, чем для LM — несколько дней вместо нескольких секунд.

Единственный путь полностью обойти проблемы LM: использовать в сети *только* компьютеры Windows NT, а также установить пакет SP4. (Если используется хотя бы один клиент Windows 95, следует поддерживать систему идентификации LM.) Подробное описание проблемы и возможные решения можно найти по адресам:

```
http://www.l0pht.com/10phtcrack/rant.html
http://support.microsoft.com/support/kb/articles/ql47/7/06.asp.
```

И эти инструменты работают. Введите в L0phtcrack пароль, зашифрованный с помощью технологии LM —программа расшифрует его за несколько секунд (в зависимости от мощности компьютера).

Биометрические устройства и интеллектуальные карты

Для идентификации доступа пользователей в систему иногда используют средства, не требующие ввода паролей. В некоторых сетях с повышенными мерами защиты для идентификации личности используют интеллектуальные карты (smart cards), биометрические устройства (biometric devices) или и то, и другое. Кроме того, такие устройства могут обеспечить защитную аутентификацию (secure authentication) пользователей, которые не приучены обращаться с паролями. Их можно также применять, если защита паролями слишком громоздка, но, тем не менее, необходима.

Медосмотр с помощью системы защиты. *Биометрические устройства* однозначно идентифицируют пользователя на основе некоторых физиологических характеристик, например, отпечатков пальцев или ладони, рисунка сетчатки глаза, "отпечатка" голоса (voice print). Встречаются и другие методы идентификации подобного рода. Главное — предельно упростить ввод пароля в систему. Человеческий мозг может воспринимать пароли длиной не более И символов. Структура же кровеносных сосудов человеческого глаза абсолютно уникальна, а подделать ее весьма трудно. Эту, а также и другие структуры, свойственные только вам, можно

отсканировать и оцифровать, т.е. преобразовать в единицы и нули — точно так же, как модем "переводит" аналоговые данные в цифровые, необходимые для работы компьютера. Затем оцифрованные изображения сохраняются точно так же, как файл со списком паролей. Когда вы предоставляете сканеру отпечатки вашего пальца (глаза, руки, голоса), оригинал сканируется и оцифровывается, а затем сравнивается с образцом, хранящимся в системе. Если соответствие достаточно близкое, система позволяет войти в сеть (или сегмент сети).

До недавних пор биометрические устройства использовались исключительно в правительственных сетях с высшей степенью защиты. Идентификация по отпечатку голоса "страдает" недостатком, обусловленным тем, что голос человека звучит по-разному в зависимости от времени дня и настроения человека. Сканирование сетчатки нередко ведет к ошибкам, если, скажем, глаз человека наливается кровью из-за сенной лихорадки. Поэтому на случай отказа механизма биометрической идентификации следует предусмотреть какой-либо иной код (ID) — иначе вам просто не войти в систему. Система идентификации, которая пылится на полке, никому не нужна.

Последние усовершенствования программных средств распознавания голоса и другие технологии значительно подняли доверие к инструментам биометрической аутентификации (biometric authentication tools). По мере роста надежности эти средства стали все шире применяться для идентификации личности. Тем не менее, пока что они не слишком популярны и главным образом потому, что создают неудобства людям. Возможно, вам повезет, и вы сумеете убедить их в обратном ("Мы установим систему, в которой не надо вводить пароли!!!"). В частности, удобства таких систем в большей мере ощущают люди, далекие от техники. Кроме того, "щадящие" биометрические устройства, вроде сканеров отпечатков пальцев, воспринимаются благожелательнее, чем, например, сканеры сетчатки глаза.

Использование интеллектуальных карт. Все большее число фирм в крупных городах США требуют от служащих обзавестись идентификационными карточками (badges). Федеральное правительство добивается этого целую вечность. С недавних пор этого же требуют частные фирмы и даже общественные школы. Как правило, на идентификационные карточки помещают фотографии владельцев, а также их имена либо иной идентификатор (в особо защищенных картах имена не указывают). Нередко в идентификационных карточках предусмотрена цветовая кодировка, позволяющая охраннику с одного взгляда установить, имеет ли владелец право находиться в данной части здания или местности.

В простейшем случае карточка содержит только фотографию и код, вроде того, что содержится на водительских удостоверениях. *Интеллектуальные карты* (smart cards) помимо этой информации включают своего рода электронную подпись (electronic signature), хранящуюся на магнитной полосе (magnetic strip) карты. Примером интеллектуальной карты может быть кредитная карточка, в которой на магнитной полосе хранится номер вашего счета. Еще один пример, когда ввод данных пользователем необязателен — это запирающая система (gate system). Здесь владелец карточки, чтобы отпереть дверь, должен протянуть ее через цифровой сканер (digital scanner). Независимо от того, должен ли пользователь вводить код либо просто протянуть карточку через щель, при несовпадении введенного кода с записанным в памяти доступ воспрещается.

Примечание

В качестве интеллектуальных карт тоже можно использовать биометрические устройства. Некоторые фирмы производят карты, которые в качестве цифровой сигнатуры используют оцифрованный отпечаток пальцев (digitized fingerprint).

Все мы уже привыкли использовать интеллектуальные карты в качестве кредитных карточек, а также для входа в здание. Кроме того, их постепенно начинают использовать и для доступа в компьютеры и сети. Основные операционные системы оснащают средствами поддержки интеллектуальных карт, а в некоторых они уже реализованы.

Организация прав пользователей

Итак, наконец пользователь, так или иначе, идентифицирован и получил доступ в систему. Это отнюдь не означает, что он автоматически получает все права на доступ к файлам. В любой достаточно защищенной сетевой операционной системе доступ пользователя определяется группой, в которую он входит. Хитрость заключается в использовании преимуществ этой системы путем ограничения прав пользователя на доступ к функциональным средствам, которые ему необходимы. В гл. 10 рассматривались некоторые методы, используемые в серверах Windows NT и NetWare для организации прав пользователей и разрешений. Мы вернемся к этому вопросу.

Домены Windows NT и средство обслуживания Active Directory. Независимо от того, предусмотрена ли в серверах доменная структура или средство Active Directory (Активный каталог), в операционных системах Windows NT и Windows 2000 используются по существу одинаковые методы организации работы пользователей. *Пользователем* (user) называют члена одной или нескольких групп, причем каждой группе назначают *код группы* (Group ID — GID) и предоставляют определенные права. В зависимости от назначенных прав и разрешений, члены данной группы могут читать имеющиеся файлы, создавать новые, использовать сетевые устройства, запускать утилиты администрирования (administration utilities), а также пользоваться многими другими правами и разрешениями, предусмотренными операционной системой. Кроме того, пользователям можно предоставлять индивидуальные права и разрешения, однако каждый пользователь должен входить, по крайней мере, в одну группу.

Примечание

На жаргоне Windows NT действия пользователя, определяются его *правами*, а объекты, к которым он может получить доступ, - *разрешениями*.

Если пользователь входит сразу в несколько групп, имеющих разные права, применяется наиболее полный набор прав (они "суммируются"). Единственное исключение — запрет группе выполнять какое-либо действие (пользователю запрещается исполнять это действие, даже если оно разрешено другой группе, в которую он входит).

Средство обслуживания NetWare (NDS) фирмы Novell. Вместо предоставления прав пользователям и группам, в системе NDS (NetWare Directory Services — средство обслуживания каталогов NetWare) организует их в соответствии с *организационными единицами* (OU — Organizational Unit). Как правило, OU представляет собою группу коллег по работе или одно подразделение фирмы, однако она определена на пользовательской основе, а потому численность OU не ограничена и допускает любую структуру организации.

В отличие от доменной системы Windows NT, система NDS позволяет пользователю одновременно входить в *единственную* OU. Таким образом, чтобы изменить массив разрешений для конкретного пользователя, его следует перевести в другую OU. При последующем входе в систему пользователь получит для работы новый набор разрешений.

Обеспечение секретности хранимых данных

Входная идентификация — это только часть процесса защиты. Действительно, вам совершенно незачем позволять любому вошедшему пользователю просматривать какой угодно сетевой файл. Следовательно, вам предстоит продумать метод организации совместного доступа к файлам (или его отмены). Возможно, для этого придется защитить файлы паролями, а особо важные — зашифровать

.

Методы организации файлов

Чтобы заблокировать пользователям возможность просматривать файлы друг друга, в первую очередь следует надлежащим образом организовать сами файлы. Действительно, намного проще защитить их, предоставив при этом необходимый доступ к ним, если логически сгруппировать файлы и защитить группы. Приведем несколько советов как это можно сделать — возможно, они вам пригодятся.

- Для хранения текущей работы пользователей, назначьте основные каталоги, доступные *только* им.

Совет

Активируйте в пользовательских приложениях опцию автоматического сохранения файлов в основном (корневом) каталоге *пользователя* — это уменьшит число "потерянных" файлов (т.е. файлов, которые пользователь случайно сохранил в стандартном (заданном по умолчанию) или программном каталоге, а теперь не может найти).

- Поместите файлы в отдельные папки, в соответствии с выполняемыми проектами или группами пользователей, но *не собирайте в одном месте* все файлы данных фирмы.
- Без необходимости *не предоставляйте общий доступ* к файлам или папкам. Точно так же не предоставляйте пользователям доступ к общим файлам или папкам, если он не нужен для выполнения их прямых производственных обязанностей.

Для более тонкой настройки системы доступа к общим каталогам можно использовать пользовательские или групповые разрешения. Для облегчения решения этой задачи желательно дополнительно подразделить ресурсы. Единственный недостаток заключается в том, что дополнительная защита затрудняет пользователям доступ к файлам. К сожалению, это неудобство — неизбежный побочный эффект логической защиты (logical security).

Защита файлов паролями

Простейший способ защиты общих сетевых файлов — назначение паролей. С этой целью можно использовать систему защиты паролями (password protection system), встроенную в приложение, либо систему управления доступом (access control system), встроенную в NOS. Защита паролями не слишком надежна, особенно, если доступ к защищенному файлу предоставлен нескольким пользователям, однако она способна отпугнуть праздных любителей почитать чужие файлы.

Примечание

Здесь слишком часто упоминается праздное любопытство. Именно оно - серьезнейшая угроза вашей сети. Она исходит от людей, которые от скуки просматривают различные файлы, чтобы просто посмотреть, что там есть. К счастью, большинству таких людей лень проделывать серьезную работу, чтобы прорваться в защищенный файл.

Защита паролями поддерживается не всеми сетевыми операционными системами — обычно она используется в низкоуровневых (lower-end) NOS, которые не содержат более совершенных средств защиты. Если ваша NOS не поддерживает пароли, но вам необходимо обеспечить дополнительную защиту помимо той, что предоставляется назначением прав пользователям, следует зашифровать данные. Об этом в следующем разделе.

Шифрование данных

Шифрование данных является более надежным методом защиты файлов. Шифрованием называют любой метод искажения текста с помощью специального алгоритма, с тем чтобы исходное сообщение могли понять только те люди, которые знают данный метод шифрования (фактически *ключ* (key) к шифру). Используемый алгоритм может быть совершенно прост, например замена одной буквы другой, которая отстоит от нее в алфавите на три позиции (см. примечание далее), однако можно использовать и чрезвычайно сложные методы. Как правило, в цифровой связи используют сложные методы, поскольку вычислительная мощность компьютера позволяет применить весьма сложные алгоритмы даже к простому тексту.

Примечание

Простым текстом называют любой текст, который можно прочитать и понять без использования специальных средств.

Что такое кодирование и шифрование

Кодирование и шифрование в равной мере применимы для того, чтобы предотвратить чтение текста без специальных средств. Тем не менее, это совершенно разные понятия.

В *шифровании* для сокрытия содержимого используют специальные алгоритмы. В кодировании с этой же целью в исходном тексте заменяют целые слова или даже фразы. Например, вы можете зашифровать простой текст "HELLO" (привет) так, что он будет читаться "JGNNQ". Здесь использован следующий алгоритм шифрования: "Возьми каждую букву и замени ее буквой, которая отстоит от нее на три буквы в алфавите". Если же в исходном сообщении каждое слово "HELLO" заменять словом "ZANY" (дурак), мы имеем дело с *кодированием.*

До тех пор пока ключ держится в тайне, прочесть кодированное сообщение намного труднее, чем шифрованное. Зашифрованное сообщение можно взломать либо грубыми силовыми методами, либо с помощью специальных приложений, созданных на основе принципов криптографического анализа. Эти приложения используют для анализа образцов зашифрованного текста. Кодирование же сообщения, как правило, не выполняется в соответствии с какой-либо (очевидной) логикой, а потому и не поддается систематическому анализу. Так, слово "HELLO" можно заменять словом "PIGGY" (поросенок) либо "MY MOTHER WEARS ARMY BOOTS" (Моя мать носит солдатские сапоги). Компьютеры работают с числами, а не буквами, поэтому, как правило, компьютерные программы позволяют зашифровать информацию. Поскольку же скорость вычислений компьютера достаточно высока, можно использовать сложные ключи, весьма устойчивые к взлому.

Методы (алгоритмы) шифрования. Известны два основных алгоритма шифрования.

- Симметричное шифрование (symmetric encryption).
- Асимметричное шифрование (asymmetric encryption), называемое также шифрованием открытым ключом (public key).

При *симметричном шифровании* для шифрования и дешифрования простого текста применяет один и тот же алгоритм. Симметричное шифрование великолепно работает, если файлы использует один пользователь, и *только он* знает алгоритм шифрования. Если же файл совместно используют несколько человек, надежность симметричного шифрования становится проблематичной, поскольку все они должны знать один и тот же ключ. Скажем, Джейн (Jane) может зашифровать данные для Джей (Joe), но обе должны знать ключ, который блокирует и деблокирует данные. Если же Джейн работает в Техасе, а Джей — на Аляске, как передать ей ключ дешифрования? Письма могут прочитать, телефонные разговоры — подслушать, а если передать с оказией, посланца могут просто подкупить. Таким образом, эта система небезопасна.

Одно из возможных решений — кодовые книги (code books) со списком *шифров* (ciphers) (алгоритмов шифрования), которые можно использовать заранее обусловленным способом. Например, по средам применяется шифр "A", так что если вы получили сообщение, подготовленное в среду, вы знаете, что должны использовать для дешифрования ключ "A". Основной недостаток кодовых книг, как обнаружили обе воюющие стороны еще в первую мировую войну — возможность их кражи. Похищенная кодовая книга бесполезна. И это не единственный недостаток симметричного шифрования. Так, если отношения между двумя людьми еще не наладились, отсутствие предварительно заданных ключей делает их общение излишне громоздким.

Примечание

Хотя стандартом шифрования данных (DES - Data Encryption Standard), разработанным федеральным правительством, предусматривается использование симметричного шифрования, он неприемлем для секретной связи (classified communications).

Шифрование с открытым ключом (public key encryption) — сегодня фактически стандартный метод шифрования данных для передачи по открытым каналам связи. В этом методе для шифрования и дешифрования используют два отдельных ключа, индивидуальных для каждого пользователя. Один ключ — открытый (public key), второй — личный (private key). Для шифрования простого текста при передаче применяют открытый ключ. Чтобы дешифровать полученный текст, получатель использует свой личный ключ. Нередко открытые ключи распространяют как часть электронной подписи (e-mail signature) данного лица. Понятно, что личные ключи следует держать в секрете.

Примечание

Среди известных криптографических систем, использующих открытые ключи, отметим следующее.
Elgamal - названа по имени создателя Тахо Элджимела (Taher Elgamal).
RSA - названа по именам создателей Рона Ривеста (Ron Rivest), Ади Шамира (Adi Shamir) и Леонарда Адлемана (Leonard Adleman).
Diffie-Hellman -тоже назван по имени создателя.
DSA (Digital Signature Algorithm - алгоритм цифровой подписи). Разработан Дэвидом Кравицем (David Kravitz), который, очевидно, не заботился о своем увековечении.

Особенностью этой схемы является то, что открытый и личный ключи настроены друг на друга. Например, чтобы зашифровать данные, для Дорис (Doris), вам следует использовать ее открытый ключ; а Дорис, чтобы дешифровать их, должна использовать личный ключ. Всеобщие открытые ключи не применяются. Кроме того, открытый и личный ключи не связаны друг с другом никоим образом. Иными словами, зная один ключ, вы не сумеете догадаться или вычислить второй.

В качестве примера широко известной системы открытых ключей (public key system) можно назвать PGP (Pretty Good Privacy — надежная конфиденциальность), изобретенную Филом Циммерманом (Phil Zimmerman). Строго говоря, PGP (кстати, широко используемую для связи по Internet, а также для защиты собственных данных), нельзя полностью отнести к системам с открытым ключом. В нее добавлен дополнительный симметричный компонент, называемый *сеансовым ключом* (session key), который уникален для каждого сеанса шифрования (encryption session). Сеансовый ключ — это число, генерируемое при случайных перемещениях мыши или вводе с клавиатуры.

Процесс шифрования с помощью системы PGP выполняется примерно так.

1. Производится сжатие простого текста, который необходимо зашифровать.
2. Алгоритм PGP создает сеансовый ключ.
3. Сжатый простой текст шифруется сеансовым ключом.
4. Сеансовый ключ шифруется открытым ключом.

Когда такой "пакет в пакете" поступает получателю, прежде всего он дешифрует сеансовый ключ (используя с этой целью личный ключ), а затем с его помощью дешифрует и разворачивает (decompress) простой текст. Получив от того же отправителя следующий пакет, получатель использует те же открытый и личный ключи, *новым* же является только сеансовый ключ.

Что нужно шифровать? Все данные - пароли, текст или другая информация, могут и *должны* шифроваться — по крайней мере, на время передачи по общедоступной сети, а иногда и в другое время. Шифрование — весьма удобный метод засекречивания локально хранящихся личных файлов, особенно если компьютером пользуются сразу несколько лиц. Чем больший ущерб может нанести рассекречивание информации, тем больше оснований использовать шифрование для ее защиты.

В частности, пароли *никогда* не должны передаваться по сети или сохраняться как простой текст, хотя иногда встречается и такое. (В конце 1998 г. внутренняя сеть Стэндфордского университета была кем-то взломана с помощью программы-анализатора (sniffer), и на протяжении примерно трех недель взломщик перехватил около 4500 паролей, посланных по сети в виде простого текста.) Чтобы ваша сеть хотя бы отдаленно соответствовала требованиям сетевой защиты, следует шифровать пароли, пересылаемые на сервер входной регистрации (authentication server). Даже система вызова/ отклика LM лучше, чем ничего. Если не использовать шифрование, то для расшифровки паролей злоумышленнику не понадобится даже L0phtcrack или его эквивалент. Любую NOS, которая не поддерживает какой-либо метод шифрования передаваемых паролей, вообще нельзя назвать защищенной.

Примечание

Заметим: выбор методов шифрования паролей, передаваемых для идентификации пользователя (если он есть вообще) не слишком обширен. Например, в Windows NT можно выбрать одну из двух опций шифрования паролей: LM (для клиентов Windows 9.x) и NTLM2 (для клиентов Windows NT).

Защита удаленного доступа

Если сеть открыта для удаленного доступа по телефонным линиям, то ее защита усложняется. В самом деле, если к локальной сети возможен только локальный доступ, то достаточно поставить охрану у входа в здание и тем самым избежать проникновения злоумышленников. Кроме того, когда вы идете по офису, вы можете увидеть всех, кто работает на компьютерах и понять, чем они заняты. Однако с удаленным доступом так не получится — все, что вы в состоянии узнать о пользователе, который "удаленно" вошел в систему — это используемая им учетная запись. Но она ничего не говорит о том, кто ее использует *фактически*. Кроме того, головную боль вызывает и этот длинный, абсолютно ничем не защищенный кабель, который соединяет удаленного пользователя с сетью. Если учесть, что вы не в состоянии предотвратить прослушивание общедоступной телефонной линии в любой точке на всем ее протяжении, то следует позаботиться о каком-либо методе защиты от перехвата злоумышленниками паролей путем подслушивания телефонных сообщений.

Защита сеансов протоколами CHAP и PAP

Основная задача защиты системы удаленного доступа — гарантировать доступ в сеть только зарегистрированным пользователям. Поскольку при удаленном доступе в качестве протокола линии связи чаще всего используют PPP (Point-to-Point Protocol - протокол узел-узел), в этом разделе мы рассмотрим два защитных средства, предусмотренные этим протоколом.

- CHAP — Challenge Handshake Authentication Protocol - протокол аутентификации по квитированию вызова.
- PAP — Password Authentication Protocol - протокол аутентификации по паролю.

В обоих протоколах защиты для идентификации пользователя применяются секретные файлы (secrets file), однако в каждом протоколе — по-разному.

Примечание

В протоколе PPP не требуется идентификация - она устанавливается по вашему выбору. Защита включается после того, как логический канал уже создан, но еще не открывался.

Принцип работы протокола PAP. PAP менее надежен, чем протокол CHAP, и используется теми клиентами, которые не поддерживают CHAP. Когда клиент пытается инициировать сеанс связи с сервером удаленного доступа, то посылает на сервер имя и пароль, указанные в учетной записи. (Пароль может быть зашифрован.) Сервер сравнивает имя и пароль пользователя с данными, указанными в его секретном файле. При совпадении клиенту предоставляется доступ. В противном случае соединение прерывается. К недостаткам метода можно отнести то, что пароль фактически пересылается в соответствии с протоколом PAP и может быть перехвачен. Кроме того, метод неустойчив и по отношению к повторным попыткам несанкционированного доступа.

Принцип работы протокола CHAP. Недостатки протокола PAP привели к разработке другого протокола защиты — CHAP. Процесс идентификации пользователя по протоколу CHAP выглядит несколько сложнее. Когда клиент пытается инициировать сеанс связи, сервер посылает клиенту *вызов* (challenge) — случайным образом сгенерированное число — а также имя сервера, которому следует ответить. Клиент отвечает за надлежащее шифрование вызова и отправление правильного отклика. С этой целью клиент просматривает собственный секретный файл, записанный как простой текст, чтобы найти отклик на полученный вызов. Когда клиент находит корректный отклик, он сопоставляет результат поиска с исходным вызовом, шифрует всю строку и отсылает серверу зашифрованную строку. Затем сервер расшифровывает пакет и сопоставляет вызов и отклик с собственной секретной базой данных (secrets database). При совпадении данных клиент идентифицируется и запускается сеанс работы. В противном случае сеанс прерывается (в некоторых реализациях сеанс *перемаршрутизируется* (rerouted) на новый, но с крайне ограниченным сетевым доступом). Преимущество этой схемы над протоколом PAP заключается в том, что по сети не пересылается секретная информация и, следовательно, ее перехват и последующий несанкционированный доступ к ней невозможны.

Еще одно преимущество протокола CHAP: процесс идентификации не обязательно завершается первоначальной идентификацией (original identification). Через некоторое время сервер может послать клиенту еще один вызов, чтобы убедиться, что за этот период сеанс связи не перехвачен злоумышленником. Если клиент не в состоянии в любой момент времени возвратить корректный отклик, сеанс прерывается.

Установка протокола RADIUS

Протоколы CHAP и PAP могут использовать не все клиенты. Некоторые из них связываются с сетью с помощью входов (login) в серверы Telnet или UNIX. Чтобы предоставить централизованный сервер входной регистрации (centralized authentication server) клиентам различных типов, разработан протокол RADIUS (Remote Authentication Dial-In User Service — служба удаленной аутентификации пользователей по телефонным линиям). Этот протокол используют для передачи информации об аутентификации (authentication), установления подлинности (authorization) и конфигурации между сервером доступа к сети (которому необходимо идентифицировать сеансы удаленного доступа) и сервером входной регистрации общего

пользования (shared authentication server). Таким образом учетные записи разных типов можно сохранять в единственной базе данных учетных записей.

Когда для удаленного доступа к сети клиент использует протокол RADIUS, то начальное соединение устанавливается с сервером доступа к сети. Этот сервер передает идентификационную информацию от клиента на сервер входной регистрации (authentication server), который либо разрешает, либо запрещает соединение. Кроме того, он указывает серверу доступа к сети тип соединения, необходимый конкретному клиенту (т.е. входы (login) Telnet, PPP, SLIP или UNIX).

Что можно сказать о защите данных, которыми обмениваются серверы доступа к сети исерверы входной регистрации? Взаимодействие этих серверов напоминает работу протокола CHAP. Идентификация выполняется с помощью общей секретной базы данных (share secrets database), поэтому их пароли никогда не пересылаются по сети. Если метод входа в сеть удаленного клиента требует, чтобы удаленный пользователь предоставил пароль для входа в сервер доступа к сети, то пароль шифруется с помощью криптографической системы шифрования открытым ключом RSA, а уже затем пересылается (rerouted) между серверами доступа к сети и входной регистрации.

Ограничение пользователей частью сети

После идентификации и входа в сеть удаленного пользователя, он все еще не всегда способен свободно получать доступ к сетевым ресурсам. Многие сетевые администраторы ограничивают доступ к сети удаленным пользователям, предоставляя им более ограниченные разрешения, чем пользователям при локальном входе.

В каком объеме следует предоставлять удаленный доступ? Часто удаленный доступ ограничивают сервером входной регистрации. Чтобы изолировать удаленных пользователей от уязвимой информации (sensitive information), разрешите им использовать только средства удаленного доступа — электронную почту, может быть, некоторые файлы (только для чтения) — но держите их подальше от основной сети (main network). Некоторые серверы удаленного доступа — скажем, система удаленного доступа Windows 98 — вообще позволяют делать только это. Другие серверы удаленного доступа, например Windows NT, позволяют указать, имеет ли пользователь право "просматривать" всю сеть либо должен ограничиться только ресурсами сервера.

Конфигурирование привязок. Если вам необходимо предоставить кому-либо лишь частичный доступ к сети, вы можете сделать это, установив в каждой части сети только необходимые протоколы. Как вы помните из гл. 3, каждый протокол должен быть "привязан" к части сетевого оборудования либо к определенной программе обслуживания — только тогда он будет доступен этому оборудованию или программе. Такой способ конфигурирования называют привязками (bindings). Другими словами, вы не можете перераспределить трафик в ту часть сети, в которой не установлен соответствующий протокол.

По практическим соображениям, пользователям удаленного доступа предпочтительнее установить протокол TCP/IP. Поэтому если вам нужно предоставить удаленным пользователям доступ к сети, и в то же время не позволить им пользоваться всем тем, что в ней есть, отмените привязку протокола TCP/IP для тех серверов, доступ к которым нежелателен. Не полагайтесь на установки системы защиты или процедуры идентификации — в этом случае вы просто не сможете воспользоваться ими, поскольку в данном сегменте протокол TCP/IP не поддерживается. Кстати, это же справедливо и по отношению к обычным пользователям локальных сетей.

Мониторинг системы

Наконец, последняя мера защиты, которую настоятельно рекомендуется соблюдать — ведите журнал (log) доступа в сеть. Любая "приличная" NOS поддерживает те или иные средства ведения журнала системы защиты (security logging). Например, в Windows NT с этой целью предусмотрено средство Event Viewer (просмотр событий). Журнал позволяет установить, кто и что делает в сети. Кроме того, его можно использовать для мониторинга успешных и неудачных попыток входов в систему либо доступа к общим файлам и папкам на отслеживаемом сервере.

С практической точки зрения вам нужна только свежая информация — от просмотра чрезмерного числа старых записей толку мало. Поэтому исключайте устаревшие записи (но сохраните их для справок в текстовых файлах либо электронных таблицах) и просматривайте журнал примерно раз в неделю. Особое внимание обращайте на многократные повторные попытки доступа — они могут указывать на намерение взлома сети или нелегального доступа к защищенным файлам.

Сохраняйте файлы журналов!

Если вы так организовали ведение вашего журнала системы защиты (security logging), чтобы по истечении некоторого срока (скажем, недели) старые записи стирались, *обязательно сохраните перед стиранием старые записи*. Не каждую неделю вам доведется обнаружить злоумышленника. Когда же вы действительно "засечете" подозрительную активность, вероятно, вам захочется просмотреть, использовалась ли ранее данная учетная запись и кому предоставлялся доступ к данным объектам.

Предположим, например, 17 мая вы обнаружили подозрительную активность, наблюдавшуюся в течение прошлой недели. Некто пытался войти в почтовый сервер Microsoft Exchange 5.5. Злоумышленник захватил средства поиска и таким образом оставил прочих пользователей без них. Иными словами, никто другой, кроме него, уже не сможет читать книгу глобальных адресов (global address book). Пользователи начинают жаловаться на неполадки в почтовом сервере. Вы проверяете протокол защиты (security log) и, несомненно, обнаруживаете изменения разрешений. Пока что все нормально — вы быстро решили проблему.

Однако задумайтесь на минутку: каким же образом злоумышленник вошел в сервер? И с чем вы разделались: с первой попыткой незаконного доступа или продолжением предыдущей? Вы знаете, что 30 апреля один из серверов UNIX вашей сети уже подвергался попытке незаконного доступа, и вы тогда же блокировали соответствующую учетную запись. Однако некоторые пользователи вашей сети с низкоуровневыми административными правами располагают двумя учетными записями с одинаковым именем и паролем. Одна используется для доступа в домен Windows NT, а другая — к серверу UNIX. (Между прочим, это очень глупо — предоставлять две учетные записи. Причины вы поймете позже.) Может быть, для незаконного доступа в Exchange Server использована блокированная учетная запись UNIX? Если вы уже стерли старые журналы по прошествии 7 дней, вам не найти ответа на этот вопрос.

Файлы журналов должны быть небольшого размера, и, тем не менее, стирание старых записей с интервалом около недели — верное решение. Однако в целях безопасности рекомендуем сохранять старые журналы в виде электронных таблиц или текстовых файлов.

Поддержка доступа к данным

Разумеется, сетевые данные следует скрывать от разных бездельников. Однако, и прежде всего, они должны быть доступны "нормальным" пользователям. В вашу задачу входит

также предотвращение отказов в обслуживании и утраты данных из-за случайного или злонамеренного удаления всех (или части) данных.

Предотвращение отказов в обслуживании

Отказом в обслуживании (DOS — Denial Of Service) называют любые условия, в которых некоторая часть (или части) сети становится недоступной. Как правило, это результат умышленного использования программы, генерирующей настолько много "бессмысленных данных", что они начинают препятствовать нормальной работе сети. Можно привести такие примеры.

- Генерирование бессмысленных данных и направление их на почтовый сервер не позволяет войти в него законным пользователям.
- Захват всех циклов работы процессора сервера.
- Повреждение сервера.
- Многократное направление команды Ping на сервер создает значительный шум в сети, поскольку серверу приходится отвечать на эти команды.

Итак, если вы не можете использовать вашу сеть, поскольку кто-то уже выполняет подобные действия, значит вы подверглись DOS-атаке.

Хорошо известны два типа DOS-атаки: Teardrop и Land. В обоих случаях для вмешательства в работу сети, подключенной к Internet, используются недостатки протокола TCP/IP. Использовав один из методов атаки, удаленный пользователь может разрушить уязвимый сервер (vulnerable server). Так, во время Land-атаки атакующий пользователь может посылать повторяющиеся широковещательные сообщения на маршрутизатор, подсоединенный к локальной сети Ethernet. Затем маршрутизатор будет повторять этот запрос во всей локальной сети, таким образом перегружая трафик.

Примечание

Известно несколько типов Land-атаки, однако всем им присуще использование *фальшивого* (spoofing) IP адреса источника.

Большинство DOS-атак выполняется из компьютеров, находящихся вне локальной сети, поэтому для защиты от них наиболее эффективны *брандмауэры*. Так называют аппаратный или программный маршрутизатор, установленный между вашей внутренней и остальной сетью - общедоступной или частной (private). Этот маршрутизатор путем входной фильтрации (ingress filtering) проверяет пакеты и отбрасывает неприемлемые. Как показано в гл. 14, некоторые средства обслуживания для внесения сообщений в список используют порты. Например, в SNMP применяют порт с номером 161. В зависимости от типа сети, можно заблокировать внешний доступ к управляющим портам (administrative ports), с тем чтобы управлять маршрутизатором только изнутри локальной сети.

Примечание

На практике можно сначала заблокировать все порты, а затем открывать их только по мере необходимости. Таким образом вы можете обеспечить начальную защиту сети. Кроме того, вас будут считать отличным парнем, который предоставляет доступ к ресурсам, а не сквалыгой, который отнимает ресурсы.

Чтобы гарантировать корректную работу брандмауэра, его программное обеспечение следует регулярно обновлять пакетами, выпускаемыми производителями, для исключения "уязвимых мест".

Совет

Обязательно отслеживайте пакеты, которые отбрасывает ваш брандмауэр, если их характер позволяет заподозрить намеренные попытки взлома сети.

Удаление данных

Когда вы подвергаетесь DOS-атаке, то на первых порах бывает трудно сориентироваться в обстановке. С одной стороны, сеть просто замедляет или прекращает работу, и вы не в состоянии немедленно найти причину, с другой — исчезновение данных обнаружить несложно. Следовательно, чтобы поддерживать доступность данных, следует убедиться в наличии их архивных копий и недоступности для рядовых пользователей разрушающих утилит (destructive utilities).

Архивируйте!

Первый "рубеж" защиты от потери данных заключается в постоянном создании резервных копий. Подробнее различные стратегии архивирования, а также другие меры защиты рассматриваются в разделе "Восстановление после аварий".

Скрывайте разрушающие утилиты

До повсеместного распространения операционной системы Windows, сокрытие разрушающих утилит не представляло труда. Так, если вы не хотели, чтобы кто-нибудь использовал утилиту `FORMAT` и разрушил свой жесткий диск, можно было переименовать эту утилиту (как и утилиты `DELETE` или `DELTREE`). В качестве дополнительной защитной меры можно было использовать атрибут `-h`, который скрывает файлы так, что они не отображаются в списке команды `DIR`. Для практического применения вам следовало знать, какие инструменты и под какими именами там находятся, и только тогда вы смогли бы воспользоваться ими. Это удерживало уволенных служащих от ввода команды **`DELETE C:`** в последний день работы с целью уничтожения учетных файлов либо от случайного форматирования жесткого диска вместо гибкого.

Это было счастливое время! Теперь же "смертоносные" инструменты находятся на каждом рабочем столе, а удалить их оттуда — непросто. Для пользователей, применяющих системы двойной загрузки Windows NT/ Windows 95/98 есть даже новая опасность — команда CONVERT. На первый взгляд она совершенно безобидна. Это инструмент для конвертирования томов FAT в тома NTFS, что позволяет более производительно использовать дисковое пространство крупных дисков, а также дополнительные средства защиты, отсутствующие в FAT. Конвертирование не затрагивает данных, хранящихся на диске, поэтому инструмент кажется безвредным. Единственный недостаток его заключается в том, что Windows 95/98 не в состоянии читать тома NTFS, а результаты работы утилиты `CONVERT` необратимы. Чтобы сделать тома NTFS снова видимыми в Windows 95/98, можно сформатировать жесткий диск обратно в файловую систему FAT и восстановить данные, уничтоженные форматированием.

Совет

Хотя Windows NT 4 (и старшие версии) не могут читать тома FAT32, которые поддерживаются Windows 95 OSR2 и Windows 98, не беда, если диск с FAT на компьютере с двойной загрузкой конвертируется в файловую систему FAT32. Существует инструмент, называемый "FAT32 for Windows NT", позволяющий Windows NT 4 свободно читать тома FAT32. Его можно загрузить с узла www.sysinternals.com. Установите этот инструмент - и тома станут доступными.

Если ваши клиенты используют Windows и сервер IE4, тогда инструменты *действительно* трудно удалить, поскольку броузер интегрирован с интерфейсом File Manager (диспетчер файлов). Если вы используете IE4 и обладаете хорошими навыками работы на компьютере, то уже поняли, что сможете просмотреть содержимое любого логического диска вводом имени этого диска. (Фирма Netscape не предусмотрела просмотр локальных дисков с помощью броузера.) Если вы уже сделали это, интерфейс изменяется так, что открывается доступ ко всем инструментам управления файлами (file management tools), в том числе и к упомянутым выше инструментам форматирования и удаления.

Что можно сделать в этом случае? Во-первых, можно использовать набор системных правил (system policies), рассмотренный в гл. 14. Они ограничивают число приложений, которые могут запускать пользователи сети. (Между прочим, это означает также блокировку команды Run (Выполнить) меню Start (Пуск), а также блокировку Explorer (Проводник), да и вообще удаление любого средства пользовательского интерфейса, которое дает возможность пользователям открывать запрещенные приложения.) Если просмотр пользователями их логических дисков нежелателен, не используйте IE4 и его позднейшие версии. Ограничьте доступ к дискам и держите под рукой их архивные копии на тот случай, если кто-нибудь по ошибке отформатирует не тот диск.

Физическая защита

Для защиты сети очень важно установить разрешения на доступ и систему идентификации пользователей. Другие вопросы защиты связаны с возможностью доступа не только к *логическим*, но и к *физическим* компонентам сетевого оборудования.

Защита серверов

Защита серверов выполняется не всегда, но достаточно часто. Особенно заботятся об этом крупные фирмы, устанавливая серверы в отдельных запертых комнатах и предусматривая специальные меры по их бесперебойному функционированию.

Изоляция серверов

Самый надежный метод защиты серверов — установка в закрытом помещении, причем иногда за двумя дверями. Чтобы исключить необходимость замены замков при смене персонала, для защиты доступа к серверным помещениям можно использовать электронный кодовый замок.

Установка серверов взаперти весьма эффективна, хотя и обходится недешево. Во-первых, она не позволит злоумышленникам приблизиться к серверу: они не сумеют выполнять задачи сетевого администрирования, либо просто-напросто красть жесткие диски. Во-вторых, уменьшает вероятность случайного повреждения сервера, что вполне возможно, если персонал постоянно ходит мимо него. Действительно, возле сервера положено находиться исключительно штату информационного отдела (IS).

Устранение средств физического останова сервера

Если вы не в состоянии содержать сервер взаперти, все же можете защитить его, заблокировав физические средства останова - кнопку Reset (Перезапуск) или выключатель ком-

пьютера (на компьютерном жаргоне он называется Big Red Switch — Большая красная кнопка). Разумеется, если это действительно необходимо, компьютер можно выключить, просто перерезав кабель питания, однако это небезопасная и "грязная" работа.

Весьма вероятно, что вам понадобится заблокировать инструменты отключения на этапе входного диалога (login screen), если, конечно, он есть вообще. В самом деле, сервер невозможно отключить, если предварительно не войти в него. Конечно, это затруднит его перезагрузку, если она действительно понадобится, однако в этом случае никто не спутает действующий сервер с испытательным (test server), и не выключит его во время работы пользователей с открытыми файлами — нечто подобное случилось на моих глазах несколько лет назад.

Защита от электронного шпионажа

Если вы все еще не слишком напуганы возможностью взлома вашей сети, сообщим вам, что существует также возможность электронного шпионажа (electronic surveillance). Вероятность ее невелика — большинство людей не собираются взламывать вашу систему. Однако если вы работаете с данными, которые привлекают внимание подобного рода, следует принять профилактические меры — опасность достаточно реальна.

Приходилось ли вам видеть кинофильм, в котором автофургон, набитый людьми, подкатывает к дому и перехватывает электромагнитные сигналы? Существует несколько типов электронного шпионажа. Один из них называют *бурный натиск* (tempest attack). Хорошо оснащенные системные кракеры (system crackers) могут перехватить электромагнитное излучение ваших компьютеров и таким образом раскрыть ваши пароли и сообщения. Можно также перехватить электромагнитное излучение, генерируемое вашим монитором, и восстановить изображение на его экране. (Этого можно избежать, если использовать мониторы с пониженным уровнем излучения, но устаревшие модели в этом отношении уязвимы.)

Что вы можете предпринять? Самый эффективный путь избежать подобной "атаки" — хороший (и большой) экран, не пропускающий электромагнитное излучение за пределы помещения или здания, в котором оно генерируется. Для экранирования комнаты либо оборудования можно использовать технологию экранирования TEMPEST. В основном она используется правительственными агентствами и подрядчиками Министерства обороны. Если вы действительно обеспокоены угрозой электронного шпионажа, можно воспользоваться коммерческим вариантом этой технологии. В ней отсутствуют разнообразные дополнительные средства полной версии, однако и она обеспечивает неплохую защиту.

Примечание

TEMPEST (буря) - это секретное кодовое имя (classified code name), а не акроним.

Если вы не можете позволить себе использовать TEMPEST, можно воспользоваться некоторыми простейшими контрмерами. Разумеется, абсолютной защиты не существует, однако вы можете, по крайней мере, затруднить перехват кондуктивных электромагнитных помех (EMI — Electro-Magnetic Interference) от вашего компьютера или сети.

Используйте малошумящие компьютеры (quiet computers). С точки зрения интенсивности электромагнитных излучений конструкция всех компьютеров должна соответствовать определенным правилам федеральной комиссии связи (FCC). Тем не менее, любой компьютер — это источник электромагнитных волн. Компьютеры, сертифицированные для домашнего пользования (класс B), излучают меньше EMI, чем те, что предназначены для производства (класс A), поэтому используйте компьютеры класса B. Более того, не эксплуатируйте компьютер со снятой крышкой и не снимайте заглушки со свободных слотов. Это полезно еще и потому, что в этом случае вентилятор компьютера работает эффективнее.

Если же вы всерьез озабочены электромагнитным излучением, поместите компьютер в "клетку Фарадея". Это устройство не пропускает электромагнитные волны и, следовательно, они не могут быть перехвачены шпионским оборудованием.

Экранируйте ваши кабели либо используйте кабели, не излучающие передаваемый

сигнал. Как уже было сказано в гл. 1, медные провода, из которых состоит кабельная система сети — это, по сути, просто огромная антенна. Чтобы не позволить ей показать свою истинную природу, провода экранируют. Чем лучше экранирование, тем ниже уровень излучаемых (и принимаемых) сигналов. В этом смысле наилучшую защиту от электронного шпионажа обеспечивают оптоволоконные кабели, поскольку они вовсе не излучают сигнал. Конечно, они кабели уязвимы к перехвату с помощью отводов, однако это уже требует *физического* доступа к кабелю.

Примечание

Случалось ли вам ненароком подслушать телефонный разговор вашего соседа по бесшнуровому (cordless) телефону? Точно так же, когда вы используете беспроводную сеть, следует шифровать все передаваемые данные, если вам вообще необходима защита.

Разумеется, сетевые кабели — не единственный потенциальный источник помех. Защищайте фильтрами еще и силовые кабели, а также телефонные провода.

Если вы хотите оценить интенсивность излучения помех вашей сетью, возьмите портативный радиоприемник, рассчитанный на прием сигналов с амплитудной модуляцией (AM), и пройдитесь по офису, поднося приемник к кабелям и компьютерам. В идеальном случае, когда вы подносите приемник близко к какому-либо компоненту сети, вы не должны услышать значительного усиления шума сверх обычных помех.

И, наконец, не принимайте все это близко к сердцу. Маловероятно, чтобы кто-нибудь шпионил за вами подобными методами. Некоторые меры, предлагаемые здесь (вроде клетки Фарадея), совершенно излишни для большинства читателей этой книги. И все же, сеть с низким уровнем помех — отличная штука.

Защита от вирусов

Последний элемент сетевой защиты, которую мы рассмотрим в этой главе, относится к вирусам. С технической точки зрения *вирусами* обычно называют бесконечно исполняемые модули (self-perpetuating executables), которые тайно заносятся в ваш компьютер. В более общем смысле вирусом называют *любую* бесконечно исполняемую злонамеренную программу (malicious program). Для простоты я буду придерживаться последнего определения, потому что не собираюсь отдельно обсуждать атаки червей (worms) — вредных, но *не* бесконечно исполняемых программ, а также троянских коней (Trojan Horses).

Берегитесь вирусов!

Существует множество злонамеренных программ (malicious codes), которые не способны к бесконечному исполнению и поэтому, строго говоря, не относятся к вирусам. Тем не менее, они весьма опасны и нежелательны. В 1998 г. один из злонамеренно исполняемых модулей (malicious executable — ME), называемый BackOrifice, вызвал немалый шум в прессе. Эта программа при попадании в компьютер Windows 95/98 позволяет злоумышленнику дистанционно управлять компьютером по Internet. Существует несколько менее известная ME-программа, чем BackOrifice, которую называют NetBus, работающая в компьютерах Windows NT.

Вам еще не страшно? Есть и другие возможности, включая аплеты Java, спроектированные для повреждения броузеров, компоненты ActiveX, представляющие собой любую исполняемую программу, а также невинные файлы с расширением .EXE - фактически пакетные файлы, форматирующие ваш загрузочный диск (boot drive).

Из всего этого следует: не запускайте приложения из неизвестного источника. Даже если это не вирус, оно все равно может испортить вам весь день.

Какое бы определение вы не использовали, присутствие вирусов в компьютере или сети совершенно нежелательно. Даже если они не относятся к явно разрушительным средствам, вирусы раздражают, вмешиваясь в вашу работу и потребляя ресурсы, которым можно найти лучшее применение. Один мой друг — отошедший от дел хакер-кракер — однажды рассказал мне, что создатели вирусов не пользуются уважением даже среди "черных шляп" (black hat), т.е. преступных или, по меньшей мере, нелегальных членов сообщества хакеров. Как поведал мой друг, если вы занимаетесь программированием и хотите чем-либо похвастать, создайте лучше полезную программу (например, WinZip) и сделайте ее всеобщим достоянием.

Единственная польза, которую вирусы приносят обществу, заключается в том, что держат на плаву бизнес гг. Нортона (Norton), доктора Соломона (Dr. Solomon) и других творцов антивирусных программ. Однако, по моему мнению, это недостаточное оправдание для их разработки.

Типы вирусов

Вирусы образуют весьма неоднородную группу. Различные вирусы вредят по-разному, а метод их атаки зависит от их типа. Тем не менее, большинству вирусов присущи такие общие элементы.

- Воспроизводящийся элемент (червь).
- Полезная нагрузка (payload).
- Логическая бомба (logic bomb), определяющая условия, при выполнении которых должна запускаться полезная нагрузка.
- Метод маскировки (троянский конь).

Данные элементы позволяют вирусу размножаться, запускать свою небольшую подпрограмму (какой бы она ни была) и маскировать себя так, чтобы он смог сделать свою грязную работу. Не во всяком вирусе содержатся все перечисленные выше компоненты. У "честного" троянского коня, который прикидывается экранной заставкой, а затем стирает содержимое жесткого диска, мало шансов размножиться. Точно так же просто работающий червь, создавая множество собственных копий, пожирающих системные ресурсы, не всегда замаскирован.

Кроме того, вирусы можно характеризовать по операционной среде, которую они предпочитают. Если вирус присоединяется к другой программе, его называют *паразитным* или *программным* вирусом. Если же вирус в основном присоединяется к загрузочному сектору диска с данными, его называют *загрузочным (или бутовым) вирусом* (boot sector virus).

Примечание

Некоторым вирусам присущи черты как программного вируса, так и загрузочного.

Единственный элемент, присущий всем вирусам — исполняемый модуль (executable element) какого-либо типа. Вирус — это программа. Следовательно, файл ASCII (скажем, сообщение электронной почты) не может быть вирусом. Конечно, вирус можно отослать как вложение в сообщение электронной почты, и если вы будете настолько неосторожны, что автоматически запустите все вложения сразу по их поступлению, вы станете "рассадником" вирусной инфекции. Однако повторяем: само по себе сообщение электронной почты не может быть вирусом — это просто невинный наблюдатель.

Программные вирусы

Программные вирусы начинают свою работу с инфицирования обычных файлов программ, в том числе и тех, что используются самой операционной системой. При запуске ин-

фицированного файла программы вирус "взводится", подобно фанате. Он не обязательно "взрывается" сразу после запуска, однако это обязательно произойдет при выполнении некоторых логических условий.

Заражение документов. В настоящее время самый распространенный тип вирусов, встречающихся в "прериях" (т.е. за пределами вирусных лабораторий) — это *макровирусы* (macro viruses). Макровирусы представляют собой макросы Microsoft Office точно такие же, как и создаваемые вами. Как правило, они поражают файлы Microsoft Word. Современные вирусы создаются с помощью средств языка Visual Basic for Application (VBA) и "живут" в среде Office 97, однако некоторые пишут вирусы на Word-Basic и поэтому такие вирусы могут инфицировать файлы, созданные с помощью устаревших версий приложения Word. Несложный синтаксис этих языков позволяет писать макровирусы даже неопытным программистам — возможно, тем и объясняется их широкое распространение.

Макрос присоединяется к шаблону документа. Когда вы открываете документ, макрос инфицирует все открытые шаблоны (особенно файл `NORMAL.DOT` — стандартный шаблон всех документов Word). Кроме того, вирус делает то, что предусмотрено его полезной нагрузкой (payload) -вынуждает сохранять изменения, внесенные в документ, в новом файле вместо редактирования существующего, пытается удалить системные файлы или просто инфицирует каждый файл который вы открываете, с целью распространения.

Примечание

Макровирусы Word невозможно передать в другой текстовый процессор, даже если он может отображать инфицированные документы. Разумеется, можно написать макровирусы для любого приложения, поддерживающего макроязык (macro language), однако до сих пор этого не случилось. Во всяком случае, такие вирусы не были замечены в "прериях".

Быстрому размножению макровирусов способствовали электронная почта и широкая популярность Word. В наше время большинству людей следует соблюдать определенную осторожность, когда они собираются запускать новую программу, поступившую из неизвестного источника. (Если до сих пор вас это не заботило, надеюсь, прочитав этот раздел, вы станете бдительнее.) Документ — это просто документ, верно? И вот некто посылает вам файл для ознакомления, и чтобы его открыть, вы щелкаете на ссылке в окне своего клиента электронной почты. Вы не всегда думаете о том, что документ прежде всего следует проверить на наличие вирусов. К сожалению, для отражения атак вирусов пользователи ПК должны поступать с вирусами точно так же, как клиенты Macintosh *обязаны* были поступать *изначально*: проверять все. В операционной системе Macintosh каждый файл данных связан с исполняемым файлом. Это означает, что в компьютерах Macintosh вирусы будут бурно размножаться. Теперь же, когда эти вирусы — часть файлов данных ПК, владельцам ПК приходится проявлять ту осторожность, которая *всегда* была обязательной чертой пользователей Macintosh.

Как можно справиться с макровирусами? Одно из решений - защита от записи файла общего шаблона Word (`NORMAL.DOT`), однако это означает, что и вы тоже не можете его изменить. Если вы запускаете Office 97, не следует пренебрегать подсказкой Word, появляющейся при попытке открыть документ, содержащий какие-либо макросы. Затем вам следует задействовать или блокировать все макросы документа. (Одно из последствий широкого распространения макровирусов проявилось в снижении полезности макроинструментов (macro tool), поскольку людям не нравится использовать вставку в документ макроса, который может оказаться вирусом.) Лучший способ избежать инфицирования большинством вирусов заключается в применении и постоянном обновлении антивирусных программ. Когда кто-нибудь присылает вам документ по электронной почте, перед открытием проверьте его на наличие вирусов.

Если же ваш общий шаблон инфицирован, вы можете просто удалить файл `NORMAL.DOT` и уничтожить вирус. При повторном запуске приложения Word следует создать новую копию общего шаблона.

Новая мишень — системный BIOS. Это уже нечто новое. Я не собираюсь подробно описывать большинство вирусов, но вот этот — единственный в своем роде — потенциально очень опасен.

Вплоть до лета 1998 г. вирусы представляли собой чисто программную проблему. Они могли перезаписать главную загрузочную запись (Master Boot Record — MBR) на вашем жестком диске либо отформатировать диск, однако обе проблемы устранялись с помощью архивов. Конечно, это раздражало пользователей и могло разрушить систему, если вы не предпринимали надлежащих мер, однако с этим можно было смириться.

Все изменилось в июне 1998 г. с появлением вируса CIN. Этот программный вирус инфицирует .EXE-файлы, распределяя код вируса (virus code) по нескольким файлам .EXE и скрываясь в неиспользуемых областях исполняемых файлов. Полезная нагрузка (payload) выполняется 26 числа каждого месяца (или 26 июня, в зависимости от разновидности вируса, который вы "подцепили"). Этот вирус перезаписывает часть системной BIOS и первый 1 Мбайт загрузочного диска, в котором хранится MBR. Вирус воздействует на все компьютеры Windows 95/98 с системой BIOS, хранимой во флэш-памяти. Если BIOS вашего компьютера предназначен только для чтения (точнее, он хранится не во флэш-памяти — Прим. ред.), как это предусмотрено в устаревших ПК, вирус не сумеет инфицировать компьютер. Если вы не уверены, возможно ли обновление содержимого флэш-памяти с BIOS вашего компьютера (flash updates), сверьтесь с документацией на компьютер или запросите информацию у производителя.

Проблему главной загрузочной записи можно решить, если вы архивировали вашу MBR, однако вы не сможете нормально загрузиться, пока не перезапишете BIOS. В некоторых компьютерах предусмотрена возможность копирования содержимого BIOS, так что если ваша система допускает, и вы воспользовались этим, восстановление возможно. В противном случае вам придется покупать новую BIOS и уповать на то, что микросхема BIOS не припаяна к материнской плате — иначе вам придется купить и новую материнскую плату.

Хотя трудно сказать, насколько широко распространился вирус CIN, но его существование в компьютерных прериях не вызывает сомнений. Кроме того, в конце 1998 г. он "мутировал" и сейчас встречается, по меньшей мере, в двух формах.

Загрузочные вирусы

После макровирусов, второй наиболее распространенный тип вирусов, который сегодня можно встретить в прериях — *загрузочные вирусы*. Они активизируются и становятся заразными при чтении загрузочного сектора инфицированного диска: с этого момента вирус загружается в память и может инфицировать остальные диски, например, гибкие.

Загрузочные вирусы легко передаются, когда информация между компьютерами в основном "перемещается" с помощью гибких дисков. Какой-нибудь пользователь с вирусом в загрузочном секторе мог передать вам дискету с электронной таблицей, скажем, объема сбыта за январь. Вы скопируете эту таблицу на свой жесткий диск, причем при этом компьютер в целом еще не будет инфицирован. Однако если по рассеянности вы оставите эту дискету в дисководе (в устройстве A:) и перезагрузите компьютер, то инфицируете ваш компьютер, когда BIOS будет читать загрузочный сектор гибкого диска. Причем не имеет значение, является ли гибкий диск загрузочным — к заражению приводит даже доступ к диску. После инфицирования вашего диска при каждой последующей загрузке вирус будет попадать в память и инфицировать гибкие диски.

В настоящее время загрузочные вирусы все еще широко распространены, хотя их "значение" уменьшается. Локальные сети намного упростили совместное использование файлов, так что дискеты и сеть SneakerNet (в которой для копирования файлов на дискеты используются пешие переходы между компьютерами) применяются все реже. Что еще важнее, вездесущая Internet и доступ к другим видам электронной почты намного облегчили передачу файлов даже между компьютерами, расположенными в разных сетях.

Чтобы избежать инфицирования загрузочными вирусами, достаточно просто не загру-

жаться с дискет. Вы должны выработать привычку всегда извлекать дискету из дисковода, т.е. должны избегать загрузки компьютера с дискеты. Отредактируйте установки BIOS так, чтобы система сначала искала загрузочный диск c:, а затем A:. Избежать инфицирования дискет можно, прежде всего защитив их от записи, таким образом предотвратив запись на них вирусов.

Предупреждение

Проявляйте особую осторожность при изменении порядка загрузки (boot order). Если вы случайно сделаете так, что компьютер будет загружаться с CD-ROM, он пытается загрузиться с компакт-диска, если тот вставлен в дисковод. В подобных случаях система обработки ошибок ненадежна: в некоторых компьютерах вы узнаете только то, что этот диск - несистемный. Это ужасно, если вы полагаете, что читаете жесткий диск.

В качестве альтернативы, блокируйте загрузку только с дискет — именно такая конфигурация обычно присутствует в хорошо защищенных машинах. Тонкие клиентные устройства, скажем, терминалы Windows, вообще не могут инфицироваться загрузочными вирусами, поскольку в них нет каких-либо дисков.

Некоторые загрузочные вирусы *полиморфны*, иными словами, они загружаются в память, подобно программным вирусам, описанным ранее.

Предохраняйтесь от инфицирования

Насколько опасны вирусы? Автор книги работает с компьютерами в том или ином качестве в деловых офисах и консультационных фирмах с начала 80-х гг. Исходя из своего опыта могу поведать вам, что за это время мне лично довелось встретить только два вируса, не поддающихся тестированию, т.е. инфицирование произошло случайно. Один из вирусов относился к макровирусам, второй - к загрузочным. Иногда в разговорах с коллегами мне доводилось слышать и о других типах инфекций, но не слишком часто. Вам *следует остерегаться* вирусов, но *не следует* паниковать. Если вы предпринимаете те или иные меры защиты, заодно следует подготовиться и к прочим неполадкам. Основная мера защиты — регулярное архивирование. Тогда худшее, что может случиться при атаке любого вируса -публичный скандал, когда клиент обнаружит, что вы прислали ему инфицированный файл.

Помните: вирус — это программа. Поэтому сообщение электронной почты само по себе не может быть вирусом. Тот, кто посылает вам вложение в сообщение электронной почты, не сможет инфицировать ваш компьютер. Тот, кто передает вам дискету, которую вы вставляете в дисковод, тоже не в состоянии сделать это. Чтение с дискеты не приводит к инфицированию компьютера, пока вы не запустите *на нем* инфицированную программу. Машину инфицирует запуск вируса или загрузка с инфицированного загрузочного сектора. Выше указано, что для инфицирования достаточно просто получить доступ к диску.

Лучший метод избежать инфекции — использование сканера или монитора вирусов. *Сканер вирусов* (virus scanner) сканирует программные файлы, отыскивая *известные вирусные сигнатуры* (virus signatures) (шестнадцатиричные строки). *Монитор вирусов* (virus monitor) представляет собой резидентную программу TSR (Terminate and Stay Resident — завершить и остаться резидентной) — точно также ведет себя и сам вирус. Монитор вирусов (virus monitor) наблюдает за активностью, свойственной вирусам (например за записью в загрузочный сектор). Постоянно обновляйте антивирусные инструменты новыми средствами, регулярно присылаемыми с Web- или FTP-узлов разработчиков. Тогда вы будете располагать новейшими известными вирусными сигнатурами. Ссылку на источники антивирусных инструментов вы можете найти и на Web-узле, адрес которого указан в Приложении А данной книги.

Совет

Иногда вам будут советовать запустить сразу два антивирусных монитора, исходя из принципа, согласно которому то, что пропустит один монитор, найдет другой. По утверждению Давида Стэнга (David Stang), специалиста по вирусам и учредителя Национальной ассоциации по защите компьютеров (National Computer Security Association), этого делать не

стоит. В лучшем случае, вы не исправите ситуацию. В худшем - взаимодействие мониторов будет мешать работе и может даже привести к их же повреждению.

Как выбирать антивирусные инструменты? Трудно придумать какую-то надежную систему оценок. Некоторые создатели антивирусных инструментов утверждают, что их инструмент лучше, поскольку обнаруживает большее число вирусов, чем конкурирующие, но в таком деле погоня за числом может быть обманчива. В некоторых продуктах пять вариантов одного вируса засчитывают как пять разных вирусов, а в некоторых — как один. Кроме того, некоторые вирусы мутируют, используя для этого Mutating Engine (машину мутаций), становясь полиморфными. Это означает, что один вирус еще можно обнаружить, а его ближайшего родственника — уже нет.

Более осмысленную оценку антивирусных программ дают тесты, в которых эффективность нескольких продуктов по отношению к заданному набору вирусов сопоставляется с продуктом, который полагается наиболее эффективным. Небольшие различия несущественны. Так, например, сканер, который по ходу испытаний обнаружил 97% вирусов, не имеет особых преимуществ перед тем, который обнаружил 95%. Однако, если различие значительно, его следует принять во внимание. В целом, помимо таких процентных оценок успехов и неудач, рекомендую при выборе пакета основываться на критериях, приведенных в табл. 15.2.

Таблица 15.2. Критерии выбора антивирусных инструментов

Критерий	Описание
Скорость	Какова скорость работы сканера? "Медлительный" — вызывает у пользователей приступ раздражения
Используемая память	Какую память использует сканер: обычную (conventional) или верхнюю (upper)? Какой объем памяти необходим для нормальной работы?
Число ошибок	Сканер, который допускает множество ошибок (т.е. сообщает о несуществующих вирусах), лучше не использовать вообще. Помните притчу о мальчике, который слишком часто кричал: "Волк!!!"?
Частота обновлений	Постоянно появляются новые вирусы. Как часто разработчики обновляют ваш инструмент, чтобы он соответствовал изменениям? Сколько стоят эти обновления?
Цена	Сколько стоит сам инструмент? Каковы условия лицензирования?
Платформа	Может ли сканер работать с вашей операционной системой? Что надо сделать, чтобы тщательно просканировать компоненты ПК?

Просмотрите эту таблицу, а затем в зависимости от полученных ответов выберите подходящий антивирусный сканер. Предпочтительно защитить как серверы, так и рабочие станции, но если вы должны выбрать одно из двух, защищайте рабочие станции. Вероятность инфицирования сервера намного меньше.

Выводы

Защита сетей — обширная тема, хотя в этой книге ей посвящена одна-единственная глава. Однако, прочитав эти страницы, вы прочувствуете ситуации, за которыми необходимо наблюдать, а также меры, которые необходимо предпринять для защиты сети. Кратко они сводятся к следующим.

- Прежде чем вводить в действие любой план защиты, определите, что именно жизненно опасно для вашей сети. Вы не сможете подготовиться ко всему, поэтому подготовьтесь к тому, что является наиболее вероятным.
- Составьте калькуляцию и оцените стоимость защиты и стоимость защищаемых данных.
- Используйте методы идентификации пользователей, чтобы разрешить доступ к сетевым ресурсам только зарегистрированным пользователям, а также закройте защитную информацию по учетным записям пользователей.
- Если вам необходима дополнительная защита, зашифруйте данные.
- Защитите вашу сеть от внешних атак, которые могут разрушить программы и данные.

Если вы сумеете сделать все это, и если вы везучий человек, можете пропустить последнюю главу. Если же вы — такой же человек, как и все мы, рекомендую прочитать и ее.

Упражнение 15

1. Каково назначение SID в сетях Windows NT?
2. Фирма Microsoft рекомендует использовать пароли длиной не менее ___ символов.
3. Что такое L0phtcrack и каковы его функции?
4. елит пользователей на группы, которым предоставляются права и разрешения на доступ к объектам. _____ для назначения прав делит пользователей по организационным единицам (OU).
5. В какое число OU может входить пользователь, если применяется система NDS?
6. RSA — пример криптографической системы_____.
7. Ответьте, "да" или "нет". В PGP используется симметричное шифрование.
8. DES — пример криптографической системы_____.
9. Что такое CHAP и как он работает?
10. Что обеспечивает лучшую защиту: CHAP или PAP? Почему?
11. В каких случаях следует использовать сервер, поддерживающий протокол RADIUS?
12. Что такое привязки и почему они важны?
13. Внешняя атака, которая перегружает сервер настолько, что он не может обрабатывать обычные запросы, служит примером атаки_____.
14. Что делает IE4 при задании набора разрешений на выполнение приложений?
15. Ответьте, "да" или "нет". Вирусы воздействуют только на программное обеспечение.
16. Что из перечисленного ниже не защитит вас от бурного натиска (tempest attack)? Выберите все, что возможно.

    A. Использование монитора с низким электромагнитным излучением.
    B. Использование ПК класса A.
    C. Установка фильтров EMI на телефонные и силовые кабели,
    D. Установка на сервере защиты от вирусов.

17. Какой тип вируса самый распространенный в настоящее время?

    A. Загрузочные вирусы.
    B. Черви.
    C. Макровирусы.
    D. BIOS-вирусы.

Глава 16

Восстановление после аварий

Замысел этой книги зародился много лет назад на курсах по построению, обслуживанию, сопровождению и ремонту локальных сетей. Курсы посещали люди, занимавшиеся обслуживанием сетей и сетевые администраторы. Одни пришли из мира персональных компьютеров, другие — из среды мэйнфреймов. Некоторые уже имели какой-то опыт, однако желали пополнить свои знания. И вот, когда мы приступили к планированию аварийных работ, урок начинался примерно с такой беседы:

— Кто из вас имеет разработанные планы восстановления после аварий?

Большинство поднимают руку.

— А у кого из вас есть разработанные письменные планы восстановления после аварий?

Множество рук опускается.

— Ну а кто из вас проверил эти планы на практике и внес соответствующие поправки?

Большинство слушателей опускают руки и смотрят потупившись. Можно побиться об заклад, что единственный ученик, который все еще не опустил руку, либо лжет, либо не расслышал последний вопрос.

В жизни каждого из нас рано или поздно наступает ситуация, когда все разваливается. Сервер не загружается. Офис сгорает. Резервные копии не читаются. Совсем не смешно представить себе файловый сервер, пожираемый огнем, однако чертовски полезнее подумать об этом загодя, чем впоследствии объяснять вашему боссу, почему вы не можете восстановить первоначальное состояние сети. В этой главе рассматривается планирование восстановительных мероприятий после аварий, и то, кто должен этим заниматься, что именно нужно предусмотреть в этом плане и некоторые вероятные решения, которые вы можете реализовать для предотвращения или восстановления после аварии.

Виды аварий в сетях

Слово "авария" звучит драматично. Если вы думаете об аварии как о стихийном бедствии либо как о взрыве бомбы в World Trade Center (Всемирный торговый центр) в Оклахома Сити, то значит вы не в состоянии представить ее как нечто близкое и реальное.

На практике аварией можно назвать *любое* событие или обстоятельство, мешающее нормальной работе вашей фирмы или организации в течение неопределенного времени. При этом данные могут остаться неповрежденными. Авария — просто "нечто, прерывающее работу". Теперь оно уже не кажется нам чем-то абстрактным и далеким.

Потенциальные причины аварий можно разделить на три категории.

- Внешние события (например, стихийные бедствия);
- Неисправности оборудования.
- Последствия человеческих поступков.

Конечно, эти категории отнюдь не взаимоисключающие: внешнее событие может привести к неисправности, а какая-нибудь неисправность вполне может привести к такому поведению пользователя, которое усугубит аварию. С точки зрения восстановления после аварии причина ее не всегда имеет решающее значение. Однако при подготовке к аварии, важно представлять ее вероятную причину.

Аварии, вызванные внешними событиями

Проживая в разных местах почти на всей территории Соединенных Штатов, я убедилась, до какой степени стихийные бедствия могут помешать и даже приостановить работу предприятия. Например, ураган — отличный пример аварии, обусловленной внешним событием. Вы обязаны прекратить работу и начать эвакуацию; ливень может нанести огромный ущерб, если не хуже; у вас исчезают необходимые источники снабжения; электроэнергия отключается и т.п. Кроме того, в Калифорнии бывают еще пожары и землетрясения; на среднем западе нередки торнадо; в Новой Англии случайные снежные бури прерывают электроснабжение и засыпают дороги; не забудьте также наводнения и грозы.

События, вызывающие аварии, вовсе не должны быть такими значительными, как землетрясение или ураган Джорж (George). Несомненную угрозу представляют пожары в одном из зданий офисной стоянки автомобилей, а также прорыв водопроводной трубы, вследствие которого вода заливает часть вашего здания. Даже если авария не затронула напрямую ваш офис, вы почувствуете ее последствия. Несколько лет назад в одном из городов Виржинии, где я жила, случилось большое наводнение. Я живу и работаю на вершине одного из холмов, так что ничего не заметила, кроме сильного дождя. Однако мой телефон не работал два дня, поскольку река, протекающая через город, поднялась на 30 футов и залила телефонные линии. Если же вы работаете с сетью с помощью средств удаленного доступа, то отказ телефонных линий — сравнительно небольшая авария (напрямую не затрагивающая сеть), если ее оценивать с точки зрения затруднений или невозможности нормального ведения дел.

Итак, идея понятна. События могут не затронуть вас непосредственно, однако они могут нарушить всю вашу работу.

Неисправности оборудования

Любое оборудование — даже изготовленное на базе полупроводниковой (твердотельной, т.е. не имеющей движущихся частей) техники — периодически выходит из строя. Чем большим количеством оборудования вы располагаете, тем выше вероятность отказа одного из компонентов. Причем неисправность не обязательно затрагивает именно тот компонент, который нужен вам для работы. Например, если выходит из строя кондиционер, а погода жаркая, вы не можете запустить серверы, даже если уговорите сотрудников работать при температуре 95 градусов (по Фаренгейту). Если попытаться запустить сервер на такой жаре, он не будет работать.

К счастью, неисправности оборудования нетрудно предвидеть и спланировать ответные действия. Во всяком случае, устранять их проще, чем аварии, произошедшие по вине самого человека.

Проблемы человеческого поведения

Большинство людей, живущих в одной части страны хотя бы год-два, могут достаточно точно предвидеть проблемы, связанные с климатическими условиями. А проблемы из-за

неисправностей можно решить за счет внесения избыточности в оборудование.

Проблемы, вызванные человеческим поведением, могут быть совсем иного порядка. Сюда относятся как очевидные проблемы, вроде эпидемии гриппа или забастовок, но, к счастью, они не часто беспокоят сетевого администратора либо остальной технический персонал, если они сами не склонны к болезням и забастовкам. Однако намеренный саботаж (первый шаг к тому — ввод команды `DELETE *.*`), пренебрежение рекомендациями по компьютерной безопасности и занесение в сеть вирусов, самовольная установка и распространение в офисе нелицензированных программ, навлекающие на вашу голову гнев SPA — это тоже проблемы, вызванные человеческим поведением, и они относятся к числу тех, которые затрагивают вас напрямую.

Подготовка к аварии – архивирование

Еще до того как вы начнете обдумывать план восстановления после аварии, следует обдумать процедуру архивирования. Архивирование — настолько важная составляющая плана администрирования сети, что оно должно стать "естественной" частью вашей сети, а не частью плана восстановления после аварии.

Помимо того, что архивирование позволяет восстановить сетевые данные, когда кто-то всадит пулю в жесткий диск файлового сервера, оно полезно и в других, менее драматических, но потенциально опасных ситуациях.

- При замене искаженных файлов:
    - файлов данных;
    - системных файлов;
    - файлов шаблонов.
- При необходимости ввода копий файлов, которые в последний раз использовались несколько лет назад.

Эти проблемы — пустяки по сравнению с трудностями, возникающими при восстановлении файлов данных всей фирмы, но тем не менее, они всегда должны учитываться.

Методы архивирования

В операционных системах Windows применяются, по меньшей мере, четыре метода архивирования (табл. 16.1). Для настройки системы архивирования в каждом случае поразному используются установки бита архивирования в атрибутах файла.

Таблица 16.1. Методы архивирования

Архивирование	Архивируемые файлы	Переустановить бит архивирования?
Полное (Full)	Выбранные независимо от установки бита архивирования	Да
Добавочное (Incremental)	С установленным битом архивирования	Да

Разностное (Differential)	С установленным битом архивирования	Нет
Ежедневное (Daily)	С установленным битом архивирования и указанием даты архивирования (timestamped).	Нет

Примечание

Здесь приведены общепринятые методы архивирования. В некоторых утилитах архивирования предусмотрены дополнительные параметры. Например, в утилите Backups Exec 7.x фирмы Seagate - установки, позволяющие архивировать все файлы, к которым предоставлялся доступ в период, заданный пользователем.

Разумеется, ежедневно архивировать все файлы непрактично. В то же время архив должен содержать *основной набор* (base set) всех файлов. Таким образом, эффективный план архивирования должен предусматривать использование сразу нескольких методов архивирования. Обычно практикуется полное архивирование через регулярные интервалы времени (скажем, раз в неделю), а в дополнение — ежедневное или разностное архивирование. Как правило, ежедневное архивирование полезно, если вы собираетесь в путешествие и желаете прихватить с собой новейшие версии файлов, однако оно поддерживается не всеми программами.

Знание методов архивирования необходимо для составления плана, поскольку их выбор определит, чего именно вы сможете добиться за счет архивирования. Насколько гибкой должна быть система архивирования с точки зрения возможности восстановления данных? А что важнее для вас — гибкость или простота использования? Как рассчитать время, необходимое на архивирование?

Например, простейшим способом архивирования, обеспечивающим восстановление данных, служит полное архивирование, поскольку для восстановления используется один источник. Архивируйте данные на одну и ту же ленту ежедневно, например, в 3 часа дня — и вы всегда будете располагать полным (и новым) архивом. Конечно, полное архивирование занимает много времени (и места): чем больше архивируемых данных, тем больше затраты времени на архивирование. Еще больше проблем возникает при выполнении одного полного архивирования каждую ночь на одну и ту же ленту, поскольку вы не сможете архивировать резервные копии. Например, если вам понадобится версия файла за среду, а в пятницу вы обновили этот файл, то нужной версии просто уже не будет, и вы останетесь у разбитого корыта. Так сколько же полных архивов вы должны сохранять? Чаще всего полное архивирование выполняют периодически, дополняя его разностным или добавочным архивированием, описанным ниже.

Добавочное архивирование. Создается архив файлов, которые изменялись со времени последнего полного или добавочного архивирования. По этой же причине продолжительность такого архивирования невелика — намного меньше полного архивирования и (как правило) разностного. Добавочное архивирование особенно полезно, когда вам необходимо найти какой-либо файл для восстановления. Однако восстановление содержимого всего сервера в таком случае несколько утомительно — вам придется восстанавливать каждый добавочный архив отдельно.

Разностное архивирование. Архивируются все файлы, измененные со времени последнего полного или добавочного архивирования. Таким образом, для восстановления проще всего использовать архивы именно этого типа — вам достаточно только восстановить полную архивную копию, а затем внести последние изменения. Единственный недостаток заключается в трудности восстановления конкретной версии файла, поскольку отследить нужную версию — нелегкое дело.

Примечание

Пример схемы архивирования, сочетающего высокую гибкость и простоту использования и состоящего из комбинации полного и разностного архивирования, описан в разделе "Разработка и реализация плана архивирования".

Разработка и реализация плана архивирования

Недавно я беседовала со знакомым консультантом. Сейчас он помогает создавать сеть в фирме, которая традиционно использовала в делопроизводстве бумажные документы. В то же время он устанавливает также новые клиентные машины, помогая фирме извлекать преимущества из использования сети, решая некоторые трудные вопросы организации связи и, конечно, разрабатывая для фирмы план архивирования.

Самая серьезная проблема, с которой ему довелось столкнуться (разумеется, после того как ему удалось убедить фирму в необходимости в первую очередь создать систему архивирования, что тоже оказалось нелегкой задачей) заключалась в том, что никто, кажется, не собирался решать проблему простыми методами. Работники отдела технической поддержки начитались о всевозможных новейших решениях с помощью альтернативных носителей, вроде перезаписываемых компакт-дисков и тому подобного. Магнитные ленты, по их мнению, уже надоели — их используют все. Они желали чего-нибудь иного.

Когда вы разрабатываете план архивирования, не стоит тратить время на выдумки. Конечно, знать о новшествах обязательно. Следует также рассмотреть различные варианты и подобрать наиболее подходящие системы. Но не отбрасывайте какую-либо систему просто потому, что ее уже используют повсеместно.

А вот что важно для плана архивирования, так это функциональные средства (средства архивных носителей, методов планирования и т.д.). Уместно изучить опыт других специалистов. Если система успешно работает в другой фирме, занимающейся тем же, что и ваша, скорее всего она прекрасно подойдет и вам.

Наметки плана

Первый этап создания плана архивирования заключается в определении регламента. Как часто необходимо архивировать данные, чтобы поддерживать работу организации? Когда следует архивировать данные, чтобы причинить сотрудникам минимум неудобств?

Примечание

Ответ на второй вопрос в определенной степени зависит от программного обеспечения, которое вы применяете для архивирования. Некоторые утилиты архивирования позволяют архивировать открытые файлы, что несколько упрощает составление плана.

Как часто необходимо выполнять архивирование? На это вопрос нет определенного ответа, поскольку он зависит от того, в какой мере для вас опасна утрата данных. Например, если вы выполняете архивирование только раз в месяц, приготовьтесь к возможности утраты данных за весь месяц. Большинство из нас в той или иной мере используют ежедневное архивирование (возможно, дополненное еженедельным полным архивированием), но и в таком случае возможна утрата каких-то данных, а некоторым, к примеру, жалко терять даже то, что они сделали за день. Однако еще более жалко терять время на постоянное архивирование. Если вы считаете, что оборудование достаточно устойчиво работает в течение 24 часов, то частое архивирование, очевидно, ни к чему. В архивировании так же, как и в защите, должен соблюдаться баланс между затратами на его выполнение, ценностью защищаемых данных и вероятностью какого-нибудь происшествия за это время.

Расписание архивирования. Как правило, постоянное выполнение процедуры архивирования оказывается обременительным. Оно мешает людям работать, поскольку отнимает рабочее время, и может вызывать перегрузку сетевого трафика (если копируются файлы, относящиеся к иной системе, нежели система архивирования). Кроме того, для этого требуется программное обеспечение, позволяющее архивировать открытые файлы.

По этой же причине архивирование в режиме реального времени (realtime backups) используется лишь немногими фирмами. Вместо этого, как правило, персонал выбирает время суток, когда архивирование причинит неудобства наименьшему числу пользователей, т.е. когда окажется весьма маловероятно, что придется закрывать файлы. Если же вы используете централизованную систему архивирования данных в глобальной сети, расположенной на нескольких часовых поясах, возможно, вообще не удастся выбрать время, когда сеть будет свободна. Но вы можете хотя бы свести накладки к минимуму.

Совет

В некоторых операционных системах, например, Windows NT, средства совместного доступа к файлам организованы в виде средства (инструмента), который можно отключить, а затем снова включить. Если в конце рабочего дня пользователи оставили свои файлы открытыми, а ваша система архивирования не поддерживает архивирование открытых файлов, создайте пакетный файл, который выключит это средство обслуживания сервера (server service), запустит процедуру архивирования, а затем снова включит средство обслуживания.

Разработка плана архивирования. В табл. 16.2 приведен пример очередности архивирования данных для небольшого офиса, рассчитанный на месячный срок. Прежде чем вы примете этот план, следует выполнить полное начальное архивирование (Полное архивирование, лента 1).

В пятницу пятой недели вы должны перезаписать ленту 1 полного архива и начать цикл заново. Данная процедура создаст двухнедельную "запись" разностных архивов и месячную - полных. Для файлов, которые используются только изредка и могут быть случайно удалены или искажены не чаще, чем раз в несколько месяцев (либо даже в несколько лет) после первоначального использования, можно рекомендовать дополнительное шестимесячное архивирование.

Таблица 16.2. Пример очередности архивирования (двухнедельная ротация)

Неделя	День недели	Тип архивирования и используемая лента
Неделя 1	Понедельник	Разностное, лента 1
	Вторник	Разностное, лента 2
	Среда	Разностное, лента 3
	Четверг	Разностное, лента 4
	Пятница	Полное архивирование, лента 2
Неделя 2	Понедельник	Разностное, лента 5
	Вторник	Разностное, лента 6
	Среда	Разностное, лента 7
	Четверг	Разностное, лента 8
	Пятница	Полное архивирование, лента 3
Неделя 3	Понедельник	Разностное, лента 1 (перезапись)
	Вторник	Разностное, лента 2 (перезапись)
	Среда	Разностное, лента 3 (перезапись)
	Четверг	Разностное, лента 4 (перезапись)

	Пятница	Полное архивирование, лента 4
Неделя 4	Понедельник	Разностное, лента 5 (перезапись)
	Вторник	Разностное, лента 6 (перезапись)
	Среда	Разностное, лента 7 (перезапись)
	Четверг	Разностное, лента 8 (перезапись)
	Пятница	Полное архивирование, лента 5

Рекомендуемые схемы архивирования

В таблице 16.2 показана упрощенная версия одной их двух моделей архивирования, рекомендуемых фирмой Microsoft, а именно дед/отец/сын (Grandfather/Father/Son — GFS). В методе GFS под "дедом" понимается полное месячное архивирование, под "отцом" — полное еженедельное, а под "сыном" — добавочное или разностное ежедневное архивирование. В методе GFS для хранения всех архивов за трехмесячный период используется всего 12 лент (либо иных носителей): четыре для ежедневного архивирования, пять для еженедельных архивов и три — для месячных.

Другая схема архивирования, рекомендуемая фирмой Microsoft, называется "ханойской башней" (Tower of Hanoi — ToH), по названию известной математической головоломки. Хотя метод ToH сложнее метода GFS, он поддерживает архив за больший срок — 32 недели вместо 12. В методе ToH пять лент (надписанных здесь буквами A-E) используются в следующем порядке: A B A C A B A D A B A C A B A E. В данном методе лента A повторно используется каждые две недели, B — четыре недели, C — 8 недель, D — 16 недель, а E — 32 недели. Метод ToH применяется только для полного архивирования, поэтому еженедельное полное архивирование следует дополнить ежедневным добавочным или разностным.

Чтобы действительно упростить свою работу, приобретите соответствующее программное обеспечение для архивирования, которое можно настроить на определенную схему, а также "подсказывающее" выбор нужной ленты. Тогда вам необязательно пунктуально следовать разработанному плану.

Выбор аппаратных средств архивирования

Какие устройства архивирования пригодны для работы с сервером? Для практических целей рекомендуем выбрать ленточный накопитель какого-нибудь типа (см. гл. 8). Они относительно дешевы, достаточно вместительны, надежны и пользуются широкой поддержкой.

Однако ленточные накопители — отнюдь не единственный инструмент для архивирования. Если вы собираетесь широко распространять содержимое ваших архивов, предпочтительно использовать записывающие CD-ROM (CD-рекордеры). Несмотря на то, что емкость компакт-диска не превышает 1 Гбайт, а, кроме того, установка параметров записи иногда довольно сложна, можете не сомневаться — в большинство компьютеров, проданных за последние три года, установлены устройства CD-ROM. Небольшая вместимость картриджей Zip и Jaz препятствует широкому практическому применению таких устройств (drives) для архивирования содержимого серверов. Однако если ваш план архивирования предназначен для клиентных машин, а не серверов, небольшие съемные диски окажутся вполне пригодны. Так, для архивирования пользовательских данных предпочтительней Jaz, а если вы используете внешний (съемный) диск (external drive), его удобно переносить между клиентными компьютерами, работающими по технологии SCSI. Если же эти методы для вас неприемлемы, файлы можно архивировать на другом жестком диске, который может находиться как на сервере, так и на другом сетевом компьютере.

В конечном счете, ваш выбор средств архивирования определяется скоростью, вместимостью и переносимостью. Эти факторы рассматриваются в следующих разделах.

Скорость архивирования. Если архивирование выполняется по ночам, то скорость процесса не столь важна, однако при *восстановлении* данных она — важнейший фактор.

Скорость определяется двумя факторами: скоростью работы самого устройства архивирования и временем соединения с сервером. Вероятно, в будущем наивысшую скорость обеспечит "фабрика коммутируемых сетевых соединений" (switched fabric network connections). Сегодня самым быстрым соединением является SCSI, затем следует IDE, а на третьем месте параллельный порт. Я уже рекомендовала использовать SCSI-интерфейс в качестве интерфейса контроллера (controller interface) для серверов. (Если вы забыли, что это значит, перечитайте гл. 7.) Параллельные порты не слишком удобны в качестве интерфейсов средств архивирования серверов (server backup interfaces), хотя они тоже могут работать на индивидуальных клиентных машинах, которые не содержат SCSI-устройств.

Кроме того, определенное значение имеет и время доступа к носителю. С какой скоростью можно переместить на него данные или считать их с него? Скорость передачи данных для различных носителей влияет на скорость считывания данных с носителя или записи данных на него.

Примечание

Хранение данных в сжатом виде снижает скорость их последующего чтения или записи.

Емкость устройства. Какой объем данных помещается на единичном носителе устройства архивирования? Можно ли поместить все данные на одном носителе, нескольких или множестве носителей? Чем больше данных помещается на единичном носителе (backup storage unit), тем проще их архивировать и восстанавливать, поскольку поддерживать порядок среди небольшого числа носителей значительно проще. Архивирование упрощается, если вам не нужно менять носители. Данные проще восстанавливать, если это можно сделать с помощью одного-двух носителей, а, кроме того, чем их меньше, тем проще хранить.

Переносимость. Вплоть до настоящего времени в качестве носителя обычно используют магнитные ленты. Хотя время доступа к ним примерно такое же, как и у дисков Zip (табл. 16.3), они имеют достаточную емкость и применяются весьма широко. Единственный параметр, который не всегда обеспечивается магнитными лентами - переносимость. Разнообразие типов лент и архивных форматов (backup formats) позволяет использовать магнитные ленты для распространения данных разве что в пределах одной фирмы. В этом отношении несомненные преимущества имеют записывающие устройства CD-ROM и съемные диски (табл. 16.3). Некоторые форматы файлов рассматриваются в гл. 8, а в табл. 16.3 перечислены устройства, альтернативные ленточным накопителям.

Табл. 16.3. Характеристики наиболее популярных не ленточных носителей архивов

Критерий	Жесткие диски	CD-R/RW	Zip	SCSI
Доступные типы соединения	IDE, SCSI, сеть	Параллельный порт, IDE, SCSI	SCSI, параллельный порт, USB, IDE	SCSI
Время доступа	>9 мс	250-350 мс в зависимости от модели	29 мс (параллельный порт)	15,5 – 17,5 мс
Ёмкость	До 13 Гбайт на один диск	650 Мбайт	250 Мбайт	2 Гбайт

Устройство-носитель информации	Жёсткий диск	Компакт-диск	Картридж размером с диск (disk-sized cartridge)	Картридж размером с диск (disk-sized cartridge)

Далеко не всякий пакет архивирования может работать с носителями всех типов. Так, утилита архивирования из Windows NT может работать только с ленточными накопителями: вы не сможете выполнить архивирование, скажем, на сетевой или переносной диск.

Выбор программного обеспечения для архивирования

При выборе утилиты архивирования особое внимание обращайте на гибкость программы, а также возможности ее взаимодействия с уже установленными сетевыми компонентами. Обдумывая применение какого-нибудь приложения для архивирования, найдите для себя ответы на такие вопросы.

- Совместимость.
  - Будет ли приложение работать с установленной операционной системой?
  - Совместимо ли оно с прочими системами архивирования, которые, возможно, уже используются?
  - Какие типы архивирования поддерживает данное приложение?
  - Как работает приложение: отдельно для каждого сервера или его можно использовать для управления архивированием нескольких серверов с единой консоли?
  - С носителями каких типов может работать это приложение?
  - Ленты какого формата следует использовать при установке данного приложения?
- Гибкость.
  - Можно ли организовать выполнение архивирования в отсутствие оператора (unattended backup)?
  - Какую свободу действий допускает данное приложение при выборе архивируемых файлов (на уровне тома, папки, файла)?
  - Будет ли оно повторять операции над (retry) открытыми файлами?
  - Будет ли оно архивировать открытые файлы?
  - Копирует ли оно структуру данных либо создает двоичный образ архивируемого диска?
- Надежность.
  - Предусмотрена ли в приложении надежная система коррекции ошибок?
  - Можете ли вы проверить целостность данных?
  - Насколько просто данное приложение в работе?
  - Предоставляется ли вам контроль за ходом исправления ошибок?
  - Поддерживает ли приложение выполнение проверки (ревизии) в заданный срок?

В большинство современных сетевых операционных систем — в том числе и одноранговых — встроено собственное приложение для архивирования, которым вы можете воспользоваться и таким образом избежать покупки особого приложения. Так, утилита архивирования, встроенная в Windows NT, представляет собой упрощенную версию BackupExec фирмы Seagate. Чтобы воспользоваться всеми ее функциональными средствами, включая архивирование открытых файлов, следует приобрести оригинальную версию фирмы Seagate. Однако и утилита, встроенная в NOS, обеспечивает великолепную защиту данных, хранящихся на сервере.

Исполнение плана

Выполнение разработанного плана относится, главным образом, к обязанностям сетевых администраторов и, в принципе, никак не связано с используемыми сетевыми технологиями. Следует запланировать, кто должен выполнять план архивирования, где должны храниться архивы, а также испытать на практике ваш план восстановления данных.

Кто должен заботиться о сохранности данных? Администратором резервного копирования должен быть человек, пользующийся доверием, поскольку в его руках находится судьба данных фирмы. Кроме того, его доступ к серверу менее ограничен, чем у рядовых пользователей. Убедитесь, что он знает методы выполнения соответствующих процедур, а также, куда следует обращаться при возникновении каких-либо проблем. К числу процедур относятся следующие.

- Архивирование данных.
- Проверка записей.
- Хранение и маркировка архивных лент.
- Ротация и повторное использование лент.

Особо убедитесь, что специалиста, который может оказать помощь, можно без труда найти на рабочем месте. Автору известен один случай, когда администратор, выполнявший резервное копирование, сталкивался с проблемами, относящимися к носителям или к программному обеспечению, — и не мог понять причину их появления. Офисный эксперт по архивированию в основном путешествовал, а когда появлялся на рабочем месте, не имел времени заняться проблемой. Администратор же пытался перехватить эксперта, когда у того было время. Эпилог вы можете дописать сами: файловый сервер разрушился, архивирование не помогло (оказалось, что магнитная лента в кассетах была слабо натянута, так что восстановить архив оказалось невозможным). Персоналу, занятому восстановлением данных, пришлось изрядно потрудиться. Картина безрадостная.

Наконец, ответственный за резервное копирование сменный администратор должен постоянно находиться на рабочем месте. Если главный администратор заболеет или уйдет в отпуск, кто-то другой должен немедленно заменить его. Недопустимо назначать сменщиком любого сотрудника только потому, что его угораздило попасть вам под руку, когда было замечено отсутствие обычного администратора. В таком случае необходимая работа будет сделана неверно, если вообще будет сделана.

Совет

После завершения архивирования и проверки его результатов повесьте план архивирования с графами для заметок. Это полезно по двум причинам. Первая: расписание напоминает о необходимости выполнения архивирования. Вторая: расписание, висящее на стенке, позволяет с одного взгляда установить файлы, которые архивировались последний раз, тип архивирования и исполнителя.

Проверка восстановления данных. Критерием эффективности плана архивирования является гарантированное восстановление архивированных данных. Потенциальные источники проблем заключаются в ошибках оператора или сбоях оборудования (вспомните слабое натяжение ленты). Проблемы подобного рода желательно обнаружить прежде, чем ситуация станет критической. Поэтому заставьте администратора, отвечающего за резервное копирование, проверять содержимое всех лент и восстанавливать искаженные файлы (предпочтительно те, которые не изменялись с момента архивирования).

Хранение архивных копий. Вам не сулит ничего хорошего ситуация, когда после архивирования диска вы обнаружите, что архив бесполезен. Если офис сгорит, архив, хранившийся на полке рядом с компьютером, вам не поможет. Точно так же он не принесет

шийся на полке рядом с компьютером, вам не поможет. Точно так же он не принесет пользы, если ящик с архивом стоит под солнечным светом на подоконнике — дискеты постепенно "поджарятся" на солнце и выйдут из строя. С другой стороны, если не надписать диски соответствующим образом и не хранить их в надлежащем порядке, то вам будет трудно (или невозможно) найти то, что надо, когда понадобится восстановить данные.

Что же необходимо делать, чтобы поддерживать архивы в надлежащем порядке? Четко надписывайте резервные копии. Укажите имя компьютера, диска, дату архивирования, а также номер диска или ленты. Надпись или запись в картотеке (file card) можно сделать примерно так.

ПОЛНЫЙ АРХИВ компьютера PALADIN D: 07/15/99 #4/6

Храните свои архивы в безопасном, прохладном и сухом месте. Лучше всего хранить важные архивы вне офиса, тогда они уцелеют в случае пожара. Если по каким-то причинам вы не сможете это сделать то, по крайней мере, перенесите его на другой этаж, чтобы он уцелел хотя бы при локальных "катаклизмах".

Предупреждение

Если вы покупаете несгораемый шкаф для хранения архивов, убедитесь, что его класс защиты соответствует защите данных, а не бумаг. Температура воспламенения бумаги довольно высока. Ленты же могут расплавиться даже под солнечными лучами, не говоря уже о пожарах. Сейф для хранения данных обойдется намного дороже (около 300 $ вместо 50 $), но данные вашей фирмы могут стоить еще больше.

Не сохраняйте ненужные архивы — впоследствии они вас только запутают. Если вы форматируете жесткий диск компьютера и начинаете все заново, то сотрите архивные файлы данного компьютера в последнюю очередь, после того как убедитесь, что на диске не было ничего стоящего.

Периодически проверяйте ваши архивы, чтобы убедиться в их работоспособности. Тепло, влага и электромагнитные поля могут разрушить данные. Помните: диски и люди хорошо работают примерно в одинаковых климатических условиях. Если вы не в состоянии часами сидеть в комнате для хранения архивов, значит она совершенно не соответствует своему назначению.

Если архивы хранятся годами, не надейтесь, что они останутся в сохранности без вашей помощи. Диск, забытый на полке, медленно утрачивает записанные на нем данные. Это напоминает запись на пляжном песке: она постепенно исчезает, если вы не будете переписывать ее ежедневно. Вы можете дать "вторую жизнь" вашим лентам, если скопируете архивы на заново сформатированные носители, а затем отформатируете старые ленты. Как правило, срок службы лент не превышает 2—3 года.

Защита данных в режиме реального времени

Возможно, вы полагаете, что архивирование в режиме реального времени практически невозможно, поскольку оно слишком дорого, требует больших ресурсов и т.п. Однако есть некоторые методы, которые можно использовать для сравнительно непрерывного сохранения обновленных данных, позволяющие сохранять обновленные данные даже при авариях дисков. Такие методы имеет несколько преимуществ. Они не только обеспечивают избыточность и обновление данных по ходу работы, но также повышают производительность сети путем *выравнивания нагрузки*, т.е. распределения доступа к данным по множеству дисков или серверов. При обычном же архивировании обеспечивается только избыточность данных.

Использование массивов RAID

RAID (Redundant Array of Inexpensive Disks — избыточный массив недорогих дисков) — общее название технологии, объединяющей ресурсы нескольких жестких дисков для повышения общей надежности и/или производительности системы хранения информации на дисках. Аппаратные массивы RAID строят на основе подсистемы RAID SCSI-дисков, в то время как в программных RAID-средствах для создания массива используют специальные программные средства. Основные параметры RAID-массива таковы.

- Отказоустойчивость массива позволяет выдерживать аварию одного из дисков. Утраченные данные могут быть восстановлены с помощью остальных дисков.
- Работа массива зависит от совместной работы множества физических дисков. Для создания RAID можно комбинировать и логические тома. Если же физические диски не работают совместно, их называют JBOD (Just a Bunch of Disks — простой набор дисков).
- Физические диски не обязательно должны быть одного типа и размера, однако размеры логических разделов (logical divisions) в пределах массива должны быть одинаковыми. Иными словами, размеры всех логических
- частей массива должны совпадать.
- Массив RAID можно использовать для защиты всех либо части физических дисков.

Совет

Вы можете создать программный массив RAID и на базе EIDE-дисков, но SCSI-диски обеспечивают большую производительность. Как указано в гл. 7, интерфейс SCSI обеспечивает многозадачный режим операций чтения/записи на единственном контроллере, в то время как интерфейс EIDE - только однозадачный.

Массивы RAID приобрели широкую популярность, когда стоимость жестких дисков значительно упала. Программные RAID-массивы позволяют использовать эту технологию даже людям со средними доходами. Как правило, используются два типа отказоустойчивых RAID-массивов: с зеркальным отображением диска (disk mirroring) и с чередованием дисков (disk stripping) с контролем четности. Они рассматриваются в последующих разделах.

Зеркальное отображение диска. Обеспечивает защиту всех данных путем их записи сразу в двух местах. Каждый раз, когда вы создаете, редактируете или удаляете файл, изменения регистрируются в обоих местах. Для этого необходимы два отдельных диска, непосредственно объединенных в зеркальный набор (mirror set). Если что-либо происходит с данными на одном из накопителей, то вы разделяете зеркальный набор и получаете доступ к точной (и новейшей) копии данных на другом. Следует отметить, что зеркальные наборы неэффективны с точки зрения использования дискового пространства. Действительно, в таком случае избыточность означает, что для хранения данных требуется вдвое большее дисковое пространство, чем при обычном хранении. И тем не менее, это великолепный способ зашиты данных. Кроме того, в системах SCSI применение таких RAID-массивов уменьшает время считывания, поскольку операция чтения может выполняться сразу с двух дисков в многозадачном режиме.

Примечание

Если каждый диск в зеркальном наборе имеет собственный контроллер (и, таким образом, авария одного контроллера не приводит к потере доступа к обоим дискам), эта технология называется дуплексированием дисков (disk duplexing). В остальных случаях зеркальный набор работает именно так, как было описано выше.

Чередующийся набор с контролем четности. Подобно зеркальному отображению диска, чередование дисков с контролем четности позволяет защитить данные, распределяя их по множеству дисков. Данные записываются на дорожки каждого жесткого диска чередую-

щимся набором. Чередующиеся наборы с контролем четности должны состоять не менее чем из трех физических дисков. Кроме исходных данных, на диски записывается информация о четности. Как и исходные данные, она распределяется по физическим дискам, однако сохраняется отдельно от тех, к которым относится. При отказе одного из дисков чередующегося набора, для восстановления пропавших данных используется информация о четности из остальных дисков. Благодаря этому сохраняется доступ ко всем данным. Объем информации о четности зависит от количества дисков в чередующемся наборе, поскольку информация о четности рассчитывается так, чтобы восстановить данные на одном диске. Таким образом, в чередующемся наборе из трех дисков для хранения информации о четности будет использоваться третья часть всей суммарной емкости, а в наборе из 10 дисков — десятая. Чем больше дисков в наборе, тем эффективнее его работа.

Если же в чередующемся наборе одновременно выходит из строя несколько дисков, данные теряются, однако авария одного диска устраняется без какого-либо вмешательства с вашей стороны. Допустим, вы собрали RAID-массив из четырех дисков и используете его в качестве основы чередующегося набора с контролем четности. Внезапно отказывает один из дисков. Когда вы перезагрузите сервер и откроете Disk Administrator (Администратор дисков), появится сообщение о том, что диск отказал, а утраченные данные будут восстановлены. Можно будет записывать и считывать данные из чередующегося набора так, как будто отказавший диск все еще работает. Конечно, вы должны как можно скорее его заменить. Если откажет еще один диск, то восстановить чередующийся набор будет просто невозможно.

Примечание

Информация о четности жизненно важна для обеспечения отказоустойчивости. Один из видов RAID-массива - чередующийся набор дисков без контроля четности - отказоустойчивость не обеспечивает. Он спроектирован главным образом для повышения производительности дисков. С этой целью операции чтения и записи разнесены по множеству дисков. Поскольку в этом случае диски сильно зависят друг от друга (codependent) и не содержат информацию о четности, дисковые массивы такого типа должны регулярно архивироваться - отказ хотя бы одного диска разрушит весь массив.

Достоинства и недостатки различных типов RAID-массивов. Что лучше, использовать чередующиеся наборы с контролем четности или зеркальное отображение диска? Массивы с зеркальным отображением диска отличаются невысокой начальной стоимостью, поскольку для создания зеркального набора достаточно всего двух дисков, в то время как для отказоустойчивого чередующегося набора — не менее трех. Кроме того, операции записи в массивах с зеркальным отображением диска выполняются быстрее. В зеркальных SCSI-наборах операции записи/чтения могут выполняться более-менее одновременно вследствие "многозадачности" интерфейса SCSI. Поэтому зеркальное отображение диска действительно повышает скорость операций чтения/записи. В чередующихся наборах с контролем четности операции записи менее производительны, поскольку в данном случае при каждом изменении данных необходимо повторно рассчитывать информацию о четности. Это не относится к операциям чтения, однако по сравнению с одиночным диском или зеркальным набором запись выполняется медленнее. Наконец, расчеты, необходимые для поддержки чередующихся наборов, выдвигают дополнительные требования к оперативной памяти и производительности процессора сервера по сравнению с зеркальным отображением диска.

Отметим, что чередующиеся наборы с контролем четности применяют чаще остальных типов RAID-массивов. Зеркальное отображение весьма расточительно занимает дисковое пространство — оно используется менее эффективно, чем в чередующихся наборах с контролем четности. Причем эффективность последних повышается с увеличением количества дисков в чередующемся наборе. Высокая эффективность использования дискового пространства компенсирует любые недостатки производительности (фактически, они совершенно незаметны сетевым клиентам). Кроме того, благодаря удешевлению оборудования, дополнительные ресурсы, необходимые для поддержки чередующихся наборов, реально не сдерживают использование этого более совершенного типа RAID-массивов.

Репликация данных

Если же простой системы абсолютно недопустим, можно применить один из двух методов. Первый заключается в кластеризации серверов (clustering) (см. следующий раздел), а второй — в репликации данных. *Репликацией* называют копирование данных и их структуры с одного сервера на другой. Это весьма популярный метод, используемый для обеспечения целостности и распределения данных (data load) между несколькими серверами. Сначала данные записывают на один из серверов (называемый в сетях Windows NT *сервером экспорта* (export server)), а затем копируют на другой сервер (*сервер импорта* (import server)). Для выравнивания нагрузки между серверами обслуживания клиентов (client load) вы можете установить связи между ними с режимом ручного разделения или же использовать режим автоматического разделения.

Как правило, реплицируют данные двух типов: те, которые ни в коем случае не должны быть утрачены и те, для которых полезно выравнивание нагрузки. Из-за ограниченной полосы пропускания сети, репликацию редко используют для защиты обычных данных. Это обусловлено тем, что копирование каждого изменения данных на крупный файловый сервер может занять всю полосу пропускания, необходимую для решения остальных задач. Для защиты файлов данных можно использовать RAID-массивы. Тем не менее, репликация - весьма эффективный метод защиты баз данных или иной жизненно важной информации, например информации об установленных соответствиях (mappings) сервера WINS или каталога со сценариями входа. Таким образом, вместо обслуживания всех запросов клиентов с центрального сервера репликация позволяет распределить эту работу по нескольким серверам и одновременно гарантировать существование избыточного числа копий базы данных.

Кластеризация серверов

Кластеризация в некотором смысле напоминает RAID-систему, однако она более совершенна. Для обеспечения отказоустойчивости и повышения производительности в методе кластеризации вместо создания массивов RAID применяется создание *массивов серверов*.

Кластеризация реализуется разными методами, которые отличаются как функциональными средствами, так и технологиями связывания и взаимодействия серверов. В функциональном отношении кластеры подразделяются на три основных типа.

- Активный/активный.
- Активный/резервный (standby).
- Отказоустойчивый.

В принципе, ту или иную поддержку отказоустойчивости обеспечивают кластеры любого типа, однако ее уровень и скорость, с которой функции отказавшего сервера передаются другому, зависят от типа кластера.

В кластере типа активный/активный все серверы непрерывно функционируют и обслуживают пользователей. При отказе любого сервера остальные серверы (или сервер) продолжают управлять своей рабочей нагрузкой и, кроме того, принимают на себя рабочую нагрузку отказавшего. На передачу нагрузки отказавшего сервера остальным серверам кластера уходит 15—90 с. В кластере типа активный/резервный один из серверов обслуживает запросы пользователей либо выполняет иные задачи, а второй ждет отказа этого сервера. Это отнюдь не уменьшает *время восстановления после сбоя* (failover time): при отказе первого сервера для передачи его рабочей нагрузки второму по-прежнему необходимо 15—90 с. (При передаче рабочей нагрузки резервному серверу все соединения и сеансы, исполняемые им, завершаются.)

Отказоустойчивые кластеры проектируют так, чтобы их годичный простой не превышал 6 мин. Эти кластеры отличаются от кластеров типа активный/ активный и активный/резервный. В отказоустойчивом кластере все серверы *идентичны* и работают в связках, выполняя абсолютно одинаковые операции. Таким образом, при отказе одного сервера, его нагрузка фактически мгновенно подхватывается остальными серверами. Отказоустойчивые кластеры используют ресурсы менее эффективно, чем кластеры типа активный/активный или активный/резервный, однако при отказе одного из серверов отказоустойчивые кластеры обеспечивают практически бесперебойную работу. Кластеры других типов, напротив, могут прекратить работу на время до полутора минут, а чтобы исказить операцию записи достаточно даже 15с. Сравнительные характеристики этих трех типов кластеров приведены в табл. 16.4. Тип кластера позволяет определить, создан ли кластер для обеспечения отказоустойчивости или повышения производительности, а также метод распределения рабочей нагрузки между серверами, входящими в кластер. Кластерные *продукты* различаются применяемой технологией совместного использования данных, методом соединения серверов кластера, а также степенью гибкости поддержки различных аппаратных средств. Кроме того, продукты различаются количеством серверов, из которых образован единый кластер. Так, некоторые продукты поддерживают кластер, содержащий не более двух серверов — первичный и вторичный. Более дорогостоящие продукты поддерживают большее число кластеров.

Таблица 16.4. Сравнение типов кластеров

	Активный/ активный	**Активный/ резервный**	**Отказоустойчивый**
Функции первичного/вторичного сервера	Различаются	Различаются	Идентичны (с целью обеспечения полной избыточности)
Влияние на вторичный сервер при отказе первичного	Принимает на себя рабочую нагрузку первичного сервера	Сбрасывает собственную рабочую нагрузку и принимает нагрузку первичного сервера	Не влияет, поскольку оба сервера перед отказом исполняют одну и ту же работу
Требуется ли идентичность дисковых систем?	Нет	Нет	Да
Время восстановления работоспособности	15-90 с	15-90 с	<1 с

Для организации совместного использования данных в кластерах применяют *репликацию, коммутацию* (switching) или *зеркальное отображение* (mirroring). При *репликации* данные, записанные на жесткий диск первичного сервера, реплицируются через сетевое соединение между серверами на диск вторичного сервера. При *коммутации* каждый компонент кластера содержит собственный диск, однако все диски соединены одной шиной SCSI, с тем чтобы при отказе диска первичного сервера, его нагрузку принял на себя диск вторичного. Принцип зеркального отображения описан ранее, в разделе "Использование массивов RAID". В этом случае данные одновременно записываются на диски как первичного, так и вторичного серверов.

Кроме того, в каждом продукте предусмотрено различное *физическое* соединение компонентов кластера. Иногда серверы кластера соединяют между собой обычным сетевым соединением, скажем, Ethernet; иногда — через соответствующие разъемы. Возможны и другие решения, скажем, фабрика коммутируемых соединений (switched fabric connection) — если они поддерживаются конкретным программным продуктом.

Точно так же и аппаратные средства разных типов отличаются степенью гибкости. Не-

которые программы обслуживания кластеров могут работать только с вполне определенными типами оборудования. Это очень неудачное решение. Лучше использовать продукты, поддерживающие любые два сервера, а еще лучше — те, которые поддерживают серверы, работающие на разных платформах (например, один сервер на базе x.86, второй — Alpha). Отметим, что гибкость подобного рода не относится к отказоустойчивым кластерам: все серверы, входящие в них, должны быть идентичны.

Создание плана восстановления после аварии

Архивирование — важный, но не единственный аспект подготовки к восстановлению после аварии. Оно составляет только часть общего плана.

План восстановления после аварии представляет собой подробный документ, описывающий процесс восстановления работоспособности предприятия после какой-либо катастрофы. Очень важно создать план в письменной форме. В таком случае можно проинструктировать конкретных исполнителей даже в отсутствие разработчика плана. План должен быть настолько подробен, насколько это возможно, тогда для выполнения восстановительных работ не обязательно приглашать эксперта.

Примечание

В хороший план восстановления после аварии входят также детали, связанные не с техникой, а, например, с персоналом. Тем не менее, в основном он должен акцентировать внимание на технических проблемах.

Хорошо составленный план должен, удовлетворять следующим требованиям.

- Соответствовать указаниям руководства.
- Иметь ясно указанную цель восстановительных работ.
- Содержать четко заданный порядок передачи полномочий.
- Не содержать ни единой ошибки.
- Обеспечивать достаточную гибкость на случай изменения обстоятельств.

Эти элементы — отнюдь не перечень разделов идеального плана, однако их следует учесть для создания грамотного плана восстановления после аварий.

Очень важно заручиться поддержкой со стороны высшего руководства, поскольку для разработки и выполнения плана вам придется советоваться с вашим начальством. Полный план восстановления после аварий достаточно сложен и связан с решением множества вопросов, не относящихся к технике, поэтому его подготовку нельзя вести совершенно изолированно от остальных подразделений фирмы.

Ясность цели означает всего лишь то, что план должен соответствовать реальности. План — не диссертация по теории сетей или по узкоспециализированным задачам. Напротив, это должен быть отчетливо сформулированный документ, поясняющий методы возобновления работы сети и детально описывающий действия, необходимые для этого. Постороннюю информацию можно сохранить для презентации "Знакомство с сетью" для *нетехнического персонала* (или чего-нибудь подобного), однако в план следует включать только существенные инструкции. Определяя цель плана, вы должны ответить на такие вопросы.

- Какова область действия плана? Предназначен ли он для полного восстановления работы сети или просто для аварийного запуска ее на некоторое время, чтобы позднее заняться

полным ремонтом?
- Какую часть сети следует восстановить в первую очередь? Некоторые службы важнее остальных, однако их работа взаимосвязана.

Процесс восстановления значительно ускорится, если указать лиц, персонально ответственных как за подготовку к аварии, так и за восстановление после нее. Если отчетливо понимать свою задачу, то вы не потеряете время, решая вопросы полномочий. Кроме того, распределение ответственности гарантирует безусловное и эффективное выполнение работы — меньше шансов упустить из вида важные элементы.

Примечание

Один их элементов распределения ответственности заключается в определении "отклика" людей на это событие. Иными словами, когда происходит авария, каждый должен знать, что именно ему следует делать: оставаться дома и ни во что не вмешиваться либо приступить к работе по восстановлению сети. Кроме того, следует уведомить ваших деловых партнеров о задержке или о поставке, например, какого-нибудь товара из другого места в силу сложившихся обстоятельств.

Конечно, правильное распределение обязанностей при подготовке к аварии и последующем восстановлении очень важно, но всякая надежная система должна иметь некоторую избыточность. Успех или неудачу исполнения плана нельзя возлагать на плечи одного человека или на единственный компонент оборудования. Недопустимо, чтобы предотвращение аварии зависело только от одного элемента. Это означает следующее.

- Существует система подчинения, указывающая, кто кого замещает при отсутствии какого-нибудь служащего.
- Последние резервные копии должны храниться вне вашего офиса (здания), что уменьшает вероятность полного краха, возникающего вследствие катастрофы, разрушающей исходные данные вместе с их резервными копиями.
- При необходимости поврежденное оборудование немедленно заменяется.

И, наконец, хороший план отличается гибкостью. Самый лучший план — модульный. Он не полагается на умение единственного человека или совпадение специфических обстоятельств. Фирмы растут, служащие приходят и уходят, а программные и аппаратные средства изменяются. План должен быть таким, чтобы его можно было адаптировать к каждому изменению сети без полной переработки.

Кого привлечь к восстановлению сети

План восстановления сети разрабатывается несколькими специалистами -это итог совместного труда и усилий целой команды сотрудников:

- пользователей сети;
- персонала, обслуживающего сеть;
- людей, контролирующих наличные ресурсы.

Численность команды зависит от структуры вашей фирмы. Независимо от числа людей, занятых составлением плана, вы не сумеете создать полезный план, если не учтете пожелания сотрудников из всех указанных выше групп.

Примечание

Не забудьте учесть мнение еще одного человека - вашего босса. Ведь кто-то же должен подписывать чеки и одобрять покупку дополнительного оборудования.

Пользователи сети

Люди, лучше всех знающие, какие именно сетевые средства и компоненты имеют наибольшее значение — не обязательно те, кто отвечает за эксплуатацию сети. Как сетевой администратор, вы обязаны знать взаимосвязи между службами, но можете ли вы сказать, какие источники данных и серверы жизненно важны для работы вашей фирмы? Поэтому обязательно учтите замечания пользователей сети или их представителей.

Ремонтный персонал

В команде разработчиков плана восстановления после аварий, безусловно, важнейшую роль выполняет персонал, обслуживающий сеть, т.е. отвечающий за техническую сторону задачи. Именно им (т.е. вам) положено знать, какие именно системы восстановления (recovery systems) нужны, что есть у вас сегодня, стоимость требуемых дополнительных компонентов и источники получения дополнительной информации. Сетевой администратор должен сообщить пользователям достоверную информацию о том, что именно можно *физически* сделать в сети (например: "Нет, мы не можем реплицировать файловый сервер на внешний сервер с помощью модема на 33,6 Кбит/с"). Кроме того, в задачу персонала технической поддержки входит помощь тем сотрудникам, которые работают с определенными поставщиками и принимают решения.

Сетевой администратор обязан знать не только то, что необходимо для восстановления после аварии, но также и то, что нужно в настоящий момент. Например, если в сервере используется SCSI-интерфейс, бессмысленно покупать для него устройство архивирования с IDE-интерфейсом. Это очевидно, однако нередко упускается из вида. Я припоминаю один случай, который произошел несколько лет назад, когда коммерческий директор купил про запас несколько жестких дисков и контроллеров, чтобы иметь их под рукой на случай отказа основных дисков. К сожалению, ему было невдомек, какой интерфейс используется в существующих контроллерах. Таким образом, когда настал час замены одного из дисковых контроллеров на запасной, оказалось, что закупленная плата контроллера VL-Bus не может работать с сервером ISA/PCI.

Люди, контролирующие ресурсы

Сетевой администратор заботится о технической стороне дела, но коммерческому директору приходится учитывать стоимость и распределение ресурсов. Иногда план восстановления после аварий далек от оптимального с финансовой точки зрения. Поэтому коммерческий директор обязан составить калькуляцию, чтобы убедиться, что план восстановления сети не потребует чрезмерных затрат.

Кроме того, коммерческий директор должен контролировать инвентарную опись сетевого оборудования, которую мы обсуждали в гл. 14. Инвентаризация оборудования имеет большое значение, поскольку позволяет установить, насколько устарело оборудование, какие детали следует закупить в первую очередь, а какие пустить на запчасти.

Содержание плана восстановления

Детальное содержание плана зависит от конструкции конкретной сети. Однако, как правило, план восстановления после аварии содержит следующее.

- Определение цели, описывающее состояние сети после ее восстановления.
- Информация о связях всех участников восстановительных работ.
- Список ответственных за восстановление конкретных элементов.
- Инструкции по восстановлению:
    - различных сетевых серверов (файлового, приложений, DHCP, WINS, Web), а также их запуску вместе с зависимыми средствами обслуживания;

Примечание

Взаимозависимость компонентов очень важна! В процессе восстановления следует убедиться, что ремонтники свели воедино все части сети надлежащим образом. В противном случае сеть будет работать неправильно, если заработает вообще.

- данных из архивов;
- данных, хранящихся в RAID-массиве.

В приложение С "Пример плана восстановления сети" включены выдержки из реального плана восстановления сети, демонстрирующие ту степень подробности, которой желательно придерживаться и вам. Создание плана восстановления после аварии занимает немало времени и труда. Так, один из известных мне планов представляет собой документ на 145 страницах, однако восстановить и запустить сеть с его помощью без полного штата ремонтников, вероятно, невозможно.

Завершающие рекомендации

В сущности, планы восстановления после аварии — самая важная часть сетевой документации. Иными словами, они должны рассматриваться и тестироваться во взаимосвязи с остальной сетевой документацией. Прежде чем положиться на план, убедитесь в его работоспособности и соответствии применяемым версиям программных продуктов.

Во-первых, проверьте точность плана. По мере написания каждой части, заставляйте кого-нибудь выполнять ваши инструкции. Это гарантирует, что в плане предусмотрено все, что необходимо, а ваши инструкции точны. Идеальный исполнитель *не должен* уметь выполнять то, что предписано инструкцией — восстанавливать данные с помощью резервных копий, устанавливать сервер DHCP и т.п. Дело в том, что такой исполнитель не станет замечать пропущенные детали и исправлять ваши ошибки, тогда как опытный сотрудник сможет сделать это автоматически и не задумываясь. Можно также подобрать какого-нибудь чрезвычайно требовательного человека. Однако вы никогда не должны проверять инструкции самостоятельно, за исключением тех ситуаций, когда это просто неизбежно. *Любой* человек сумеет проверить ваши инструкции лучше вас.

Во-вторых, проверьте пригодность вашего плана. Сработает ли он так, как вы его написали? Все ли его элементы не зависят от специальных условий и взаимодействуют друг с другом так, как предусмотрено? Если хотя бы на один из этих вопросов вы ответите "нет", доработайте план и повторите испытания.

Наконец, сохраните в надежном месте несколько датированных *твердых* копий плана. Если одна копия пропадет во время аварии, у вас останется вторая. Если у вас уже есть несколько планов, вы сумеете установить по датам, с какой версией имеете дело сегодня.

Вызов варягов: центры восстановления данных

В некоторых случаях сеть не удается полностью восстановить после аварии. Так, ваши архивы могут оказаться не пригодными для работы либо вообще разрушиться. Но прежде чем объявлять пользователям, что все результаты их месячных трудов безвозвратно погибли, попробуйте обратиться в центр восстановления данных. Эти центры укомплектованы экспертами по извлечению данных из различных носителей (чаще всего — жестких дисков), доступ к которым обычным путем невозможен.

Центры восстановления данных неодинаковы. Некоторые из них (фактически те, что появились первыми) действительно укомплектованы *чрезвычайно* компетентными специалистами по восстановлению и запуску неисправных жестких дисков. Используя свое мастерство, они могут "воскресить" диск, скопировать его содержимое на другой носитель, а затем вернуть вам данные на новом носителе.

Совет

Если вас заинтересовал этот вопрос, ознакомьтесь с книгой Марка Минаси "Модернизация и ремонт ПК. Полное руководство", издательство BEK+, 1999г. (Mark Minasi "The Complete PC Upgrade and Maintenance Guide", Sybex, 1998 г.).Там вы узнаете, каким образом можно восстановить "мертвый" жесткий диск, чтобы извлечь данные, хранившиеся на нем.

Кроме того, некоторые организации могут извлекать искаженные данные, невосстановимые обычными методами. Они работают на самом низком (двоичном) уровне, считывая данные с "мертвого" носителя (причем, если проблема достаточно серьезна, они даже вскрывают герметичную камеру с жесткими дисками), а затем копируют данные на свой носитель. Вся работа обычно занимает 1—2 дня, плюс время на доставку.

Стоимость восстановления данных зависит от:

- метода восстановления (как правило, ремонт жесткого диска обходится дешевле, но при этом не гарантируется восстановление данных);
- срочности работы;
- объема восстановленных данных.

Совет

Обдумайте возможность сохранения жизненно важных данных на особом физическом диске, т.е. отдельно от данных, замена которых не вызывает проблем. Специалисты не могут восстанавливать данные выборочно. Иными словами, если файлы данных и системные файлы хранятся на одном физическом диске, вы не сумеете сэкономить деньги, попросив в центре восстановить только файлы данных, даже если они находятся в двух разных логических разделах.

До недавних пор вы должны были отослать жесткий диск в центр восстановления данных и получить взамен уже восстановленные данные. Это означало как минимум двухдневную задержку. Службы дистанционного восстановления данных могут решать некоторые проблемы, связанные с программным обеспечением, при этом диск не требуется куда-то отсылать, а иногда его можно даже не вынимать из компьютера. Используя прямое удаленное соединение, центр восстановления данных может решить ваши проблемы по телефонной линии. На конец 1998 г. такую услугу оказывал единственный центр восстановления данных — OnTrack.

Выводы

Авария может произойти по самым разным причинам, как техническим, так и организационным. Но, независимо от этого, ваша цель одна: восстановление и запуск сети. Для этого нужен набор хороших резервных копий и корректный план восстановления после аварии. Полезны также удачливость и мастерство, в противном случае вам помогут только архивы и предварительная подготовка.

Большую часть усилий по восстановлению после аварии следует затратить *до* аварии. Именно в это время вы должны аккуратно выполнять архивирование, проверять резервные копии и тщательно хранить их так, чтобы данные можно было быстро найти и восстановить. Кроме того, еще до аварии вы можете задействовать отказоустойчивую систему, например, RAID-массив, репликацию данных и/или кластеризацию серверов.

На случай, если подготовительные меры не сработают, следует тщательно разработать план восстановления сети после аварии. Для успешного выполнения этого плана в него следует включить подробное описание методов восстановления и запуска сети. Работа должна выполняться по возможности быстро и эффективно, начиная с наиболее важных операций. Если же вы не смогли полностью восстановить данные, обратитесь в центры восстановления данных. Конечно, намного дешевле изначально позаботиться о сохранности данных, чем отсылать их носители в центр — все же расстаться с деньгами легче, чем навсегда утратить данные.

Итак, мы подошли к концу. Если вы осилили эту книгу, значит вы приобрели достаточно знаний, чтобы спроектировать локальную сеть, построить ее, запустить и поддерживать работу. Для вас уже не является тайной работа кабельной системы. Вы знаете, как построить надежный сервер, соответствующий вашим требованиям и выбрать для него клиентное оборудование. Вы получили представление о приложениях, которые можно выполнять в сети, а при небольшом везении, но большой заботе и надлежащих предосторожностях сумеете содержать сеть в порядке и избежать аварий, — а если вам не повезет, то вы все-таки самостоятельно справитесь с проблемой.

Не довольно ли? В конце книги вы найдете словарь использованных терминов. В приложениях можно найти дополнительные источники информации.

- Список полезных адресов Web-узлов, доступных в интерактивном режиме (online).
- Несколько образцов форм, которые можно использовать для управления сетью.
- Выборку из действующего руководства по восстановлению после аварии.
- Ответы на упражнения, которые входят в каждую главу.

Спасибо за внимание и удачи вам!

Упражнение 16

Предположим, что сегодня пятница. Некоторые документы Word были инфицированы макровирусом, заставляющим пользователя сохранять каждое изменение файла в новом документе, т.е. этот вирус нетрудно обнаружить. Люди, использующие файлы, заявляют, что не замечали ничего подозрительного, когда редактировали файлы в течение недели. Точный день они не помнят, но знают, что вчера все было нормально. Можно предположить, что файлы инфицированы при просмотре либо вчера, либо сегодня.

1. Какие файлы следует восстановить, чтобы избавиться от вируса и предотвратить дальнейшее инфицирование?

2. Каким образом можно восстановить неинфицированные файлы без перезаписи отредактированных файлов на тот же накопитель?
3. Допустим, вы сумели установить, что инфицирование произошло в течение нескольких последних дней. Какой тип архивирования может в наибольшей мере облегчить работу по восстановлению? Почему?
4. Перечислите типы RAID-массивов, рассмотренные в этой главе.
5. Какой тип RAID-массива можно использовать в кластере, состоящем из двух серверов?
6. Время восстановления отказоустойчивого кластера после сбоя составляет:

   A. <15 с.
   B. 15-90 с.
   C. <10 с.
   D. Ничего из перечисленного выше.

7. Ответьте, "да" или "нет". Использование чередующихся наборов с контролем четности увеличивает время, необходимое на выполнение операций считывания с диска по сравнению с единичным диском.
8. Какой метод защиты данных можно использовать при распространении по сети обновляющей копии непосредственно с основной базой данных?
9. Почему время восстановления после сбоя у отказоустойчивого кластера меньше, чем у кластера типа активный/активный?
10. Чем различаются методы восстановления после сбоя кластеров активный/ активный и активный/резервный? Как это влияет на время восстановления после сбоя?

Приложение А

Ресурсы Internet

В 90-х гг. основной предметной областью автора книги вместо операционной системы персонального компьютера стала сеть Web.

Компьютер — средство, позволяющее вам получать информацию, а Web это и есть информация в чистом виде. Все прошедшие годы я собирала новые драйверы, помешенные на электронные доски объявлений, получала документацию от служб, возвращающих факсимильные сообщения (fax-back services), которые в свою очередь требовали от вас знания номера нужного документа, получала техническую поддержку по телефону или из групп новостей и исследовала справочные материалы в бесчисленном множестве статей в журналах и газетах. Но их уже нет — Web-паутина свела всю требуемую информацию в одно место. Web — это очень привлекательно. Вы можете не найти здесь ответы на все вопросы, но можете получить, по крайней мере, исходную информацию для начала поиска ответов на них.

Все изложенное ниже представляет собой набор ссылок на некоторые узлы, которые автор по тем или иным соображениям считает полезными. Некоторые из них информативны, другие — прекрасные источники утилит, а третьи — предоставляют полезную справочную информацию. Если вы захотите сделать небольшие покупки, можете воспользоваться включенными сюда ссылками на пару онлайновых торговых центров. Набор ссылок совершенно *субъективен*, так что если не найдете свой излюбленный узел, не принимайте это близко к сердцу. Никто не платил автору за включение того или иного узла в список. Просто это — ссылки, которые автор считает полезными.

Эти ссылки также можно найти и на Web-узле издательства Sybex. Вы можете получить к ним доступ в Web, посетив сайт Sybex по адресу `http://www.sybex.com`. Для нахождения ссылок и другой информации по тематике этой книги, щелкните на кнопке **Catalog**, введите в поле поиска число **2258** и нажмите на клавишу **Enter**.

Сделаем два замечания. Во-первых, динамическая природа Web означает, что ссылки имеют склонность перемещаться или вообще пропадать. Я постаралась предоставить ссылки как можно точнее, но не могу контролировать их, и не могу запретить кому-либо перемещать или удалять страницы. (Web-узел Microsoft, например, регулярно перестраивается.) Если ссылка больше не работает, попытайтесь поискать ее по ключевому слову в **Alta Vista** (мой любимый поисковый сервер) по адресу `http://www.altavista.com/cgi-bin/query?pg=aq&what=web`. Если ссылка на страницу Microsoft разрушена, попытайтесь использовать карту узла для нахождения искомого тематического раздела.

Во-вторых, сейчас существует так много узлов производителей, что я даже и не пыталась все перечислить, а вместо этого сконцентрировалась на паре самых крупных. Если здесь не указана ссылка на интересующего вас производителя, попытайтесь ввести имя требуемой компании в адресную строку своего броузера (`www.название компании.com`). Если это не приведет к успеху, произведите поиск в Alta Vista по названию продукта или компании.

Информация

Эти ссылки расскажут, как должны работать различные, необходимые вам вещи и предоставить начальную информацию. Если вы ищете информацию по организации сетей или иную справочную информацию, побывайте в следующих местах.

Ссылки на каталог Запросов комментариев

```
http://www.rfc-editor.org/rfc.html
```

Запросы комментариев (Request for Comments — RFC) представляют собой документы, описывающие работу стандартов Internet. Окончательную версию документа называют *стандартом*. Версию, находящуюся в данное время в работе (отсюда название "Запросы комментариев") называют *предлагаемым стандартом (proposal standard)* или *рабочим стандартом (draft standard)*. Этот узел не содержит ссылки на все документы, но зато ссылается на поисковые серверы или страницы RFC, которые позволят вам найти требуемый документ.

Избранный механизм поиска RFC

```
http://info.internet.isi.edu/7c/in-notes/rfc/.cache
```

Этот механизм позволит вам производить поиск по ключевым словам, возвращая все RFC-запросы, в том числе выбранные ключевые слова.

Указатели IEEE

```
http://www.latech.edu/tech/IEEE/ieeeref.html
```

Если вам нужны детальные сведения о каких-либо окончательных версиях стандартов IEEE, например Ethernet или Token Ring, поищите их в этом списке, упорядоченном по номерам комитетов.

PC Webopaedia

```
http://webopaedia.internet.com/
```

Вам потребуется этот узел. PC Webopaedia не только содержит термины, относящиеся к ПК, и дает вам для ознакомления список связанных между собой терминов, но также предоставляет ссылки на узлы, относящиеся к запрашиваемым терминам.

Бюллетень вирусов

```
http://www.virusbtn.com/
```

Обращайтесь сюда за общей информацией о вирусах. Из этой страницы вы сможете получить доступ к обзорам по антивирусному программному обеспечению, к списку последних появившихся вирусов и отчетов о том, какие вирусы чаще всего упоминаются в списках. Это прекрасная отправная точка для получения информации о вирусах.

Онлайновый мир тонких сетей

```
http://www.thinword.com
```

Прекрасный узел для получения основных сведений об организации тонких клиентных сетей. Сам он не содержит детальной информации, но является источником полезных ссылок.

Онлайновые журналы

Здесь приведен список некоторых онлайновых журналов, имеющих отношение к информационным технологиям, используемым автором чаще других для получения полезной информации или слухов, циркулирующих в данной отрасли.

Windows NT Magazines

```
http://www.winntmag.com/
```

Онлайновая версия известного журнала Windows NT Magazine. Да, именно этот журнал упомянут в списке первым, и я не стала бы этого делать, если бы он не был и в самом деле хорош. Домашняя страничка предлагает ссылки на источники информации о различных событиях, архивы статей и другие технические публикации Duke Communications. Все статьи появляются в сети через три месяца после их опубликования, а некоторые изначально были опубликованы именно в Web.

WUGNet

```
http://www.wugnet.com/
```

С сетью WUGNet (Windows User Group Network — Сеть группы пользователей Windows) я впервые столкнулась при работе с CompuServe. В то время это был деятельный и полезный форум, позволяющий получить ответы на вопросы о Windows. С тех пор форум расширился и превратился в Web-узел, являющийся источником обзоров, новостей и другой полезной информации по Windows. Ежедневные обзоры Пауля Зарота (Paul Thurrot) просто прекрасны.

CNet News

```
http://www.news.com/?st.en.gp.tbtop.News
```

Здесь не так много чисто технических новостей, но это хорошее место, где можно найти различные новости компьютерной индустрии и ссылки на соответствующие узлы. Узел CNet является хорошим источником обзоров продукции.

IDG Online

```
http://www.idg.com
```

Этот узел содержит ссылки на заголовки публикаций издательства IDG типа PC world и Info World.

Производители

Если вы хотите найти техническую документацию на имеющиеся у вас комплектующие, белые книги и технические отчеты или новейшую информацию о перспективной продукции, или оперативные исправления, узел производителя будет лучшей отправной точкой. Здесь не перечисляются все производители продукции, имеющей отношение к сетям. Укажем

несколько официальных узлов.

Web-узел Microsoft

```
http://www.microsoft.com/
```

Здесь можно найти информацию обо всем, что выпускает Microsoft. Ищете ли вы информацию для пользователей или последние новости для разработчиков в сети MSDN (Microsoft Developer Network — Сеть Microsoft для разработчиков) — все это можно найти здесь. Я провела на этом узле немало времени.

Web-узел Novell

```
http://novell.com/
```

Как и Web-узел Microsoft, узел Novell очень полезен при поиске документации и технических описаний. Как представляется автору, карта этого узла немного понятнее карты узла Microsoft, возможно, благодаря менее сложной структуре узла.

Домашняя страница Linux

```
http://www.linux.org/
```

Хотите получить информацию об операционной системе Linux, узнать что с ней можно делать или где можно получить копию? Посетите этот узел, который создан энтузиастами, что, безусловно, отражается на его содержании, но он не более тенденциозен, чем узлы Microsoft или Novell. Однако данный узел имеет более удачный логотип.

Домашняя страница технологии Java

```
http://www.java.sun.com/
```

Вас интересует возможность узнать побольше о технологии Java? Это официальный узел, разработанный и запущенный сотрудниками фирмы Sun Microsystems, создавшими этот язык разработки программ. Вы можете найти здесь новости, документацию, примеры и техническую поддержку.

Системы Citrix

```
http://www.citrix.com/
```

Если вы интересуетесь тонкими клиентными технологиями, то вы сможете ознакомиться с ними в узле ThinWord или в разделе Windows Terminal узла Microsoft. Не забудьте познакомиться также с информацией на узле Citrix. Этот узел содержит ссылки на соответствующие разделы Windows Terminal Server узла Microsoft, так что вы сможете начать с него свой поиск.

Загрузка и онлайновые утилиты

Программное обеспечение редко бывает полностью завершенным, но даже если это так, всегда появляются новые усовершенствования и улучшения. Посетите указанные далее

узлы для обновления сетевого программного обеспечения или клиентной операционной системы.

Система изнутри

```
http://www.sysinternal.com/
```

Узел Марка Руссиновича (Mark Russinovich) и Брюса Когсвелла (Bruce Cogswell) — прекрасный источник информации о мощных инструментальных средствах и современных операционных системах Windows. Не пропустите страничку утилит для NT. Некоторые средства можно загрузить бесплатно, но помните, что в этом мире любая вещь стоит денег, даже если она далека от совершенства.

Обновления Windows NT Server

```
http://www.microsoft.com/NTServer/all/downloads.asp
```

Эта страница содержит ссылки на все служебные пакеты Windows Service Pack (исправления ошибок и обновления), а также ссылки на инструментальные средства, аналогичные Zero Administration и бета-версии программного обеспечения, предназначенного для тестирования.

Высокоуровневая конфиденциальность

```
http://www.pgpi.com/download/
```

Если вам требуется загрузить себе личный и общий ключи, вы можете сделать это на данной странице. На ней также есть соответствующая документация.

Tucows

```
http://tucows.bealenet.com/
```

Прекрасный многоцелевой узел для выбора бесплатного (freeware) и условно бесплатного (shareware) программного обеспечения практически для любой компьютерной платформы. Программное обеспечение классифицировано и описано так, что вам будет легко выбрать то, что вы хотите получить.

Центр условно и полностью бесплатного программного обеспечения NoNags

```
http://www.nonags.com/
```

Хотите получить бесплатное программное обеспечение? Посетите этот узел. Большая его часть не очень полезна (ведь бесплатно же), но иногда в нем можно найти нечто стоящее.

Равноправная поддержка

Иногда можно обойтись без чтения нединамичных, быстро устаревающих статей, прибегнув к услугам консультанта, который сможет ответить на конкретный вопрос и не запросит с вас 150 $ за привилегию задавать ему вопросы или за выслушивание туманных разглаголь-

ствований. Когда вам потребуется поддержка такого типа, вам следует попробовать обратиться к онлайновому форуму. Здесь не всегда ждут каких-либо вопросов, и многие форумы равноправной поддержки (peer support forum) не предоставляют достаточного трафика, что несколько снижает их полезность, но, тем не менее, они заслуживают краткого упоминания.

Совет

В настоящее время автор предполагает отказаться от использования групп новостей из-за большого количества содержащегося в них "мусора". Однако если вы заинтересованы в получении информации о различных продуктах, то можете найти в домене Nowell информацию о фирме Novell (такую, как в `nowell.zenworks.install`), а в домене Microsoft - о фирме Microsoft (такую, как в `microsoft.public.sms.admin`). Используйте свой инструмент чтения новостей для просмотра узла с адресом, содержащим имя интересующей вас компании, - и вы сможете найти группу новостей, отведенную для нее.

Онлайновые технические форумы Windows NT Magazine

`http://www.winntmag/com/Forums/Forum.cfm`

Группа новостей типа Q&A (Ответы и вопросы), без всякой чепухи. Эти форумы содержат информацию о многих направлениях, начиная от различных вопросов о Windows 2000, и кончая информацией о терминальном сервере Windows и сервере SQL.

Равноправная поддержка Microsoft TechNet

`http://207.109.70.246/technet/peer/default.asp`

Это другой форум, спроектированный специально для предоставления пользователям равноправной поддержки. Трафик, предоставленный разделам с информацией о NT и вопросам организации сетей, вполне приемлемый, но этот форум не такой удобный, каким ему следовало бы быть. Вы должны знать, что и где в нем находится, чтобы найти нужные данные (т.е. вам надо каким-то образом за этим следить), а используемый почтовый формат означает, что длинные строки в тексте не форматируются. Такой текст тяжело читать. Однако в нем рассматривается широкий круг вопросов, и вы имеете много шансов получить ответ или, как минимум, отклик.

Посещение магазинов

Посетите следующие узлы — онлайновые магазины.

Путеводитель по онлайновым магазинам фирмы CNet

`http://www.shopper.com/?st.ne.nav.sh`

Будете вы делать покупки или нет с помощью этого путеводителя, вы сможете определить реальную стоимость всего того, что вам необходимо. Введите тип продукции, которую вы ищете, и механизм поиска возвратит список ее производителей, онлайновых пунктов продажи вместе с информацией о стоимости и отгрузке. Автор книги умышленно исключила большую часть информации о стоимости, поскольку эти сведения в узлах за время выхода книги могут устареть.

JDR Microdevices

```
http://www.jdr.com/
```

У фирмы JDR Microdevices хороший печатный каталог продукции, онлайновая версия которого также имеется на ее узле. Это прекрасный источник сведений почти обо всем, что вам нужно для установки в сеть: память, периферийные устройства, инструменты. Вы вводите их названия, и они появляются перед вами вместе с ценой.

Я надеюсь, что все изложенное выше даст вам хорошую отправную информацию для онлайнового поиска требуемых ресурсов. Приятного путешествия!

Приложение В

Сетевые формы

Таблица сведений о рабочей станции	
Имя ПК	
Физический сетевой адрес:	
Логический сетевой адрес:	
Тип сетевой платы:	
	IRQ
	Адреса ОЗУ сетевой платы:
	Адреса ПЗУ сетевой платы:
	Базовые адреса ввода/вывода:
	Прочее:
Сведения о жестком диске (из CMOS)	
Тип видеоплаты:	
	IRQ:
	Адреса ОЗУ:
	Адреса ПЗУ:
Дополнительные сведения:	
Прочее оборудование:	
Серийный номер:	

Рис. В.1. Таблица сведений о рабочей станции

Таблица сведений о сервере	
Физический адрес узла сети:	
Имя сервера:	
Сетевая операционная система:	
Тип сетевой платы:	
	IRQ:
	Адреса ОЗУ сетевой платы:
	Адреса ПЗУ сетевой платы:
	Базовые адреса ввода/вывода:
	Прочее:
Сведения о жестком диске (из CMOS):	
Тип видеоплаты:	
	IRQ:
	Адреса ОЗУ:
	Адреса ПЗУ:
Дополнительные сведения:	
Прочее оборудование:	
Серийный номер:	

Рис. В.2. Таблица сведений о сервере

Специальное оборудование	
Описание:	Установки:

Рис. В.3. Специальное оборудование

Сведения о сети
Физическая топология:
Логическая топология:
Спецификация кабелей по всей сети:

Рис. В.4. Сведения о сети

Приложение C

Пример плана восстановления сети

Вы еще не знаете, насколько детальным должен быть план восстановления после аварии? Замысел его состоит в том, чтобы работоспособность сети мог восстановить любой человек, умеющий пользоваться компьютером. Разумеется, здесь неуместно обучать основным приемам работы мышью, однако в прочих отношениях документ должен быть простым и подробным — это позволит избежать ошибок. Не стоит полагаться, что ремонтом сети займется сетевой администратор или лицо равной ему квалификации.

Ниже описан метод установки средства обслуживания DHCP и установки диапазона адресов сервера DHCP. Установка позволит восстановить IP-адреса, выделенные для сети Windows NT. Разумеется, здесь не описана полная процедура установки сервера DHCP (см. "Mastering Windows NT 4", издательство Sybex, 1999 г.), а просто приведен пример плана восстановления после аварии.

Примечание

Обратите внимание: в инструкциях предусматриваются не только те задачи, которые необходимо решить, но и какие инструменты ему для этого необходимы. Кроме того, они позволяют идентифицировать компьютер, на котором с помощью этой инструкции устанавливается соответствующее программное средство. (Отнеситесь со всей серьезностью к указанию имен серверов!)

Восстановление IP-адресов, выделенных сети

Для автоматического назначения IP-адресов сети вы должны установить средство обслуживания DHCP (Dynamic Host Configuration Protocol — протокол динамического конфигурирования компьютера) на сервере PALADIN и диапазон адресов (scope), которые могут выделяться сети.

Установка службы DHCP

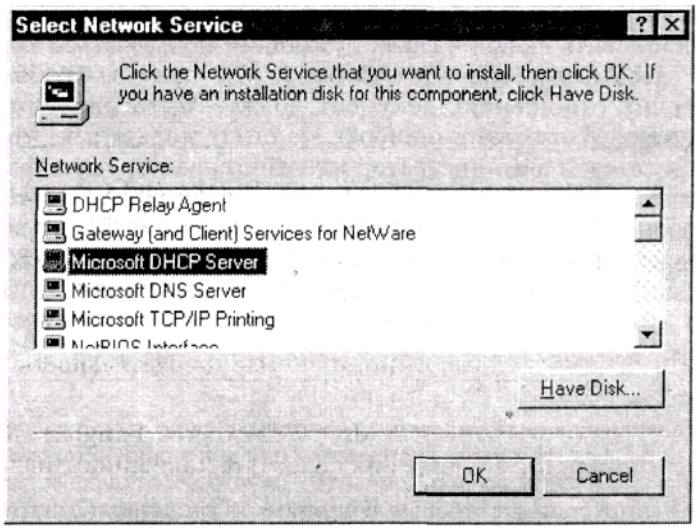
1. Вставьте установочный компакт-диск Windows NT Server 4 в устройство CD-ROM сервера PALADIN.
2. Запустите аплет **Network (Сеть)** на **Control Panel (Панель управления)** и выберите вкладку **Services (Службы)**. Щелкните на кнопке **Add (Добавить)**.

Примечание

Если элемент Microsoft DHCP Server уже находится в списке установленных средств, то повторная установка не нужна. Пропустите следующий раздел, вплоть до установки диапазона IP-адресов.

3. Выберите в списке элемент Microsoft DHCP Server (см. ниже) и щелкните на кнопке **ОК**. Укажите путь к установочному компакт-диску Windows NT Server (Предположим,

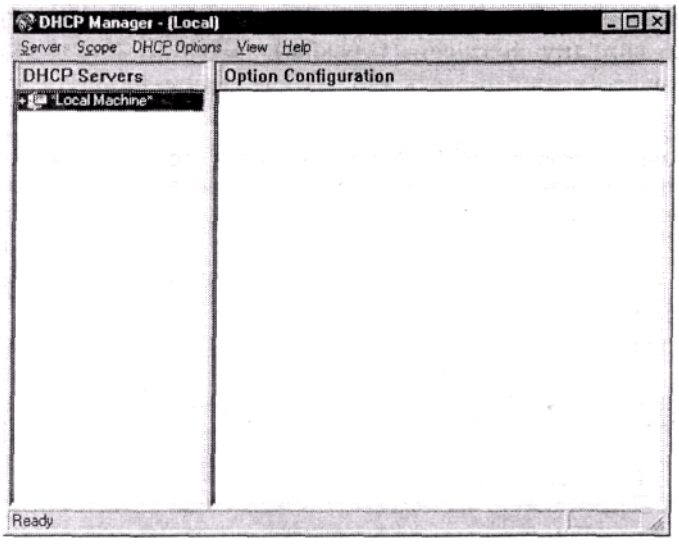
диску G:).



4. На экране появится информационное диалоговое окно с предложением изменить все IP-адреса локальной сетевой платы (плат) на статические адреса. Щелкните на кнопке **ОК.**
5. Программа установки скопирует на сервер необходимые файлы. Перезагрузите компьютер.

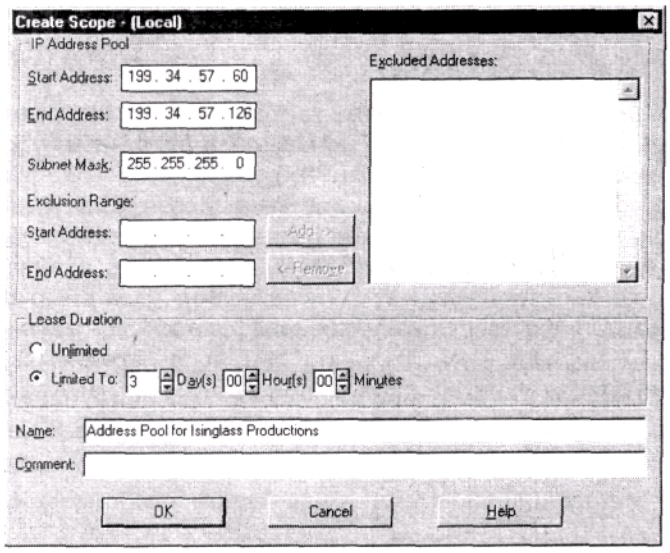
Создание адресного пула

1. Откройте DHCP Manager (диспетчер DHCP), воспользовавшись командой меню **Programs/Administrative Tools (Программы/Административные инструменты)**. Вы увидите диалоговое окно, показанное ниже.



2. Выберите в меню команду **Scope/Create (Диапазон/Создать)**. На экране появится диалоговое окно **Create Scope (Создание диапазона)**.
3. В поле **Start Address (Начальный адрес)** введите 199.34.57.60. В поле End Address (Конечный адрес) введите 199.34.57.126. В поле **Subnet Mask (Маска подсети)** введите 255.255.255.0.

4. Установите значение **Leased Duration (Продолжительность выделения)** равным 3 дням, 0 часам, 0 минутам.
5. Присвойте регистру имя "Address Pool for Isinglass Production" (адресный пул фирмы Isinglass Production). Заполненное диалоговое окно выглядит так.



6. Щелкните на кнопке **ОК**. На экране появится диалоговое окно, сообщающее о том, что диапазон адресов создан, но не активизирован, и предлагающее активизировать его. Чтобы активизировать и немедленно задействовать этот диапазон адресов, щелкните на кнопке **Yes (Да)**. В данном случае перезагружать компьютер не надо.

Приложение D

Ответы на упражнения

Упражнение 1

Тип кабеля	Предельная скорость передачи данных	Максимально допустимая длина рабочего участка	Используемые средства подавления помех	Используемый разъем
Коаксиальный	**10 Мбит/с**	750 м	**Медная оплетка передающих проводников**	BNC
Неэкранированная витая пара (UTP)	100 Мбит/с	90м	Скручивание пар проводников	**RJ-45**
Экранированная витая пара	100 Мбит/с	**90м**	Скручивание пар в сочетании с металлическим экраном	**D-shell**
Оптоволокно	155 Мбит/с	**10 км**	Специальные средства не используются	ST или SMA

Упражнение 2

1. Если сеть отказывает из-за разрыва кабеля, неисправность проще устранить в сети, построенной по физической звездообразной топологии "звезда" (в этом случае сетевые соединения прокладываются в радиальном направлении к центральному концентратору). Это обусловлено тем, что каждое сетевое соединение с центральным коммутационным узлом прокладываются отдельно. В то же время в сетях с шинной и кольцевой топологиями на всем протяжении сети используют общую магистраль. Таким образом, любой разрыв кабеля нарушает работу всей сети.
2. Первая сеть — 10BaseT Ethernet. В ней используют физическую звездообразную топологию, но логическая топология — шинная. Вторая — сеть Token Ring. В ней используют физическую звездообразную топологию, но логическая топология - кольцевая.
3. Никакое. Кадры обоих типов совместимы без трансляции.
4. 802.4
5. Gigabit Ethernet.

Упражнение 3

1. В данном случае для пересылки данных можно использовать протоколы IPX/SPX и TCP/IP. Протокол NetBEUI использовать невозможно, поскольку он относится к немаршрутизируемым, а на приведенном рисунке показано маршрутизированное соединение.
2. На компьютере, работающем под управлением Windows 98, можно использовать драйверы ODI и NDIS. Однако на компьютере, работающем под управлением DOS, можно использовать только драйверы ODI, поскольку операционная система DOS работает в режиме реального времени, а драйверы NDIS работают в защищенном режиме.
3. TCP/IP.
4. 32, 128.
5. Перехватчик (редиректор).
6. Гнездом.
7. Драйвер. Включает как транспортный протокол, так и драйвер устройства, что позволяет операционной системе взаимодействовать с сетью.

Упражнение 4

1. В данном случае установка платы невозможна. Хотя оба IRQ свободны, ни один из них не поддерживается сетевой платой. Для ее установки вы должны изменить IRQ, используемые другой платой, с тем чтобы данная плата использовала одно из свободных IRQ и освободила либо IRQ 10, либо 11.
2. B.
3. Кабели, проложенные под полом, должны по возможности располагаться в середине комнаты. Это облегчает доступ к ним, когда он понадобится. Кабели, размещенные возле стены, при расстановке мебели желательно помещать под столами.
4. Нет. Диапазоны должны быть раздельными, поскольку данные, относящиеся к каждому устройству, должны сохраняться в собственном диапазоне адресов ввода/вывода.

Упражнение 5

1. A.
2. Промежуточное сохранение для контроля целостности пакета.
3. Метод OSPF (Open Shortest Path First - маршрутизация с предпочтением кратчайшего пути).

Упражнение 6

1. Если необходимое вам программное обеспечение не поддерживает ретрансляцию кадров либо вы находитесь в местности с ненадежными линиями связи, но хотите, чтобы ваша глобальная сеть обеспечивала контроль ошибок, предпочтительно использовать протокол X.25.
2. B, C.
3. Протокол L2TP (Layer 2 Transfer Protocol — протокол туннелирования 2-го уровня).
4. Скорость могла бы соответствовать параметрам канала T1, однако фактически вы не сможете дать ответ только на основе предоставленной информации, поскольку CIR зависит не только от параметров линии связи, но также и от сетевого трафика.

Упражнение 7

1. Кэш L1 представляет собой небольшую часть SRAM, размещенную внутри процессора. Он используется для хранения кодов и данных, доступ к которым предоставлялся последний раз. Хранение этой информации в кэше L1 ускоряет доступ к ней по сравнению с обращением к основной памяти.
2. Как правило, процессор работает быстрее, поскольку оперативная память функционирует с тактовой частотой системной платы, а внутренняя тактовая частота процессора может превышать частоту системной платы в несколько раз.
3. 8; 33.
4. B.
5. См. ниже текст, выделенный жирным шрифтом.

Тип SCSI	Описание
SCSI-2	Используется 50-штыревой коннектор, **8**-битовая шина. Обеспечивается скорость передачи данных 4 Мбит/с
Wide SCSI	Используется **68**-штыревой разъем и 16-битовая шина
Fast SCSI	Аналогичен обычному SCSI-интерфейсу, но тактовая частота повышена вдвое. Обеспечивается скорость передачи данных 10 Мбит/с
Fast and Wide SCSI	Объединяет 16-битовую шину интерфейса Wide SCSI и тактовую частоту интерфейса **Fast SCSI**. Обеспечивает скорость передачи данных **20** Мбит/с
Ultra SCSI	Использует 8-битовую шину, но поддерживает скорость передачи данных 20 Мбит/с
Ultra Wide SCSI/SCSI-3	Используется 16-битовая шина. Обеспечивается скорость передачи данных **40** Мбит/с
Ultra2 SCSI	Используется **8**-битовая шина. Обеспечивается скорость передачи данных 40 Мбит/с
Ultra2 SCSI Wide	Используется 16-битовая шина. Обеспечивается скорость передачи данных **80** Мбит/с

6. В автономных UPS электроэнергия на преобразователь подается от аккумулятора, чем улучшается качество электроэнергии. Когда внешнее электропитание отключается, на переключение питания от аккумулятора время не затрачивается. В коммутируемых UPS электроэнергия подается на устройство непосредственно из внешнего источника, а некоторая ее часть расходуется на подзарядку аккумулятора. При отключении электропитания UPS необходимо около 4 мс, чтобы переключить питание на аккумулятор (на этот промежуток времени электропитание устройства прерывается).

Упражнение 8

1. Файловыми (серверами).
2. В ленточных накопителях данные считываются методом последовательного доступа. Это означает, что для считывания некоторой части данных устройство должно последовательно перейти к месту расположения этих данных на ленте.
3. A. Кассеты DLT, поскольку они могут вмещать до 53 Гбайт данных на одну кассету.
4. Память принтера, поскольку принтер должен сохранять в собственной памяти все печатные задания без поддержки памяти сервера печати.
5. Пул (pooling).
6. Около 40 Кбит/с.
7. B.
8. 64 Кбит/с.
9. Дисковые серверы сохраняют карту структуры каталогов на клиентных машинах, в то время как файловые серверы сохраняют ее на сервере.

Упражнение 9

1. Windows NT Workstation.
2. Нет. Память SGRAM однопортовая.
3. Сетевая. Если сетевая поддержка отсутствует, они не смогут связываться с сетью и получать доступ к приложениям, исполняемым на сервере.
4. B.
5. Merced.
6. D.
7. Поддержки видео.

Упражнение 10

1. У пользователя нет учетной записи на Windows NT Workstation, предоставляющей доступ к общему ресурсу. После ее установки пользователь получит возможность получить доступ к ресурсу без ввода пароля.
2. У базы данных Active Directory, поскольку вместе с каждым объектом сохраняются разрешения на доступ, в то время как в NDS они хранятся на высших уровнях дерева каталогов.
3. NetWare 5 — новая NOS и (когда писалась эта книга) процесс сертификации еще не успел завершиться. Это совсем не означает, что NetWare 5 защищена хуже, чем NetWare 4.11, однако некоторые правительственные агентства обязаны использовать NetWare 4.11 (или иной NOS, обладающей сертификатом C2) вплоть до завершения сертификации обновленной версии.
4. По сравнению с Windows NT, UNIX — более стабильная и расширяемая операционная система, поэтому ее предпочтительно использовать в крупных сетях. Windows NT проще устанавливать и ею легче управлять, поэтому она предпочтительна для сетей среднего размера, сетевой администратор которых знаком с Windows.
5. Нет. В Linux используется коллективная многозадачность, которая применяется и в Windows 3.x, а не многозадачный режим с приоритетами.
6. A.

Упражнение 11

1. **A.** 0 лицензий.

B. 0 лицензий.
C. 5 лицензий.
D. 8 лицензий.

2. **A.** 20 лицензий.
   B. 20 лицензий.
   C. 20 лицензий.
   D. 20 лицензий.
3. Лицензия по числу рабочих мест дешевле, когда число ваших пользователей превышает число компьютеров, например, при сменной работе.
   Приложения для локальных сетей должны хранить эту информацию вместе с файлами системной конфигурации, относящимися к пользовательской информации, а не с теми файлами, которые относятся к информации о компьютерах.
4. B.
5. Они различаются главным образом с точки зрения членства в группах. Групповое программное обеспечение работает на уровне рабочей группы, обеспечивая связь только между участниками проекта. Коммуникационное программное обеспечение, наоборот, не ограничивает связь только конкретной группой, позволяя всем связываться со всеми, используя соответствующее программное обеспечение.

Упражнение 12

1. Семь. Седьмой сеанс поддерживает средства для работы сервера. Этот сеанс отличается от клиентных сеансов тем, что не выполняет загрузку изображения на клиентный компьютер. Вместо этого он полностью обрабатывает и создает изображение, передаваемое на локальный компьютер.
2. Протокол RDP (Remote Display Protocol — протокол удаленного дисплея) и протокол ICA (Independent Computing Architecture - архитектура независимой вычислительной системы).
3. В данной ситуации возможен выбор следующих протоколов.
   A. ICA или RDP.
   B. ICA.
   C. ICA.
   D. ICA или RDP.

Упражнение 13

1. XML (Extensible Markup Language — расширяемый язык разметки) или ASP со средствами Front Page/IIS.
2. A и D. ASP зависит от оборудования сервера, а HTML имеет универсальную поддержку. Java не поддерживается полностью IE, а XML поддерживается только IE.
3. Нет. Это утверждение справедливо только в отношении ASP, но не CGI.
4. D. Функциональные средства для работы с формами не являются частью языка разметки.
5. Нет. Фирма Netscape разработала JavaScript, фирма Sun Microsystems -Java.

Упражнение 14

1. Аудит функционирования.
2. Инструмент наблюдения за сервером.
3. Анализатор.
4. Физическую.

5. Имеется две причины. Первая: локальный запуск монитора потребует части ресурсов сервера, отбираемой у текущих заданий. Вторая: локальный запуск монитора исказит результаты наблюдения, поскольку в них будут показаны используемые ресурсы, не связанные с обслуживанием запросов клиентов.
6. A.
7. Протокол UDP (User Datagram Protocol — протокол пользовательских дейтаграмм).
8. C.
9. Нет. Некоторые реализации SNMP-протокола могут посылать сообщения с помощью IPX вместо UDP. Однако это обеспечивается не во всех реализациях SNMP.
10. Версия 1.1 технологии Z.E.N.works фирмы Novell.
11. B, C.
12. В результате поиска будут возвращены документы, содержащие фразу "NetWare 5", находящуюся на расстоянии не более 8 символов от слова "zero", в том числе слово "Administration".
13. NT XOR NetWare.
14. Создание тестового узла, установка изменения в части сети и установка нескольких изменений поочередно с соответствующей проверкой работоспособности.

Упражнение 15

1. Защитный код (SID) идентифицирует пользовательскую учетную запись. Если пользователь попытается получить доступ к объекту, операционная система проверит, разрешен ли к нему доступ с данным защитным кодом.
2. 11.
3. Этот инструмент дешифрует пароли вызовов/откликов LM.
4. Средство обслуживания каталогов Active Directory фирмы Microsoft или доменная структура. Средство обслуживания каталогов NDS фирмы NetWare.
5. В одну.
6. Открытым ключом.
7. Да. Для симметричного шифрования данных используют открытые ключи.
8. Симметричного шифрования.
9. Протокол CHAP (Challenge Handshake Authentication Protocol - протокол аутентификации по квитированию вызова) представляет собой одну из систем защиты, предусмотренных протоколом PPP. Когда клиент запрашивает защищенный сеанс (secure session), сервер передает ему случайное число. Данее клиент должен найти в своем секретном файле соответствующий числу отклик и передать его обратно серверу.
10. Протокол CHAP, поскольку в этом случае по сети не передается пароль.
11. Если вы используете несколько серверов доступа к сети для удаленных соединений разных типов, но желаете сохранить все учетные записи удаленного доступа в единой базе данных.
12. Сетевые привязки связывают сетевой протокол со средством обслуживания или адаптером. Если протокол не привязан к сетевому компоненту, то данный компонент не может использовать этот протокол.
13. DOS (Denial of Service — отказ в обслуживании).
14. Пользователи могут просматривать свои локальные и логические диски с помощью IE4, поэтому они способны запускать любые исполняемые файлы, находящиеся на этих дисках.
15. Нет. Они могут форматировать жесткие диски или даже искажать системный BIOS.
16. B, D.
17. C.

Упражнение 16

1. Необходимо восстановить файлы документов и инфицированные шаблоны.
2. Восстановить только поврежденные файлы, а прочие не трогать.
3. Возможно, проще всего восстановить резервные копии из разностных архивов, поскольку вы знаете последний день, когда данные файлы редактировались. Кроме того, вам известно, что файлы были инфицированы после последнего редактирования. Неинфицированные файлы можно также получить из добавочного архива, однако тогда вам придется правильно выбрать день, иначе вы не сможете найти нужные файлы или не сумеете получить новейшие версии. Если же восстановить файлы разностного архива (differential files) за среду, вы получите все последние версии файлов, причем без вирусов.
4. Зеркальное отображение диска или дуплексирование, чередующиеся наборы без и с контролем четности.
5. Зеркальное отображение диска.
6. D. (Время восстановления не превышает 1 секунду.)
7. Нет. Это повышает длительность операций записи, поскольку требует вычисления контрольной суммы, однако время считывания не изменяется.
8. Репликацию.
9. Время восстановления отказоустойчивых кластеров ниже, поскольку оба сервера, входящие в кластер, выполняют абсолютно одинаковые операции.
10. При отказе сервера в кластере активный/активный второй сервер перехватывает нагрузку отказавшего сервера в дополнение к собственной. При отказе сервера в кластере активный/резервный второй сервер отбрасывает собственную нагрузку и принимает на себя нагрузку первичного сервера. Это не влияет на время восстановления — оно одинаково для кластеров обоих типов.

Словарь терминов

Символы

10Base2. Обозначение сети Ethernet, реализованной на базе физической топологии соединительных линий, в качестве которых используют тонкий коаксиальный кабель. Длина сегмента сетине может превышать 187 м. См. также *Ethernet, Bus Physical Topology, Coaxial Cable, Thinnet.*

10Base5. Обозначение сети Ethernet, реализованной на базе физической топологии соединительных линий, в качестве которых используют толстый коаксиальный кабель. Длина сегмента сети не может превышать 500 м. См. также *Ethernet, Bus Physical Topology, Coaxial Cable, Thicknet.*

10BaseT. Обозначение сети Ethernet, реализованной на звездообразной топологии. В качестве соединительных линий используется кабель UTP (неэкранированная витая пара). См. также Ethernet, Star Physical Topology, Unshielded Twisted Pair (UTP).

802.3. Стандарт, используемый для описания сетей Ethernet с любой средой передачи данных (media). См. также *Ethernet.*

802.4. Стандарты, описывающие сети звездообразной структуры с маркерным доступом, в которых для контроля за доступом и сетевым трафиком используется метод эстафетной передачи. Широкого распространения не получили. Их не следует путать с сетями Token Ring, которые описываются стандартом 802.5. См. также *Bus Logical Topology, Star Physical Topology, Token Ring.*

802.5. Стандарт, описывающий сети кольцевой структуры с маркерным доступом, в которых для контроля за доступом и сетевым трафиком используется метод эстафетной передачи. См. также *Star Physical Topology, Ring Logical Topology, Token Ring.*

A

Accounts — учетные записи. Контейнеры для хранения защитных кодов (SIDs), паролей, разрешений, имен групп и привилегий каждого пользователя системы. Для администрирования учетными записями в Windows NT используют утилиту User Manager for Domain (диспетчер пользователей домена). См. также *Security Identifiers (SIDs), Preferences, Permissions, Groups.*

Active Hub — активный концентратор (хаб). Усиливает проходящие через него сигналы.

Active Monitor — активный монитор. См. *Token Master.*

Adapter — адаптер. Любое оборудование (устройство), позволяющее соединять физически разнородные системы. Обычно адаптерами называют периферийные платы, постоянно установленные в компьютерах, которые обеспечивают связь шины компьютера с каким-либо внешним устройством, например, с жестким диском или сетью. См. также *Network Interface Card (NIC), Small Computer System Interface (SCSI).*

Address Resolution Protocol (ARP) — протокол определения адресов. Компонент набора протоколов TCP/IP преобразует IP-адреса в адреса аппаратных средств. См. также *Internet*

Protocol (IP), Hardware Address.

Administrators — администраторы. Пользователи, входящие в группу Administrators системы Windows NT. В системе защиты эта группа пользуется максимально широким набором возможностей доступа к ресурсам, предоставляемым системой защиты. См. также *Permissions, Groups.*

Advertising — оповещение. Извещение маршрутизатора о своем присутствии и о своих связях с остальной частью сети. Оповещение необходимо для отыскания маршрута. См. также *Router.*

Application Layer — прикладной уровень. Уровень модели OSI. Описывает методы взаимодействия пользовательских программ, называемых *приложениями.* На этом уровне предусмотрены сетевые средства высшего уровня, базирующиеся на средствах низших сетевых уровней. В качестве примера программного обеспечения прикладного уровня можно привести сетевые файловые системы. См. также *Named Pipes, Open Systems Interconnect (OSI) Model.*

Application Programming Interface (API) — интерфейс прикладных программ.
Стандартный набор функций, которые обеспечивают "прозрачный" доступ к операционной системе или сетевым функциям. Наличие API-функций позволяет программистам использовать один и тот же стандартный программный интерфейс для всех родственных типов оборудования вместо написания специализированных программ для каждого нового устройства.

Application Server — сервер приложений. Компьютер, с прикладным программным обеспечением для совместного использования всеми клиентами сети.

Asynchronous Data Stream — асинхронный поток данных. Способ передачи, информационных пакетов по одному, а не группой, как при синхронной передаче. Источником пакетов может быть физическое устройство, например, модем либо логическое, наподобие установленной на компьютере программы рассылки факсов. В последнем случае также используется модем.

B

Backup Browser — резервный броузер. Компьютер сети Microsoft. Поддерживает список доступных компьютеров и служб. Данные в список заносятся главным броузером. Резервные броузеры позволяют распределить загрузку рабочей группы или домена программой просмотра (Browsing). См. также *Master Browser.*

Backup Domain Controllers (BDCs) — резервные контроллеры домена. Серверы, содержащие точные копии баз данных системы защиты и пользователей. Эти серверы позволяют идентифицировать рабочие станции, если первичный контроллер домена не отвечает на запросы или перегружен. См. также *Primary Domain Controller (PDC).*

Bandwidth — полоса пропускания. Описывает доступную ширину канала (сети или шины) по частоте (измеряется в Гц). Эта величина в общем случае не может служить характеристикой скорости установленного соединения. Скорее, она аналогична диаметру "трубки" между отправителем и получателем. Более точная мера скорости соединения — пропускная способность (thoroughput). См. также *TJroroughput.*

Base I/O Address — базовый адрес ввода/вывода. Наименьший адрес ввода/ вывода из набора имеющихся, относящихся к конкретному элементу оборудования. См. также

I/O Address.

Basic Input/Output System (BIOS) — базовая система ввода/вывода. Набор программ. Обеспечивает взаимодействие аппаратных средств компьютера и операционной системы с приложениями и периферийными устройствами, присоединенными к компьютеру. В BIOS также находится и программа самозагрузки. См. также *Boot, Driver.*

Bayonet-Naur Connector (BNC) — байонетный разъем Наура. Соединители, используемые для сращивания отрезков коаксиального кабеля. Именно поэтому коаксиальные кабели иногда называют "кабелями BNC". См. также *Coaxial Cable.*

Binary — двоичный. Двоичная система счисления, в которой любое число представляют комбинацией двух цифр: 1 и 0. В компьютерах ее используют потому, что она удобнее всех остальных: в ней предусмотрены два состояния — включено и выключено. Для облегчения работы с двоичными числами, их часто преобразуют в десятичные или шестнадцатеричные. См. также *Decimal, Hexadecimal.*

Bindery — база данных описания связей. Структура NetWare (многозадачной сетевой операционной системы), в которой хранятся учетные записи и права пользователей. Аналогична диспетчеру Security Accounts Manager (Диспетчер учетных записей системы защиты), используемому в Windows NT. См. также *Security Accounts Manager (SAM).*

BIOS. См. *Basic Input/Output System.*

Boot — загрузка. Процесс загрузки операционной системы компьютера. Как правило, загрузка выполняется в несколько стадий (причем каждая последующая сложнее предыдущей), вплоть до полной загрузки и запуска операционной системы и некоторых ее приложений. Иногда вместо термина "boot" используют термин "bootstrap", т.е. "самозагрузка". Программа начальной загрузки должна входить в набор процедур BIOS компьютера. См. также *Basic Input/Output System (BIOS).*

Bridge — мост. Устройство, соединяющее две отдельные сети, в каждой из которых используют одинаковый протокол передачи данных. На сетевом уровне работа мостов не зависит от протоколов. Мост пропускает только пакеты, адресованные компьютерам на другой стороне моста. Некоторые мосты, называемые *транслирующими,* могут использоваться и для соединения сетей, с разными протоколами передачи данных. См. также *Router, Data Link Layer, Network Layer.*

Bridge Flooding — лавинная маршрутизация моста. Нормальный режим работы моста, при котором мост используют для рассылки пакетов во все (а не в единственный) сегменты сети, соединенные с ним. Лавинную маршрутизацию можно использовать для определения адреса. В некоторых случаях она может привести к *зацикливанию моста* (bridge looping). При этом возникают некоторые проблемы, однако сама по себе лавинная маршрутизация — нормальное явление. См. также *Bridge, Bridge Looping.*

Bridge Looping — зацикливание моста. Возможный побочный эффект лавинной маршрутизации моста, возникающий в сетях со множеством мостов. Пакет распространяется от первого моста сразу на несколько сегментов сети. Это может разрушить таблицы MAC-адресов второго моста, поскольку они не укажут обратный путь к сегменту, в котором пакет появился впервые.

Browser — броузер. Компьютер сети Microsoft, который поддерживает список компьютеров и услуг, доступных в данной сети.

Browsing — просмотр. Запрос (у броузера) списка ресурсов, совместно используемых в сети.

Bursting Technology — технология пакетной передачи. Технология считывания данных из памяти: считываются не только четыре текущих бита, а сразу вся страница (4 Кбайт в компьютерах x86). Ее использование сокращает периоды ожидания из-за повторного поиска в одной и той же странице памяти. См. также *Wait State, Extended Data Output (EDO), Random Access Memory (RAM).*

Bursty Transmission — пакетная передача. Пакеты информации отсылаются периодически, а не непрерывно. Так, например, пакетная передача применяется в электронной почте (при передаче же видеосигналов используется непрерывный поток данных).

Bus — шина. Совокупность проводников для передачи данных от одной части компьютера к другой либо от одного сетевого компьютера к другому. Скорость передачи данных определяется разрядностью и быстродействием шины.

Bus Logical Topology — топология логическая шинная. Используется в сетях Ethernet. Все ее узлы передают информацию по всей сети. Они могут "прослушивать" всю передаваемую информацию, однако принимают только то, что адресовано либо им персонально, либо всем узлам сети. См. также *Ethernet, Logical Topology.*

Bus Mastering — управление шиной. Технология, позволяющая в некоторых развитых шинных архитектурах передавать функции центрального процессора по управлению передачей данных периферийным устройствам, расположенным на платах расширения. Управление шиной поддерживается PCI-платами. См. также *Bus, Peripheral Connection Interface (PCI).*

Bus Physical Topology — физическая топология шины. Топология сети, в которой кабель проходит от одного сетевого узла к другому, связывая все компьютеры в цепь. Все сетевые компьютеры совместно подключены к единому кабелю, как правило, коаксиального типа. На этой топологии основаны сети 10Base2 и 10Base3. Обычно она ассоциируется с сетями Ethernet. (Для корректного функционирования каждый конец шины (кабеля) должен быть подключен к согласованной нагрузке, т.е. специальному резистору (terminator), сопротивление которого должно равняться волновому сопротивлению используемого коаксиального кабеля (обычно 50 Ом). - Прим, ред.) См. также *Ethernet, Coaxial Cable, 10Base2, Logical Topology, Terminator, Thinnet, Thicknet.*

C

Caching — кэширование. Технология оптимизации производительности компьютера. Копии последних использованных данных хранятся в быстром, весьма дорогостоящем устройстве памяти малой емкости (кэш-памяти), а не в основном устройстве памяти (ОЗУ, жесткий или гибкий диск). При этом предполагается, что последние данные, вероятнее всего, будут использованы повторно. Их выборка из кэш-памяти выполняется намного быстрее, чем из более емкого, но менее скоростного основного устройства хранения данных. Кроме того, большинство алгоритмов кэширования предусматривают копирование тех данных, которые будут запрошены с наибольшей вероятностью, а также организуют кэширование операций записи (write caching), что ускоряет работу. См. также *Write-Back Caching, Write-Through Caching.*

CSMA/CD (Carrier Sensing Multiple Access with Collision Detection) — множественный доступ с контролем несущей частоты и обнаружением конфликтов. Метод, применяемый

в сетях Ethernet, гарантирующий, что в данный момент времени только один узел сети ведет передачу. При использовании такого метода, каждый узел "прослушивает" сеть, и, только убедившись, что остальные узлы "молчат", начинает передачу. Если же случайно два узла одновременно начнут передачу, то обнаружат конфликт и временно ее прекратят. См. также *Ethernet, Collicion, Truncated Binary Exponential Backoff.*

Cell Relay — ретрансляция ячеек. Технология доступа в сетях WAN, созданная для управления постоянным потоком данных. Все пакеты, передаваемые через сеть WAN, независимо от типа содержащихся в них данных, состоят из 53-байтовых ячеек. Когда ячейки достигают места назначения, они обрабатываются в том же порядке, в каком передавались. Поэтому передача протекает настолько равномерно, насколько это возможно по условиям распространения. См. также *Wide-Area Network (WAN), Frame Relay.*

Central Processing Unit (CPU) — центральный процессор. "Мозг" компьютера, который управляет всеми процессами и выполнением инструкций. В персональных компьютерах CPU — это одна микросхема (специализированный микропроцессор). В больших компьютерах, например, универсальных вычислительных машинах (мэйнфреймах), CPU состоит из нескольких микропроцессоров, расположенных на общей монтажной плате. Любой процессор состоит из двух основных частей: арифметико-логического устройства, выполняющего арифметические и логические операции, и блока управления, который извлекает из памяти инструкции, а затем декодирует и выполняет их, обращаясь, при необходимости, к ALU.

Certificate — сертификат. Вложение (дополнительная запись) в передаваемые данные, идентифицирующее личность отправителя.

Circuit-Switched Network — сеть с коммутацией каналов. Разновидность сети WAN, в которой задается статический маршрут от отправителя к получателю, используемый в течение всего сеанса передачи. Пакеты, пересылаемые по сетям с коммутацией каналов, не должны содержать информацию о маршруте, поскольку она уже содержится в параметрах организуемого виртуального канала.

Client — клиент. Сетевой компьютер (или лицо, работающее на нем), пользующийся ресурсами, предоставляемыми компьютером-сервером. См. также *Server.* Кроме того, так называют внешний компонент той части программного обеспечения, который связан с внутренней частью программы, выполняемой на сервере.

Client Element — клиентный компонент. Часть программного обеспечения. Реализует удаленный доступ или удаленное управление. Запускается на компьютере, инициализирующем подсоединение к удаленному компьютеру. См. также *Server Element, Remote Control, Remote Access, Thin Client Networking.*

Client/Server — клиент/сервер. Сетевая архитектура. Отдельные компьютеры, называемые *серверами,* специально выделяют для работы в качестве поставщиков услуг всем другим компьютерам, называемым *клиентами,* на которых пользователи выполняют свои задания. Серверы могут применяться для выполнения одной или нескольких функций, например, хранения данных, печати, связи, электронной почты и доступа в Web. См. также *Share, Peer.*

Client/Server Applications — приложения клиент/сервер. Крупные приложения, разделенные на две части: процессы, выполняемые на серверах приложений и требующие значительных затрат ресурсов компьютера и средства пользовательского интерфейса, обслуживающие клиентные машины. Обе части приложения клиент/сервер "общаются" через сеть с помощью механизмов взаимодействия процессов. См. также *Client, Server, Interprocess Communications (IPC).*

Client/Server Network — сеть клиент/сервер. Обслуживается специально выделенным сервером, к которому открыт доступ клиентов сети. См. также *Peer Network.*

Cluster — кластер. Логическое объединение секторов. Используют в файловых системах Microsoft. Наименьшая возможная единица хранения данных. Число секторов в кластере зависит от типа файловой системы и размеров устройства, входящего в файловую систему. Кроме того, кластером называют группу из нескольких серверов, соединенных сверхскоростной сетью и специально спроектированных для совместной работы с целью повышения отказоустойчивости и производительности.

Coaxial Cable — коаксиальный кабель. Состоит из внутреннего (обычно медного) проводника, заключенного в изолятор (диэлектрик) и покрытого слоем медной фольги или проволочной оплетки (экраном), защищающей центральный проводник от внешних воздействий. (Внешний проводник предназначен не только для защиты от внешних воздействий (помех), но и для создания совместно с центральным проводником определенной проводящей системы, по которой распространяются электромагнитные волны. — Прим. ред.). Внешний проводник дополнительно покрывают снаружи пластиковой оболочкой. Коаксиальные кабели, используемые для прокладки сетей, должны соответствовать стандарту RG58. См. также *Bayonett-Naur Connector (BNC).*

Code — (программный) код. Инструкции для построения программного обеспечения. Кроме того, под кодом иногда понимают метод шифрования информации, заключающийся в замене одного слова другим. См. также *Encryption.*

Codec — кодек или **кодер/декодер.** Устройство, установленное на каждом конце оптоволоконного кабеля, преобразующее электрические импульсы, вырабатываемые компьютером, в световые, пригодные для передачи по кабелю, а также выполняющее обратное преобразование при приеме информации.

Collision — конфликт. Событие в сетях Ethernet, при котором два узла одновременно начинают передачу данных. См. также *Ethernet, Carrier Sensing Multiple Access with Collision Detection (CSMA/CD), Truncated Binary Exponential Backoff.*

CISC (Complex Instruction Set Chip) — процессор с полным набором микрокоманд. В процессоре с такой архитектурой для выполнения одной микрокоманды требуется несколько аппаратных циклов. Используют в процессорах семейства x86. См. также *Central Processing Unit, Reduced Instruction Set Chip (RISC).*

Components — компоненты. Взаимозаменяемые элементы сложного программного обеспечения или оборудования. См. также *Module.*

Compression — сжатие. Схема (процесс, алгоритм) оптимизации дискового пространства. Уменьшает размер (длину) набора данных. Сжатие основано на сокращении избыточности, которую, как правило, содержат данные. Уменьшает избыточность путем создания записей (symbols) меньшего размера, чем данные, которые они представляют, а также индексов, определяющих размер записей каждого сжатого набора данных.

Computer Name — имя компьютера. Состоит из 1—15 символов. Применяется в службе NetBIOS для однозначной идентификации сетевого компьютера. См. также *Network Basic Input/Output System (NetBIOS).*

Connected Star — "связанная звезда". Вариант физической топологии звездообразной сети, в которой концентраторы подключаются последовательно друг к другу для связывания нескольких локальных звездообразных сетей. Такая сеть — комбинация звездообразных

сетей, объединенных по схеме "общая шина". Используется в сетях Ethernet. См. также *Ethernet, Bus Physical Topology, Star Physical Topology.*

Connection-Oriented — связь с логическим соединением. Способ установления сетевого соединения, при котором *перед* отсылкой данных от отправителя к получателю между ними организуется виртуальное соединение. Используется для повышения надежности передачи данных. См. также *Connectionless.*

Connectionless — без соединения. Сетевое соединение. Основано на дейтаграммах, которые не требуют подтверждения приема. Передача данных начинается без предварительной установки какого-либо виртуального канала связи. См. также *Connection-Oriented.*

Container Object — объект-контейнер. Элемент сервисного каталога. Может содержать различные объекты. См. также *Directory Services, Leaf Object.*

Control Panel — панель управления. Элемент пользовательского интерфейса Windows. Обеспечивает доступ к аплетам (инструментам), управляющим запуском конкретных задач в операционной системе. Установки панели управления сохраняются в системном реестре и задаются системой и/или пользователями. См. также *Registry, Accounts.*

Cooperative Multitasking — коллективная многозадачность. Схема организации многозадачного режима работы, в которой каждый процесс должен самостоятельно предоставлять время центральной программе-планировщику заданий (scheduling route). Если какой-либо процесс не в состоянии обратиться к планировщику, компьютер зависает. Используется в операционных системах Windows 3.x, Macintosh, а также Linux. См. также *Preemptive Multitasking, Windows 3.11 for Workgroup.*

Cost — стоимость. Цена достижения заданного пункта назначения сетевым устройством, рассчитанная на основе количества ретрансляций, выполненных при достижении пункта назначения, а также других факторов. Чем выше стоимость маршрутизаторов данного типа, тем менее желательно их использование.

CPU Cache — кэш центрального процессора. Высокоскоростная память SRAM, встроенная в CPU. Предназначена для кэширования инструкций и данных. В состав процессора Pentium II входит встроенный кэш L1 и внешний кэш L2, расположенный на одной подложке с процессором CPU. Кэш L1 имеет малый объем, однако он очень быстрый, поскольку работает на частоте тактового генератора CPU. У кэша L2 большая емкость, но он медленнее, поскольку работает с тактовой частотой системной шины. См. также *Central Processing Unit (CPU), Caching, Static RAM (SRAM).*

CSMA/CD. см. *Carrier Sensing Multiple Access with Collision Detection (CSMA/CD).*

Cut-Through Switching — сквозная коммутация. Высокоскоростной метод коммутации, при котором коммутатор считывает MAC-адрес пункта назначения фрейма *до* его отправки в порт, через который этот MAC-адрес должен быть найден. Такая коммутация обеспечивает быстродействие, сравнимое с быстродействием самой линии связи.

CRC (Cyclic Redundancy Checking) — контроль с использованием циклического избыточного кода. Метод контроля ошибок, используемый в некоторых сетям с коммутацией пакетов (packet-switched network), например, X25. До передачи пакета отправитель вычисляет соответствующую контрольную сумму, которая включается в пакет вместе с остальным содержимым. Когда конечный узел принимает пакет, то повторяет процедуру ее вычисления. Если полученный результат не совпадает с включенным в пакет, пакет посылает сообщение об этом отправителю и требует повторить передачу.

D

Data Link Connection — соединение канала передачи данных. См. *Logical Link Connection (LLC).*

Data Link Layer — канальный уровень. Уровень модели OSI. Обеспечивает цифровую связь сетевых устройств и предоставляет программное обеспечение, непосредственно работающее с этими устройствами, например с сетевыми интерфейсными адаптерами. См. также *Physical Layer, Network Layer, Open Systems Interconnect (OSI) Model.*

Data Path — тракт данных, информационный канал. Разрядность (width) информационного канала CPU. Чем она выше, тем больше данных можно одновременно загрузить в CPU. См. также *Central Processing Unit (CPU), Word Size.*

Database — база данных. Связанный набор данных, упорядоченных по типу и назначению. Этот термин применяют и к программному обеспечению, манипулирующему данными. Примером базы данных может служить системный реестр Windows NT, в котором хранится информация о конфигурации системы. См. также *Registry.*

Datagram — дейтаграмма. Пакет, передаваемый в сеть без маршрутизации отсылаемой информации. Дейтаграммы не нуждаются в подтверждении приема, поэтому для их передачи не требуется сеть с высокой пропускной способностью. См. также *Packet, Connectionless.*

Decimal — десятичный. Обозначение десятичной системы счисления. В компьютерах используется двоичная система. Десятичные числа можно встретить, главным образом, в IP-адресах. См. также *Internet Protocol (IP).*

Desktop — рабочий стол. Фоновое изображение, находящееся на заднем плане оболочки Windows Explorer. Поверх него отображаются значки объектов, содержащих локальные устройства хранения данных и доступные сетевые ресурсы. Рабочий стол — один из основных компонентов Windows GUI. См. также *Explorer, Shell.*

DHCP. См. *Dynamic Host Configuration Protocol (DHCP).*

Dial-Up Connection — удаленное соединение. Цифровое соединение. Организуется с помощью модема по телефонной линии. Обеспечивает канальный уровень модели OSI. Выражение "удаленное" относится к временным соединениям в противовес *выделенным* телефонным линиям, которые обеспечивают постоянное соединение. См. также *Data Link Layer.*

Direct Memory Access (DMA) — прямой доступ к памяти. Метод передачи данных от периферийных устройств в основную память (ОЗУ). Реализуется с помощью микросхем контроллера DMA самого периферийного устройства, т.е. без участия CPU. Для передачи данных необходимо предоставить периферийному устройству канал DMA. См. также *Central Processing Unit (CPU), Programmable Input/Output (PIO).*

Directory Services — службы каталога. Средства организации всех ресурсов и учетных записей сети в иерархию объектов. Некоторые из этих объектов могут включать другие объекты, а некоторые — нет. Службы каталога в сетях Novell называют NetWare Directory Services (NDS); в Windows 2000 — Active Directory. См. также *NetWare, Windows 2000.*

Disk Server — дисковый сервер. Сетевой компьютер, предоставляющий доступ к своему дисковому пространству клиентам сети. Каждый клиент работает с собственной копией

структуры дисковых томов, поэтому общий доступ к каждому тому диска должен предоставляться клиентам автономно, чтобы избежать путаницы и искажения данных. В настоящее время дисковые серверы вытесняются файловыми. См. также *File Server.*

Display Protocol — протокол дисплея. Протокол канального уровня. Используется в т.н. "тонкой" клиентной сети для обмена данными с сервером терминала. См. *Thin Client Networking, Terminal Server.*
DNS. см. *Domain Name Service.*

Domain — домен. В сетях Microsoft доменом называют структуру, состоящую из серверов и клиентов, имеющую собственное имя и совместно использующую единую базу данных системы защиты, содержащую информацию об уровнях доступа к ресурсам. В Internet доменом называют семейство узлов и субдоменов, зарегистрированных под уникальным именем в InterNIC. См. также *Workgroup, InterNIC.*

Domain Controllers — контроллеры домена. Серверы. Идентифицируют рабочие станции, которые запрашивают вход в сеть. С этой целью они сопоставляют имя и пароль пользователя с информацией, хранящейся в базе данных учетных записей. Без идентификации контроллером домена, пользователь не сможет получить в него доступ. См. также *Primary Domain Controller (PDC), Backup Domain Controller (BDC).*

Domain Name — доменное имя. Текстовый идентификатор конкретного компьютера Internet. Доменные имена имеют такую форму: *сервер организация.тип* (например, www.microsoft.com). Серверы имен доменов преобразуют эти имена в адреса Internet. В сетях Windows NT можно также указывать имя группы компьютеров, совместно использующих общую базу данных системы защиты. См. также *Domain Name Server.*

Domain Name Server — сервер имен домена. Компьютер Internet, выделенный для преобразования полных имен доменов в IP-адреса. См. также *Domain Name.*

Domain Name Service (DNS) - служба имен домена. Служба сети TCP/IP, транслирующая имена компьютеров в числовые адреса сети Internet. См. также *Transmission Control Protocol/Internet Protocol (TCP/IP), Internet.*

Driver — драйвер. Программа, обеспечивающая взаимодействие с оборудованием (физическими устройствами) или какой-либо частью операционной системы, например, файловой системой. Драйверы разрабатываются для управления конкретными устройствами и предоставляют общий программный интерфейс между оборудованием и операционной системой компьютера, позволяя ей управлять всеми однотипными устройствами (например, жесткими дисками или видеоплатами различных изготовителей) так, как если бы они были стандартными устройствами. См. также *Data Link Layer, Operating System.*

Dual-Boot — двойная загрузка. Конфигурация для загрузки нескольких операционных систем. Необходимую систему выбирают при запуске компьютера с помощью меню. Например, система двойной загрузки позволяет загрузить Windows NT Workstation, Windows 98 и OS/2.

DDE (Dynamic Data Exchange) — динамический обмен данными. Метод взаимодействия процессов в операционной системе Microsoft Windows.

DHCP (Dynamic Host Configuration Protocol) — протокол динамического конфигурирования компьютера. Метод автоматического присваивания IP-адресов клиентным компьютерам сети.

Dynamic Link Libraries (DLLs) — динамически подключаемые библиотеки.
Набор функций, которые могут использоваться одновременно различными программами при выполнении различных задач.

Dynamic RAM (DRAM) — динамическая оперативная память. Запоминающие устройства, используемые для организации основной памяти (ОЗУ) компьютера. Содержимое DRAM необходимо регенерировать каждые 4 мс. См. также *Random Access Memory (RAM), Static RAM (SRAM).*

E

Electrical Topology — электрическая топология. См. *Logical Topology.*

Electronic Mail (E-Mail) — электронная почта. Приложение, организующее взаимодействие клиент/сервер. Обеспечивает работу службы маршрутизации и сохранения сообщений, переданных любыми двумя пользователями данного приложения. См. также *Internet.*

Encryption — шифрование. Процесс скрытия информации путем ее модификации с помощью соответствующей математической функции, известной только получателю. Шифрование позволяет защитить информацию, передаваемую по незащищенной среде передачи данных. См. также *Security.*

Enhanced Integrated Drive Electronics (EIDE) — улучшенный интерфейс жестких дисков (улучшенный IDE-интерфейс). Интерфейс между компьютером и внешними устройствами долговременного хранения информации, например жестким диском или CD-ROM. EIDE-стандарт предусматривает обслуживание устройств с емкостью, превышающей 528 Мбайт (ограничение, налагаемое стандартным IDE-интерфейсом). Кроме того, EIDE-устройства позволяют обмениваться данными со скоростью 4—16,6 Мбайт/с, что в 3—4 раза выше значения, обеспечиваемого IDE-устройствами. См. также *Integrated Drive Electronics (IDE), Small Computer System Interface (SCSI).*

Enterprise Network — сеть масштаба предприятия. Сеть, состоящая из множества серверов и доменов, расположенных в обширной географической области. Нередко сети масштаба предприятия работают одновременно с несколькими операционными системами и сетевыми протоколами.

Environment Variables — переменные окружения. Переменные (такие, как путь к файлам), содержащие информацию о текущей среде операционной системы, доступную для использования в программах и пакетных файлах.

Ethernet. Наиболее популярный стандарт (канального уровня) организации локальной сети. Для обеспечения доступа в сеть множества компьютеров, предусматривается применение метода *CSMA/CD.* Данный стандарт поддерживает использование среды передачи данных любого типа, в том числе беспроводной. Скорость работы сети, построенной в соответствии со стандартом Ethernet, достигает 10 Мбит/с. Скорость работы сети по стандарту Fast Ethernet достигает 100 Мбит/с. См. также *Data Link Layer.*

Exchange. Серверное приложение. Разработано фирмой Microsoft и предназначено для обмена сообщениями. Exchange Server обеспечивает программный интерфейс почтовых приложений (MAPI — mail application programming interface) и другие протоколы передачи сообщений, например POP, SNMP, а также факсимильной связи. При этом достигается гибкость в работе системы отправки и приема сообщений. См. также *Electronic Mail (E-Mail).*

Explorer. Стандартная оболочка всех 32-битовых операционных систем Windows. По сравнению с диспетчером программ (Program Manager) в ранних версиях Windows в Explorer реализована более гибкая концепция рабочего стола. См. также *Desktop*.

Extended Data Output (EDO) — расширенный вывод данных. Разновидность памяти типа DRAM, в которой обеспечивается поиск следующего запрошенного бита данных во время передачи в CPU первого бита. Время доступа к памяти этого типа составляет около 40 нс, что выше, чем у памяти типа FPM (более 60 нс), однако меньше, чем у памяти SDRAM (10 нс). См. также *Random Access Memory (RAM), Fast Page Mode (FPM) RAM, Dynamic RAM (DRAM).*

Extender — удлинитель. Устройство, усиливающее электрические или световые сигналы для увеличения области уверенного приема сигнала. Используется для удлинения сегментов сетей Ethernet без применения повторителей. См. также *Repeater*.

F

Fast Ethernet — "быстрая" Ethernet. Тип сетей Ethernet, обеспечивающих скорость передачи данных до 100 Мбит/с по кабелю "неэкранированная витая пара" (UTP) категории 5. См. также *Ethernet, Unshielded Twisted Pair (UTP).*

Fast Page Mode (FPM) RAM — память с быстрым постраничным доступом.
Самая первая модификация памяти DRAM, в которой обращение к конкретной ячейке памяти выполнялось в два этапа: сначала относительно медленное обращение к странице, содержащей требуемую ячейку, а затем весьма быстрое обращение ко всем ячейкам, расположенным на данной странице. Время доступа для такой памяти составляет 60—70 нс. Пользовалась всеобщим признанием около десятилетия, однако в настоящее время вытеснена памятью типа EDO и SDRAM. См. также *Random Access Memory (RAM), Extended Data Out (EDO), Dynamic RAM (DRAM).*

FAT. см. *File Allocation Table.*

Fiber Distributed Data Interface (FDDI) — распределенный интерфейс передачи данных по оптоволоконным каналам. Оптоволоконная сеть кольцевой структуры. Как правило, для обеспечения целостности соединений применяется двойная кабельная проводка.

Fiber Optic Cable — оптоволоконный кабель. Состоит из тонкого, оптически однородного стеклянного или пластикового волокна, окруженного изоляционным слоем (оболочкой) и защитным покрытием (jacket). Нечувствителен к внешним электромагнитным воздействиям, поскольку для передачи данных используются световые, а не электрические сигналы.

Fibre Channel — оптоволоконный канал. Метод создания сетей, при использовании которого периферийные устройства и узлы сети соединяются в единую сеть, обеспечивающую скорость передачи данных в несколько Гбит/с. Так, например, сервер можно соединить с жестким диском, расположенным в другом конце комнаты, и в то же время быстродействие соединения будет точно таким же, как и при установке диска непосредственно внутри сервера. Сеть может быть двухточечной (т.е. соединять устройства попарно) либо соединять все устройства в физическое кольцо, либо образовывать структуру, в которой все устройства — части логической сети. Оптоволоконные каналы успешно конкурируют со SCSI-системами. См. также *Small Computer Systems Interface (SCSI).*

File Allocation Table (FAT) — таблица размещения файлов. Файловая система, используемая в MS-DOS. Поддерживается также в других операционных системах, например в Windows (любой версии), OS/2 и Macintosh. Благодаря простоте и большой популярности использование FAT стало своего рода гарантом совместимости запоминающих устройств

большой емкости. В FAT не предусмотрены развитые средства обеспечения отказоустойчивости, поэтому со временем могут возникать ошибки даже при ее безаварийном использовании. См. также *File System.*

File Attributes — атрибуты файла. Биты, указывающие статус файла (например "архивный", "скрытый", "только для чтения"). Сохраняются вместе с именем и местоположением файла в каталоге. В различных операционных системах используют дополнительные атрибуты файлов, позволяющие организовать режимы совместного использования, сжатия и защиты.

File Management — управление файлами. Общий термин, используемый для обозначения совместного применения, передачи и защиты информации сетевыми компьютерами.

File Server — файловый сервер. Компьютер, обеспечивающий совместный доступ к своим файлам или каталогам прочим сетевым компьютерам. Поддерживает файловую структуру и обновляет ее по мере добавления или удаления клиентами сети файлов общих каталогов.

File System — файловая система. Компонент программного обеспечения, управляющий размещением файлов в устройствах хранения. Предоставляет соответствующие средства, позволяющие создавать, считывать, записывать и удалять файлы. Для этого она создает в устройстве хранения упорядоченные базы данных файлов, называемые *томами,* в которых для их организации используется иерархическая система каталогов. См. также *Volume, Database.*

File Transfer Protocol (FTP) — протокол передачи файлов. Простой протокол Internet, описывающий способ передачи файлов с FTP-сервера клиенту FTP. Предоставляет простой метод передачи файлов между компьютерами, однако не предусматривает наличия функций просмотра списков адресов; Для того чтобы соединиться с FTP-сервером, необходимо знать его адрес. См. также *Internet, Uniform Resource Locator (URL).*

Filtering — фильтрация. Процесс отбрасывания пакета данных без перенаправления его в другой сегмент сети. Для поддержки режима фильтрации можно сконфигурировать различные устройства. Так, например, мосты могут отфильтровывать принимаемые пакеты, если они направлены в тот же сегмент сети, где находится отправитель, поскольку компьютер, которому адресован пакет, уже принял его, и мосту нет необходимости повторно пересылать пакет. Маршрутизаторы и брандмауэры могут отфильтровывать пакеты по значениям их IP-адресов, типу протокола или по иным условиям с целью снижения трафика либо из соображений защиты. См. также *Bridge, Router, Forwarding.*

Flow Control — управление потоком данных. Механизм, гарантирующий, что адресат никогда не получит большее число пакетов, чем он может обработать одновременно. Управление потоком данных можно реализовать либо аппаратными, либо программными средствами.

Forwarding — направление. Процесс отсылки пакета в тот порт, через который он сможет попасть в место назначения. Мосты отсылают пакеты, адресованные в любой сегмент, за исключением того, из которого они отправлены. См. также *Filtering.*

Frame — фрейм, кадр. Сегмент данных, передаваемый на канальном уровне. См. также *Framing, Data Link Layer.*

Frame Relay — ретрансляция кадров. Метод доступа в сетях WAN, при котором передаются кадры переменной длины. Ретрансляция кадров отличается своей техникой комбинирования канального пространства (channel space) для всех пользователей WAN,

позволяющей полностью использовать полосу пропускания. Это значительно повышает пропускную способность по сравнению с той, которая достигается при раздельной поддержке всех каналов. В отличие от стандарта X.25 технология Frame Relay не предусматривает средств контроля ошибок, поэтому ее предпочтительно использовать в надежных сетях. См. также *Cell Relay, X.25.*

Frame Type — тип кадра (фрейма). Основной параметр протокола IPX/SPX. По сети могут передаваться фреймы различных типов. Фрейм можно уподобить диалекту некоторого языка. Так, в сетях Ethernet используют четыре типа фреймов или диалектов, а в сетях Token Ring — два.

Framing — формирование кадра. Процесс "упаковки" данных в сегменты, называемые пакетами или кадрами (фреймами). Формирование кадра выполняется на канальном уровне. См. также *Frame, Frame Type, Packet, Data Link Layer.*

FTP. См. *File Transfer Protocol.*

Full Duplex — дуплекс. Режим работы, оборудование, канал. Позволяют одновременно и передавать, и принимать данные. См. также *Half Duplex, Integrated Services Digital Systems Network (ISDN).*

G

Gateway — шлюз. Компьютер, выполняющий функции маршрутизатора, транслятора данных различных форматов или фильтра данных для всей сети или подсети. Кроме того, шлюзом называют устройство, которое позволяет соединить две разнотипные вычислительные машины, например, мэйнфрейм и персональный компьютер.
GDI. См. *Graphical Device Interface.*

General Protection Faults (GPFs) — ошибка общей зашиты. Такое сообщение об ошибке появляется при нарушении прикладной программой целостности системы. Это случается, когда программа пытается получить доступ к области памяти, не являющейся частью ее адресного пространства. Механизм выработки GPF-сообщений служит защитным средством операционной системы и предназначен для уменьшения ущерба от сбоя программ.

Gigabit Ethernet — гигабитная Ethernet. Версия Ethernet, поддерживающая скорость обмена до 1 Гбит/с. Сетевые карты (NIC), обеспечивающие такое быстродействие, в настоящее время весьма дороги и предназначены в основном для рынка новейших серверов, но не для клиентов или обычных серверов. Первый стандарт Gigabit Ethernet (802.3z) утвержден в 1998 г. (разработан IEEE).

Graded Index Cable — градиентное оптоволокно. Тип многомодового оптоволоконного кабеля, в котором траектория световых лучей имеет синусоидальную (а не треугольную, как в обычном оптоволокне) форму. См. также *Fiber Optic Cable, Mode, Modal Dispersion.*
Graphical Device Interface (GDI) — интерфейс графического устройства.

Программный интерфейс и графические средства, предусмотренные Win32 для интерактивного взаимодействия программ с устройствами вывода графики такими, как экран или принтер. См. также *Programming Interfaces, Win32.*

Graphical User Interface (GUI) — графический пользовательский интерфейс.
Программная оболочка компьютера (computer shell program), представляющая устройства хранения информации большой емкости, каталоги и файлы в виде графических объектов на экране (рабочем столе). Для манипулирования объектами используют курсор, перемещением

которого пользователь может управлять с помощью мыши, трекбола и т.п. Сами объекты, как правило, представлены значками, которые можно развернуть в окна, отображающие содержимое объектов. См. также *Shell, Explorer.*

Groups — группы. Группа пользователей Windows NT с единым набором прав и разрешений на доступ. Устанавливая разрешения для групп и включая пользователей в ту или иную группу (вместо установки разрешений для отдельных пользователей), сетевые администраторы могут легко поддерживать согласованную систему защиты даже очень крупных систем. См. также *Permission, Accounts, Security, Local Group.*

Groupware — групповое программное обеспечение. Общее наименование приложений, спроектированных для совместной работы заданной группы пользователей. Применяют также выражение "teamware", т.е. программное обеспечение команды, либо "workgroup productivity software" — программное обеспечение рабочей группы.

GUI. См. *Graphical User Interface.*

H

Half Duplex (HDX) — полудуплекс. Режим работы, оборудование, канал, позволяющие передавать и принимать по одному каналу связи. Пропускная способность полудуплексного канала иногда может быть выше, чем дуплексного. См. также *Full Duplex, Integrated Services Digital Systems Network (ISDN).*

Hardware Address — адрес машины. Уникальный физический адрес сетевой карты (NIC), присвоенный производителем. В сетевых картах Ethernet длина адреса составляет 48 бит.

Hardware Profiles — профили оборудования. Набор физических устройств, которые могут использоваться или не использоваться в зависимости от параметров, выбранных при запуске системы. Применяются для управления портативными компьютерами, которые могут иметь различную конфигурацию.

Hexadecimal — шестнадцатеричный. Обозначение шестнадцатеричной системы счисления, в которой для представления чисел используются шестнадцать символов: цифры от 0 до 9 и буквы от A до F. Часто применяется для сокращенной записи двоичных чисел с целью облегчения их восприятия.

Home Directory — основной каталог. Каталог, в котором сохраняются личные файлы и программы пользователя.

Hop — транзитный участок. Промежуточное соединение в цепи соединений, связывающих два элемента сетевого оборудования. Возникает всякий раз, когда пакет заново собирается и передается. При подсчете количества транзитных участков учитываются маршрутизаторы, мосты и повторители. Удлинители же при подсчете *не* принимаются во внимание, поскольку они *не* регенерируют пакеты, а только усиливают электрические сигналы для увеличения области уверенного приема сигналов. См. также *Router, Bridge, Repeater, Extender.*

Host — сервер Internet. Компьютеры, постоянно подключенные к Internet. См. также *Internet.*

HTML. См. *Hypertext Markup Language.* **HTTP.** См. *Hypertext Transfer Protocol.*

Hub — концентратор, хаб. Устройство, обеспечивающее соединение отдельных сетевых устройств (обычно, сегменты LAN). Для подключения новых сегментов в концентраторе

предусмотрены порты. Когда в один из портов поступает пакет, он копируется в остальные порты, с тем чтобы его можно было просматривать и в других сегментах LAN. См. также *Active Hub, Passive Hub, Intelligent Hub.*

Hyperlink — гиперсвязь, гиперссылка. Элемент связи в текстовых или графических файлах. Содержит указатель на другой документ или часть данного документа. Щелчок на гиперссылке позволяет пользователю переместиться в другую часть документа или иной документ, хранящийся на этом же компьютере или в Web. Гиперссылку нетрудно идентифицировать — обычно она выделена цветом, отличным от цвета остального документа. Как правило, используется в интерактивной справочной системе и Web-страницах. См. также *World Wide Web (WWW).*

Hypertext Markup Language (HTML) — язык разметки гипертекста. Язык форматирования. Для идентификации разделов документа, например, заголовков, списков, гипертекстовых связей и т.д. применяются соответствующие коды. Данные в формате HTML используется в World Wide Web для оформления Web-страниц. См. также *Hypertext Transfer Protocol (HTTP), World Wide Web (WWW).*

Hypertext Transfer Protocol (HTTP) — протокол передачи гипертекста. Основной протокол Internet для передачи документов HTML, а также средство, обеспечивающее соответствующую реакцию на действия пользователя, например при щелчке мышью на гиперсвязи. См. также *Hypertext Markup Language (HTML), World Wide Web (WWW).*

I

I/O Address — адрес ввода/вывода. Область памяти, выделенная для отдельного физического устройства, где устройство сохраняет информацию, необходимую для работы с CPU, а также накапливает результаты вычислений, выполненных для него CPU. См. также *Central Processing Unit (CPU).*

IIS. См. *Internet Information Server.*

Infrared Communications — инфракрасная связь. Тип беспроводной связи, в которой для передачи данных используются сигналы инфракрасного диапазона. Обеспечивает высокую скорость передачи, однако при передаче сигналов в открытое пространство могут возникать интерференционные помехи. См. также *Wireless Networking.*

Industry Standard Architecture (ISA) — стандартная промышленная архитектура. Стандарт, описывающий электрические и механические параметры 16-битовых системных плат и периферийных плат компьютеров, реализованных на платформе Intel. Адаптеры и интерфейсные платы должны соответствовать стандартам шин, использованных в системной плате компьютера. В настоящее время ISA вытесняется 32-/64-битовым стандартом шин PCI.

Instruction Set — система команд. Набор инструкций (команд) на машинном языке. Воспринимаются и могут обрабатываться процессором (CPU). См. также *Central Processing Unit (CPU), Microcode.*

Integrated Drive Electronics (IDE) — встроенная электроника накопителя. Интерфейс устройств хранения большой емкости. Используется простая шина, обеспечивающая скорость передачи данных до 5 Мбит/с и обслуживание двух подсоединенных устройств. Его название отражает то, что необходимые схемы управления располагаются на самом устройстве, и при этом отпадает необходимость в отдельной плате контроллера. См. также *Small Computer Systems Interface (SCSI), Enhanced Integrating Drive Electronics (EWE).*

Integrated Services Digital Network (ISDN) — цифровая сеть с интеграцией услуг. Сеть, обеспечивающая прямое цифровое удаленное соединение через коммутируемую телефонную сеть общего пользования (PSTN). Работает на канальном уровне со скоростью 64 Кбит/канал. Для соединения абонента с центральным офисом PSTN используется кабель "витая пара". Две витые пары позволяют мультиплексировать до 24 каналов. См. также *Data Link Layer.*

Intelligent Hub — интеллектуальный концентратор. Мощный концентратор (powered hub), поддерживающий управляющие протоколы, например, SNMP. См. также *Hub, Active Hub, Simple Network Management Protocol (SNMP).*

Internet. Добровольное объединение глобальной сети компьютеров на основе семейства протоколов TCP/IP. Разработан Управлением Перспективных Исследований и Разработок (ARPA) Министерства обороны США для улучшения связи между армейскими сетями и бесплатно предоставлялся университетам. Очевидная польза соединения во всемирную цифровую сеть и доступность бесплатного и сложного сетевого программного обеспечения, разработанного в университетах, выполняющих оборонные исследования, привлекло прочие университеты, исследовательские институты, частные организации, коммерческие фирмы и, наконец, отдельных пользователей. В настоящее время сеть Internet доступна на всех коммерческих вычислительных платформах. См. также *File Transfer Protocol (FTP), World Wide Web (WWW), Transmission Control Protocol/Internet Protocol (TCP/IP).*

Internet Information Server (IIS) — информационный сервер Internet. Программный продукт, реализующий Web-сервер в среде Windows NT. Сервер IIS обслуживает протоколы Internet высшего уровня (HTTP и FTP), для работы с клиентами, использующими броузеры Web. См. также *Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), World Wide Web (WWW).*

Internet Protocol (IP) — протокол Internet. Протокол сетевого уровня, на котором основана работа сети Internet. Обеспечивает простой обмен пакетами путем трассировки межсетевых адресов. См. также *Transmission Control Protocol/Internet Protocol (TCP/IP), Internet.*

Internet Service Provider (ISP) — поставщик услуг (провайдер) Internet.
Фирма, предоставляющая удаленный доступ к Internet. См. также *Internet.*

Internetwork Packet Exchange (IPX) — межсетевой обмен пакетами. Сетевой протокол, разработанный фирмой Novell для сети NetWare. IPX — маршрутизируемый протокол (наподобие IP), однако им гораздо проще управлять, а коммуникационные издержки (communication overhead) намного меньше. Кроме того, под IPX часто имеют в виду семейство протоколов, в которое входит и протокол последовательного обмена пакетами (SPX). SPX — протокол с маршрутизацией информации; он работает на транспортном уровне модели OSI и, подобно TCP, гарантирует надлежащее отправление и прием сообщений. См. также *Internet Protocol (IP), NetWare.*

Internetworking — объединение сетей, интерсеть. Соединение нескольких сетей, при котором между сетями можно передавать сообщения, но сами сети сохраняют свою самостоятельность. См. также *Intranetworking.*

InterNIC — Центр сетевой информации Internet. Организация, ответственная за назначение IP-адресов. См. также *Internet Protocol (IP), IP Address.*

Interprocess communication (IPC) — взаимодействие процессов. Общий термин, используемый по отношению к методам обмена данными между программами, запущенными в одной сети, а также по отношению к протоколам связи клиент/сервер любого типа, особенно

тем, которые применяются на уровне представления данных, сеансовом и прикладном уровнях модели OSI. Метод обмена информацией между клиентом и сервером должен предоставлять и механизмы взаимодействия процессов. См. также *Named Pipes, Remote Procedure Calls (RPCs), Network Basic Input/Output System (NetBIOS), Network Dynamic Data Exchange (NetDDE).*

Interrupt Request (IRQ) — запрос прерывания. Запрос прерывания, или просто "прерывание" — это сигнал от периферийного физического устройства к CPU, указывающий на то, что устройство имеет данные, требующие обработки на CPU. Если CPU в настоящий момент не занят исполнением более важного задания, то прерывает текущую работу и обрабатывает запрос. В персональных компьютерах предусмотрены 16 линий запроса на прерывание с номерами от 0 до 15. Вообще, для каждого устройства компьютера предпочтительнее выделять отдельную линию запроса на прерывание, но это возможно далеко не всегда. См. также *Central Processing Unit (CPU).*

Intranet — внутренняя сеть. Корпоративная сеть, работающая на основе технологии World Wide Web с использованием протоколов семейства TCP/IP. См. также *Transmission Control Protocol/Internet Protocol (TCP/IP).*

Intranetworking — внутрикорпоративная сеть, интрасеть. Совместное объединение нескольких сетей, обеспечивающее передачу сообщений между ними. Сами сети при этом сохраняют свою автономность. См. также *Internetworking.*

IP-address — IP-адрес. Четырехбайтовое (32 бита) число, однозначно идентифицирующее компьютер в интерсети, работающей по протоколу IP. Первые байты IP-адресов Internet и их иерархия задаются InterNIC. Крупным организациям, например правительственным, или крупнейшим ISP присвоены адреса класса A; корпорациям и большинству ISP — класса B, а небольшим фирмам — C. В адресах класса A InterNIC определяет только первый байт, а остальные три назначает организация-носитель адреса. В адресах класса B InterNIC или ISP высшего уровня определяют первые два байта, а организация-носитель адреса — остальные два. В адресах класса C организация InterNIC или ISP определяют первые три байта, а оставшийся байт назначает сама организация. Организации, не соединенные с Internet, могут беспрепятственно выбирать любые IP-адреса для внутреннего использования. См. также *Internet Protocol (IP), Internet, InterNIC.*

IPC. См. *Interprocess Communication.*

IP Security (IPSec) — защита IP. Протокол сетевого уровня, используемый для создания сетей VPN. Вместо туннелирования, предусматривает шифрование IP-пакетов для передачи по общедоступным сетям. Для идентификации получателя используются сертификаты. См. также *Virtual Private Network (VPN), Certificate, Internet Protocol (IP), Encryption.*

IPX. См. *Internetwork Packet Exchange.*

IRQ. См. *Interrupt Request.*

ISA. См. *Industry Standard Architecture (ISA).*

ISDN. См. *Integrated Services Digital Network.*

ISP. См. *Internet Service Provider.*

J

Just a Bunch Of Disks (JBOD) — простой набор дисков. Набор жестких дисков сервера, не организованный в массив RAID.

K

Kernel — ядро. Базовый элемент операционной системы. Использует многозадачный режим работы с приоритетами, и состоящий из планировщика многозадачного режима и основных систем защиты. В зависимости от операционной системы в ядро могут встраиваться и другие системы, например драйверы виртуальной памяти. Ядро отвечает за управление потоками и процессами. См. также *Operating System, Driver.*

L

LAN Manager — диспетчер LAN. Фирменное название сетевого продукта Microsoft, разработанного совместно с IBM. Ранее обеспечивал работу приложений клиент/сервер. LAN Manager/Server был вытеснен NetWare, однако заложил основу многих важных протоколов, а также механизм IPC, которые используется и поныне (NetBIOS, именованные каналы и NetBEUI). Частично этот продукт используется и в настоящее время в OS/2 Warp Server.

LAN Server — сервер LAN. Фирменное название сетевого продукта IBM, разработанного совместно с Microsoft. См. также *LAN Manager.*

Layer 2 Tunneling Protocol (L2TP) — протокол L2TP. Протокол канального уровня, используемый для создания сетей VPN в любой сети, поддерживающей дейтаграммы UDP. Спроектирован для обеспечения объединения с протоколом IPSec, однако, если IPSec недоступен, используется протокол PPP. См. также *Data Link Layer, Virtual Private Network (VPN), IP Security (IPSec), Point-to-Point Protocol (PPP), Datagram, Point-to-Point Tunneling Protocol (PPTP).*

Leaf Object — объект-лист. Объекты в структуре каталогов, в которые не могут входить другие объекты. См. также *Directory Services, Container Object.*

Leased Line — выделенная линия. Выделенная частная линия для двухточечных соединений в сетях WAN.

License — лицензия. Форма приобретения пользователем программного обеспечения. Покупатель оплачивает не программное обеспечение, а только право на его использование ограниченным числом пользователей или компьютеров. Лицензии предоставляются по числу пользователей, числу компьютеров либо иному принципу.

Line Protocol — протокол линии связи. Протокол канального уровня, используемый для организации удаленного соединения с сервером по проводной линии. См. также *Data Link Layer, Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Remote Access, Remote Control.*

Local Area Network (LAN) — локальная сеть. Сеть, ограниченная пределами здания или офиса.

Local Group — локальная группа. Группа, внесенная в локальную базу данных учетных записей компьютера, работающего под управлением Windows NT (Workstation и Server). В локальные группы могут входить как отдельные пользователи, так и группы пользователей.

Local User Profiles — локальные профили пользователей. Набор пользовательских настроек 32-битовой операционной системы Windows. Локальные профили сохраняются только на локальном компьютере. Если пользователь входит в один из компьютеров и изменяет параметры сред системы, а затем входит в другой, то изменения в первом компьютере не отразятся на втором.

Logging — регистрация. Процесс записи информации о работе и ошибках операционной системы. Имена файлов журналов часто имеют расширение . LOG . Их можно просматривать с помощью текстового редактора или специальной утилиты.

Logical Topology — логическая топология. Электрическая схема сети, описывающая передачу данных, защиту рабочих станций от взаимного влияния и систему контроля низкоуровневых ошибок. Иногда называется *электрической топологией.* См. также *Bus Physical Topology, Ring Physical Topology, Physical Topology.*

Logical Link Connection (LLC) — связь логических каналов. Элемент организации связи канального уровня, управляющий взаимодействием всех сетевых топологий и протоколов связи сетевого уровня. Иногда называется соединением каналов передачи данных (data link connection). См. также *Data Link Layer, Media Access Control (MAC).*

Logon Script — сценарий входа в систему. Пакетный файл, позволяющий автоматизировать процесс входа в систему путем запуска всевозможных служебных операций, таких как подсоединение к дополнительным ресурсам сервера или автоматический запуск программ на основе учетной записи пользователя, входящего в систему.

Long File Name (LFN) — длинное имя файла. Имя файла, длина которого превышает восемь символов плюс три символа на расширение, используемое в MS-DOS. В 32-битовой операционной системе Windows имена файлов могут состоять не более чем из 255 символов.

M

MAC Address — MAC-адрес. См. *Physical Address.*

MAC Table — MAC-таблица. Таблица, доступ к которой поддерживается мостами, определяющими адрес порта для отправления пакета. Мосты создают MAC-таблицы, собирая исходные MAC-адреса принимаемых пакетов и отмечая порты, через которые передаются пакеты. См. также *Bridge, Physical Address.*

Mandatory User Profile — обязательный профиль пользователя. Создается администратором и хранится в файле с особым расширением . MAN, для того чтобы пользователь сам не смог никоим образом его изменить. Обязательные профили могут назначаться как отдельному пользователю, так и группе. Обычно применяют для отображения согласованного рабочего стола во всей сети. См. также *User Profile.*

Master Boot Record (MBR) — главная загрузочная запись. Небольшая программа, выполняемая каждый раз при загрузке операционной систем компьютера. Как правило, MBR постоянно находится на первом секторе жесткого диска. Система начинает процесс загрузки с просмотра таблицы разделов диска и определяет раздел, который должен использоваться для загрузки. Затем она передает программное управление загрузочному сектору этого раздела, который и продолжает процесс загрузки. В системах DOS и Windows MBR можно создать командой FDISK/MBR.

Master Browser — главный броузер. Сетевой компьютер, поддерживающий список компьютеров и услуг, доступных в данной сети, а также распространяет этот список между

другими броузерами. Кроме того, главный броузер может использоваться для создания других броузеров на основе потенциально пригодных для этого компьютеров. См. также *Browser, Browsing, Backup Browser.*

Media Access Control (MAC) — управление доступом к среде передачи. Часть канального уровня, поддерживающая драйвер сетевой карты и помогающая наблюдать за ошибками передачи и преобразования сигналов. См. также *Data Link Layer.*

Microcode — микрокод. Набор команд низкого уровня, определяющих способы выполнения данным процессором команд на машинном языке. См. также *Instruction Set, Central Processing Unit (CPU).*

Microprocessor — микропроцессор. Интегральная полупроводниковая микросхема, предназначенная для автоматического исполнения наборов логических и арифметических операций. Современные микропроцессоры самостоятельно управляют буферными областями памяти (memory pool) и обеспечивают выполнение нескольких раздельных наборов инструкций, называемых *потоками.* Кроме того, микропроцессоры способны реагировать на запросы прерывания от периферийных устройств, а также содержат встроенные средства поддержки сложных арифметических операций с плавающей запятой. Для начала работы микропроцессору необходимо предоставить специальные инструкции, которые хранятся в энергонезависимой памяти (ПЗУ), являющейся одним из аппаратных компонентов BIOS. См. также *Basic Input/Output System (BIOS), Operating System, Central Processing Unit (CPU).*

Modal Dispersion — модальная дисперсия. В оптоволоконных кабелях так называют рассеяние светового импульса, вызванное дисперсией (разбросом) скоростей волновых компонент передаваемого сигнала. Не только снижает соотношение сигнал/шум, но и ухудшает форму сигнала. См. также *Fiber Optic Cable, Mode.*

Mode — мода. Отдельная волновая компонента оптического сигнала (луч света, входящий в оптоволоконный кабель под конкретным углом). Оптоволоконные кабели могут быть как одномодовыми (для передачи одного луча), так и многомодовыми (для нескольких лучей). В одномодовых кабелях используют лучи очень высокой интенсивности. Поэтому кабели данного типа в основном применяют для передачи данных на большие расстояния, например между зданиями. Многомодовые кабели чаще применяют для внутренней проводки, так как они дешевле одномодовых. См. также *Fiber Optic Cable, Step Index Cable, Graded Index Cable.*

Modem Pooling — модемный пул. Совместное применение множества физически идентичных модемов с одинаковым логическим именем, для того, чтобы любой из них мог обработать запрос на использование модема с данным логическим именем.

Module — модуль. Компонент программного обеспечения, входящий в модульную операционную систему (modular operating system) и выполняющий определенную функцию. Модули можно устанавливать или удалять в зависимости от набора ресурсов, необходимых для работы программного обеспечения компьютера. Кроме того, применение модулей позволяет настраивать операционную систему и приложения под конкретные потребности пользователя.

Monolithic Device Driver — монолитный драйвер устройства. Драйвер устройства, в котором программа управления связью между аппаратными средствами и операционной системой скомбинирована с сетевым протоколом. Поскольку подобному решению недостает гибкости, в настоящее время используется редко.

Multibank DRAM (MDRAM) — многоблочная DRAM. Видеопамять, разделенная на

несколько блоков (банков) для того, чтобы операции чтения и записи могли выполняться одновременно для нескольких блоков.

Multiprocessing — многопроцессорная обработка. Одновременное использование нескольких процессоров для выполнения вычислений. В зависимости от операционной системы такая обработка может выполняться *асимметрично,* когда некоторым процессорам назначаются определенные потоки, независимо от той нагрузки, которую создает их обработка, либо *симметрично,* когда потоки назначаются процессорам динамически, в соответствии со схемой равноправного планирования задач (equitable scheduling scheme). Если компьютер способен поддерживать одновременную работу нескольких процессоров, то этим термином обычно обозначают способность к мультипроцессорной обработке, заложенную в компьютер на уровне аппаратных средств. Однако термин *многопроцессорная обработка* может также применяться к сетевому компьютерному приложению (network computing application), выполняемому путем использования механизма взаимодействия процессов. Приложения клиент/сервер являются примером многопроцессорной обработки. Windows 98 *не поддерживает* многопроцессорные компьютеры. См. также *Interprocess Communication (IPC).*

Multitasking — многозадачность. Способность операционной системы быстро переключаться между исполняемыми потоками. Режим многозадачности позволяет распределить процессорное время (processor time) между потоками так, как если бы каждый поток выполнялся на отдельном медленном процессоре. Операционные системы, поддерживающие многозадачный режим, допускают запуск одновременно нескольких приложений и предоставляют для этого средства более высокого уровня, чем однозадачные (скажем, MS-DOS). Операционные системы фирмы Microsoft поддерживают либо коллективную многозадачность (cooperative multitasking), либо многозадачный режим с приоритетами (preemptive multitasking). В первом случае приложение возвращает управление процессору тогда, когда это необходимо другому приложению. Во втором же случае время для обработки потоков приложения выделяется самим процессором на основе приоритетов потоков. См. также *Multiprocessor, Multithreaded.*

Multithreaded — многопоточный. Процесс (программа) обеспечивающий параллельное обслуживание нескольких конкурирующих процессов. При исполнении многопоточных программ обрабатывается несколько цепочек операций вычислений. Таким образом, их работа опирается на средства многозадачной или многопроцессорной операционной системы. Наличие множества исполняемых цепочек операций позволяет программам одновременно решать несколько задач. В компьютерах, использующих многозадачный режим, применение многопоточности предоставляет дополнительные удобства, поскольку делает выполнение программ более равномерным и освобождает систему от необходимости переключаться между различными задачами. В многопроцессорных компьютерах многопоточность позволяет распределить вычислительную нагрузку между процессорами. Однопоточные программы не могут использовать преимущества многопроцессорного компьютера, однако на нем можно одновременно запускать несколько таких приложений. См. также *Multitasking, Multiprocessor.*

N

Named Pipes - именованный канал связи. Коммуникационный интерфейс прикладного программирования, используемый сетевыми приложениями. Реализован как компонент файловой системы, позволяет модифицировать программы без соответствующих средств интерфейса прикладных программ. Именованные каналы связи разработаны для обеспечения более надежных и удобных средств связи приложений клиент/сервер, чем простые средства NetBIOS. См. также *Interprocess Communications (IPC).*

NCP. См. *NetWare Core Protocol.*

NDIS. см. *Network Driver Interface Specification.*

NDS. см. *NetWare Directory Services.*

NetBEUI. см. *NetBIOS Extended User Interface.*

NetBIOS. см. *Network Basic Input/Output System.*

NetBIOS Extended User Interface (NetBEUI) — расширенный пользовательский интерфейс среды NetBIOS. Простой транспортный протокол сетевого уровня, разработанный для поддержки приложений NetBIOS. Протокол NetBEUI не маршрутизируемый и поэтому не пригоден для применения в больших сетях. Он является наиболее быстрым транспортным протоколом из всех поддерживаемых в Windows 98.
NetBIOS Gateway - шлюз NetBIOS. Комбинация программных и аппаратных средств, предоставляемая системами удаленного доступа (Remote Access Service) Windows NT и позволяющая передавать запросы NetBIOS, независимо от используемого транспортного протокола. Например, запросы NetBIOS от удаленного компьютера, подключенного посредством NetBEUI, могут быть посланы через сеть с помощью протокола NWLink. См. также *Network Basic Input/Output System (NetBIOS), NetBIOS over TCP/IP (NetBT), NetBIOS Extended User Interface (NetBEUI).*

NetBIOS over TCP/IP (NetBT) - NetBIOS над TCP/IP. Сетевая система, реализующая средства NetBIOS IPC дополнительно к стеку протокола TCP/IP. См. также *Network Basic Input/Output System (NetBIOS), Interprocess Communication (IPC), Transmission Control Protocol/Internet Protocol (TCP/IP).*

NetBT. см. *NetBIOS over TCP/IP (NetBT).*

NetDDE. см. *Network Dynamic Data Exchange.*

NetWare. Популярная сетевая операционная система, разработанная фирмой Novell в начале 80-х гг. NetWare — хорошо оптимизированная операционная система коллективного пользования, поддерживающая многозадачный режим и предназначенная для использования сетевыми серверами. Она поддерживает большинство основных клиентных операционных систем. Последние версии NetWare содержат инструменты графического интерфейса для взаимодействия с пользователем, предназначенные для администрирования с клиентных рабочих станций. Одно время NetWare занимала 70% рынка сетевых операционных систем, однако система Microsoft Windows NT сумела усилить свои позиции и частично вытеснить NetWare. См. также *Windows NT.*

NetWare Core Protocol (NCP) — протокол ядра NetWare. Используется для реализации процедуры, обеспечивающей ответы сервера на запросы с рабочих станций. Для подключения к серверу NetWare клиент должен поддерживать NCP.

NetWare Directory Services (NDS) — служба каталогов NetWare. В операционной системе NetWare это — распределенная иерархическая структура сетевых средств, например серверов, общих томов и принтеров. NetWare реализует систему NDS в виде структуры каталогов с развитыми средствами защиты и механизмами администрирования. Windows 98 поддерживает связь с томами NetWare с помощью приложения Service for NetWare Directory Service. См. также *NetWare, Bindery.*

NetWatcher. Интерактивное инструментальное средство, поставляемое с Windows 98, и

предназначенное для создания, управления и отслеживания удаленных общих ресурсов.

Network Basic Input/Output System (NetBIOS) — сетевая базовая система ввода/вывода. Сетевой протокол для обеспечения взаимодействия процессов приложений клиент/сервер. Разработан фирмой IBM в начале 80-х гг. NetBIOS предоставляет относительно примитивный механизм для организации связей в приложениях клиент/сервер, но ее широкое признание и наличие в большинстве операционных систем делают ее выбор логичным для простых сетевых приложений. Многие сетевые механизмы IPC в Windows NT реализуются с помощью NetBIOS. См. также *Interprocess Communication (IPC), Client/Server.*

Network Computer — сетевой компьютер. "Тонкое" клиентное устройство, предназначенное для запуска приложений на сервере терминала, а также локального запуска небольших (обычно, созданных на основе Java) приложений. См. также *Thin Client Netorking, Terminal Server.*

Network Driver Interface Specification (NDIS) — спецификация интерфейса сетевых драйверов. Спецификация Microsoft, которой должны соответствовать драйверы сетевых адаптеров при работе с сетевыми операционными системами Microsoft. Спецификация NDIS предоставляет привязки типа "многие-ко-многим", выполняемые между драйверами сетевых адаптеров и транспортными протоколами, что упрощает процесс разработки драйверов за счет исключения монолитных стеков драйверов/протоколов. См. также *Transport Protocol.*

Network Dynamic Data Exchange (NetDDE) — динамический обмен данными в сети. Механизм взаимодействия процессов, разработанный Microsoft для поддержки распространения DDE-приложений по сети. См. также *Interprocess Communication (IP), Dynamic Data Exchange (DDE).*

Network Interface Card (NIC) — сетевая интерфейсная плата. Соединительное устройство (оборудование) позволяющее компьютеру подключаться и связываться через сеть с другими сетевыми устройствами. См. также *Ethernet, Token Ring, Adapter.*

Network Layer — сетевой уровень. Уровень модели OSI, на котором устанавливается путь линий связи между двумя компьютерами с помощью маршрутизированных пакетов. Сетевой и транспортный уровни стека OSI реализуются транспортными протоколами. См. также *Internet Protocol (IP), Open Systems Interconnect Model (OSI).*

Network Number — сетевой номер. Идентификатор физического сегмента сети IPX/SPX, к которому подсоединен компьютер. Также называется внешним сетевым адресом. Вместе с узловым номером этот адрес идентифицирует компьютеры и их расположение в сети. См. также *Node Number.*

Network Operating System (NOS) — сетевая операционная система. Операционная система компьютера, специально спроектированная для оптимизации способности компьютера предоставлять сетевые услуги. Сетевые операционные системы запускаются на серверах. Так, Windows NT Server и NetWare являются сетевыми операционными системами, предназначенными для работы приложений клиент/сервер, а Windows 98 — пример одноранговой NOS. См. также *Windows NT Server, NetWare, Client/Server, Network Operating System (NOS), Peer Network, Operating System.*

Network Binding Interface — интерфейс сетевых связок. Интерфейс между драйвером сетевой карты и стеком протокола. Делает ненужными монолитные драйверы устройства. Функционально подобен API. См. также *Driver, Protocol Stack, Monolithic Device Driver, Application Programming Interface (API).*

New Technology File System (NTFS) **— файловая система новой технологии.** Защищенная, ориентированная на выполнение транзакций, файловая система, разработанная для Windows NT. Содержит модель системы защиты Windows NT, предназначенную для задания уровней доступа и распределения общих ресурсов. Оптимизирована для использования на жестких дисках емкостью свыше 500 Мбайт; требует слишком больших накладных расходов при использовании на жестких дисках емкостью менее 50 Мбайт.

NIC. См. *Network Interface Card.*

Node Number — узловой номер. Называется также внутренним сетевым адресом. Идентифицирует отдельный компьютер в сети IPX/SPX (точнее, плату NIC внутри компьютера — компьютер может иметь несколько узловых номеров, если в нем установлено несколько NIC). Этот номер объединяется с сетевым номером, что позволяет полностью идентифицировать компьютер и его расположение в сети. См. также *Network Number.*

Non-Browser — не-броузер. Компьютер сети, не поддерживающий список других компьютеров и служб сети. См. также *Browser, Browsing.*

NTFS. См. *New Technology File System.*

O

Open Graphics Language (OpenGL) — открытый язык обработки графики. Стандартный интерфейс для представления двух- и трехмерных визуальных объектов.

Open Shortest Path First (OSPF) — маршрутизация с предпочтением кратчайшего пути. Протокол определения маршрута, в котором маршрутизаторы логически упорядочиваются в древовидную структуру. Каждый маршрутизатор немедленно после подключения регистрирует себя на непосредственно примыкающих к нему маршрутизаторах и получает от них данные. Используя эту информацию, маршрутизаторы выстраивают пути к различным пунктам назначения сети, указывая при этом главный путь, а также резервные (в отличие от протокола RIP, который предусматривает установку единственного пути). Маршрутизаторы, использующие протокол OSFR, разделены по областям, которыми ограничена лавинная маршрутизация. Магистральный маршрутизатор пересылает маршрутные таблицы из одной области в другую.

Open System — открытая система. Сетевая система, которая может легко связываться с другими сетевыми системами, использующими одинаковые коммуникационные модели. См. также *Open Systems Interconnect (OSI) Model.*

Open Systems Interconnect (OSI) Model — модель взаимодействия открытых систем. Определяет возможности взаимодействия сетевых компонентов. Разработана ISO (International Standards Organization — Международная организация по стандартизации) для обеспечения совместимости аппаратного и программного обеспечения различных поставщиков. Модель OSI предусматривает разделение процесса передачи данных по сети на семь отдельных уровней. Каждый последующий, более привилегированный уровень использует функции предыдущих, менее привилегированных для обеспечения своей деятельности. См. также *Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer.*

OpenGL. см. *Open Graphics Language.*

Operating System — операционная система. Набор программных средств, отвечающих за распределение системных ресурсов (памяти, процессорного времени, дискового пространства, периферийных устройств) на основе которого исполняются приложения. Операционная система иногда может быть просто комплектом утилит, обеспечивающих ввод/вывод, реализуемых с помощью командной оболочки, например MS-DOS, или более сложной, использующей многозадачный режим с приоритетами, платформой исполнения приложений, наподобие Windows NT. См. также *Network Operating System (NOS), Preemptive Multitasking, Kernel.*

Optimization — оптимизация. Любые процедуры, уменьшающие загрузку компонентов аппаратного обеспечения путем исключения или снижения объема работы, выполняемой компонентом оборудования. Так, кэширование файла — пример оптимизации, уменьшающей рабочую нагрузку на жесткий диск.

OSI Model. См. *Open Systems Interconnect Model (OSI).*

P

Packet — пакет. Порция сетевых данных, содержащая адресную информацию, адреса источника и приемника пакета, а иногда — информацию, вводимую для исправления ошибок. См. также *Frame.*

Packet-Switched Network — сеть с коммутацией пакетов. Разновидность сети WAN, в которой не организуются виртуальные каналы между источником и приемником. Вместо этого каждый передаваемый по сети пакет несет с собой маршрутную информацию и поэтому может динамически выбирать свой путь. В течение одного сеанса различные пакеты выбирают различные пути, если, например, в середине передачи появится путь с меньшей стоимостью. См. также *Frame Relay, X.25, Routing, Cost.*

Page File. См. *Swap File.*

Partition — раздел. Специальным образом выделенная (на логическом уровне) часть жесткого диска, в которой находится отдельный том файловой системы. Можно использовать для организации на одном жестком диске нескольких операционных и файловых систем. См. также *Volume.*

Passive Hub — пассивный концентратор. Концентратор, который не управляет трафиком сети. См. также *Hub.*

PC Card — PC-карта. См. *Personal Computer Memory Card International Association.*

PCI. см. *Peripheral Connection Interface.*

PCMCIA. см. *Personal Computer Memory Card International Association.*

PDC. см. *Primary Domain Controller.*

Peer — одноранговый. Сетевой компьютер, предоставляющий ресурсы прочим компьютерам, а также использующий их общие ресурсы. Служит сервером общего назначения. См. также *Server, Client.*

Peer Network — одноранговая сеть. Сеть, в которой каждый компьютер может полностью использовать ресурсы остальной сети, причем централизованная система организации файлов

или общих ресурсов отсутствует — сеть конфигурируется и используется конечными пользователями. Сетевому администратору нет необходимости выполнять какие-либо работы с сервером, поскольку каждый узел администрируется самим пользователем.

Peripheral Device — периферийное устройство. Любое оборудование, напрямую или косвенно соединенное с системной платой компьютера. Периферийные устройства могут быть внешними (например, принтеры), или внутренними (например, сетевые платы).

Peripheral Connection Interface (PCI) — интерфейс периферийных устройств. Быстродействующая 32/64-битовая шина, разработанная фирмой Intel. Заслужила всеобщее признание в качестве преемника 16-битовой шины ISA. Шина PCI обеспечивает пропускную способность ввода/вывода примерно в 40 раз большую, чем у ISA. PCI - это 64-битовая шина, однако она обычно используется как 32-битовая. Может работать на тактовых частотах 33 или 66 МГц. При разрядности 32 бита и тактовой частоте 33 МГц пропускная способность шины достигает 133 Мбит/с.

Permissions — разрешение. Назначение уровня доступа к ресурсу группе или отдельному пользователю. Разрешение является одним из компонентов системы защиты. Оно регулирует доступ к ресурсам, используя в качестве ключевой информации имя пользователя или его принадлежность к какой-либо группе. Администратор, "выдавая" различные разрешения, может установить любой уровень доступа (например, "только чтение", "чтение/запись", "удаление") путем управления возможностями пользователей по инициализации служб объекта (object services). Защита обеспечивается проверкой соответствия кода защиты элементам списка управления доступом (access control list) каждого объекта. См. также *Security Identifiers (SIDs).*

Personal Computer Memory Card International Association (PCMCIA) — Международная организация производителей плат памяти для персональных компьютеров. Стандарт, разработанный организацией PCMCIA для описания небольших устройств размером с кредитную карточку, которые вставляют в гнезда (slots) портативных компьютеров (laptop computers). Как правило, эти устройства можно вставлять и вынимать из компьютера без его перезагрузки.

Используют три типа устройств PCMCIA, имеющие одинаковые длину и ширину, но разную толщину. Платы типа I толщиной 3,3 мм обычно применяют для комплектации компьютера дополнительной памятью ROM или RAM. Платы типа II толщиной до 5,5 мм часто используют в качестве факсов и модемов. Платы типа III могут быть толщиной до 10,5 мм и применяться для встраивания переносимых жестких дисков (portable disk drives).

Каждый тип устройств PCMCIA устанавливается в соответствующие гнезда: либо одна из плат данного типа, либо одна низшего типа. Например, в гнездо типа III можно установить либо одну плату типа III, либо одну плату типа II или I.

Physical Address — физический адрес. Адрес, "зашитый" в сетевую плату во время изготовления. Идентифицирует компьютер (точнее, сетевую плату) на канальном уровне модели OSI. См. также *Data Link Layer, Address Resolution Protocol (ARP).*

Physical Layer — физический уровень. Кабели, соединители и порты связи (connection ports) сети. См. также *Open Systems Interconnect (OSI) Model.*

Physical Topology — физическая топология. Физическая компоновка сети. См. также *Bus Physical Topology, Ring Physical Topology, Star Physical Topology, Logical Topology.*

Plenum — оболочка. Особое покрытие для сетевых кабелей, не выделяющее при горении

ядовитые газы. Поэтому, в соответствии с требованиями правил противопожарной безопасности кабели, прокладываемые в перекрытиях зданий, должны иметь именно такую оболочку. См. также *Polyvinyl Chloride (PVC).*

Plug-and-Play (PnP) — "включи-и-работай". Способность операционной системы автоматически конфигурировать платы расширения и некоторые другие устройства. Вам достаточно подключить устройство, а после перезагрузки приступить к работе, не заботясь об установках переключателей DIP, перемычек либо запуске программы установки. Данная технология позволяет установить в систему устройство Plug-and-Play без повторного конфигурирования аппаратного обеспечения или компьютерной системы.

Point-and-Print — "укажи-и-печатай". Прием работы, используемый для установки файлов драйвера сетевого принтера. Установка выполняется перемещением значка принтера сетевого компьютера, поддерживающего механизм Point-and-Print в папку Printers (принтеры). После этого документы можно отправлять на печать на сетевых принтерах путем перемещения отпускания значка документа на значке принтера.

Point-to-Point Protocol (PPP) — протокол двухточечный. Протокол линии связи канального уровня, используемый при создании двухузловых сетевых соединений, например последовательных или модемных линий связи. PPP работает с любым транспортным протоколом, который поддерживается обеими системами, соединенными линией связи. При совместном использовании с протоколом TCP/IP позволяет автоматически назначать адреса IP, DNS и шлюза. См. также *Internet Protocol (IP), Domain Name Service (DNS), Gateway, Line Protocol.*

Point-to-Point Tunneling Protocol (PPTP) — протокол туннельной двухточечной связи. Протокол канального уровня, используемый для создания защищенных соединений между частными сетями по сети Internet либо другим общедоступным сетям, соответствующим IP-спецификации (позволяет таким образом создать виртуальную частную сеть). Зависит от протокола PPP. См. также *Internet, Virtual Private Network, Point-to-Point Protocol (PPP).*

Polling — опрос. Метод, при использовании которого одно устройство периодически проверяет состояние другого, чтобы узнать, готово ли оно к обмену данными.

Polyvinyl Chloride (PVC) — поливинилхлорид. Недорогой синтетический диэлектрик, используемый в качестве наружного покрытия кабеля. При горении выделяет токсичные газы. В зависимости от условий (классифицируемых в соответствии с правилами противопожарной безопасности), применение кабелей с таким покрытием допустимо не во всех сетях. См. также *Plenum.*

PPP. См. *Point-to-Point Protocol.*

PPTP. См. *Point-to-Point Tunneling Protocol.*

Preemptive Multitasking — многозадачный режим с приоритетами. Такой тип многозадачности, реализованный на уровне операционной системы, при котором программа обработки прерываний, находящаяся в ядре, управляет распределением времени процессора между исполняемыми потоками. Потоку нет необходимости самостоятельно поддерживать многозадачность, поскольку микропроцессор сам его выгружает, используя прерывания, сохраняет его состояние, обновляет приоритеты всех потоков в соответствии с алгоритмом планирования и передает управление потоку с высшим приоритетом, ожидающему исполнения. См. также *Kernel, Thread, Operating System.*

Preferences — пользовательские значения системных переменных. Значения учетных записей пользователей (пароль, местонахождение профиля (profile location), основной каталог и сценарий входа).

Presentation Layer — уровень представления данных. Уровень модели OSI, описывающий методы взаимодействия компьютеров в сети, определяет способы конвертирования и трансляции информации между сеансовым и прикладным уровнями. См. также *Open Systems Interconnect Model (OSI)*.

Primary Domain Controller (PDC) — первичный контроллер домена. Сервер домена Windows NT, в котором хранятся основные копии баз данных системы защиты, а также учетных записей компьютеров и пользователей. Предназначен для идентификации рабочих станций. PDC может реплицировать свои базы данных на несколько резервных контроллеров домена (BDCs). Кроме того, обычно PDC служит главным броузером домена. См. также *Backup Domain Controllers, Domain, Master Browser.*

Print Driver — драйвер печати. Представляет собой особую программу, управляющую устройством печати. Для каждого принтера разрабатывается соответствующий ему драйвер. С этой целью для устройства каждого типа предусмотрен специфический набор команд управления.

Print Pooling — печатный пул. Логическая комбинация нескольких принтеров с одинаковыми именами. Дает возможность любому из них выполнить задание, отправленное на принтер с данным именем.

Print Server — сервер печати. Компьютер, к которому подключен принтер. Фактически, если задание на печать не направляется на специальный сетевой принтер, напрямую подключенный к сети, то оно сначала попадет на сервер печати.

Print Spooler (Print Queue) — буфер печати (очередь печати). Каталог или папка сервера печати, сохраняющая задание, отправленное на печать, до его выполнения. Очень важно, чтобы в любое время сервер и буфер печати имели достаточно места на жестком диске, чтобы разместить все задания на печать, ожидающие исполнения. См. также *Print Server.*

Priority — приоритет. Уровень важности выполнения программы, присвоенный потоку. В сочетании с прочими факторами уровень приоритета задает частоту, с которой данный поток будет занимать компьютерное время (в соответствии с алгоритмом планирования). См. также *Preemptive Multitasking, Thread.*

Process — процесс. Исполняемая программа, состоящая из одного или нескольких потоков. Для выполнения своих потоков, процесс инкапсулирует защищенную область памяти и соответствующее окружение.

Processor — процессор. Электронное устройство для автоматического выполнения наборов логических и арифметических операций. В отличие от микропроцессоров, процессоры могут состоять из нескольких отдельных устройств (микросхем). См. также *Microprocessor.*

Program — программа. Список инструкций процессора, составленный для выполнения определенной функции. Исполняемую программу называют *процессом (process)*. Пакет из одной или нескольких программ и сопутствующих данных, спроектированный для определенной цели (применения), называют *программным обеспечением (software) или приложением (application).*

Programmable Input/Output (PIO) — программируемый ввод/вывод. Метод, с помощью которого CPU перемещает данные из памяти периферийного устройства в основную память. В некоторых случаях вместо PIO используют более скоростной метод DMA. См. также *Direct*

Memory Access (DMA), Peripheral Device.

Programming Interfaces — программируемые интерфейсы. Механизмы взаимодействия процессов, предоставляющиеся выполняемым процессам программными средствами высшего уровня. Программируемые интерфейсы могут обеспечивать сетевую связь, графическое представление данных, а также службы программного обеспечения (software services) любого типа. См. также *Interprocess Communication (IPC).*

Protocol — протокол. Соглашение, принятое для установления связи между двумя частями компьютера. Точно так же, *сетевой* протокол — соглашение, использование которого позволяет двум компьютерам связываться через сеть.

Protocol Stack — стек протоколов. Набор сетевых протоколов, совместная работа которых обеспечивает передачу данных через сеть. Стеки протоколов действуют на нескольких уровнях модели OSI. См. также *Protocol, Open System Interconnect (OSI) Model.*

Proxy Server — прокси-сервер. Сетевой компьютер, исполняющий приложение, которое позволяет ему работать в качестве портала между одной сетью и другой, например между интрасетью и Internet. Может использоваться для защиты сети или выравнивания трафика, причем незаметно для клиентов.
Punchdown Block — врезной соединитель. Контактное устройство для соединения сетевых кабелей в топологию типа "звезда".

R

Radio Frequency Interference (RFI) — радиочастотные помехи. Возникают при передаче радиосигналов. RFI во многом подобны EMI, за исключением того, что под EMI понимаются помехи, создаваемые большими электрическими нагрузками (например, работой мощных электромоторов). Понятие RFI обычно применяют по отношению к помехам, возникающим при передаче сигналов как по кабелям, так и радиоканалам.

Random Access — произвольный доступ. Метод доступа, использование которого обеспечивает получение данных из любого места, т.е. без необходимости последовательного перемещения по всей области хранения. К устройствам с произвольным доступом относятся, например, жесткие диски. См. также *Sequential Access.*

Random Access Memory (RAM) — оперативное запоминающее устройство с произвольным доступом. Физическая память с произвольным *(не последовательным)* доступом. RAM имеет огромное значение для. работы компьютера, поскольку именно в ней хранятся все текущие данные, с которыми он работает. См. также *Static RAM (SRAM), Dynamic RAM (DRAM).*

Redirector — перехватчик (редиректор). Сетевое программное обеспечение, перехватывающее пользовательские запросы на ввод/вывод файла. В сетях Novel перехватчик реализован на основе компонент Workstation и Client Services for NetWare. В сетях Microsoft с этой целью используется программа Client for Microsoft Networks. Перехватчики позволяют применять серверы в качестве устройств хранения большой емкости, которые отображаются для клиентов как локальные.

Reduced Instruction Set Chip (RISC) - процессор с ограниченным набором команд. Вычислительная архитектура, использующая ограниченный набор выполняемых машинных команд. По этой причине соответствующие устройства могут быть достаточно просто реализованы с помощью современных полупроводниковых технологий. Обеспечивает

высокую скорость работы. При составлении программ для микропроцессоров RISC требуется большее число инструкций (т.е. программы становятся длиннее), чем для обычных микропроцессоров. Однако, поскольку эти инструкции проще, программа в целом лучше поддается оптимизации и, следовательно, работает быстрее. См. также *Microprocessor, Central Processing Unit (CPU).*

Registry — системный реестр. База данных, в которой хранятся установки, необходимые для работы Windows 98 и поддержки ее компонентов. В системном реестре находится вся информация о конфигурации, используемая компьютером, в виде иерархической структуры, и состоит из параметров (keys), разделов (hive) и записей значений (value entries). Для изменения установок имеется редактор системного реестра (REGEDIT).

Remote Access — удаленный доступ. Система, позволяющая устанавливать сетевые соединения по телефонным линиям через модемы или цифровые адаптеры (digital adapters). Компьютер, инициализирующий соединение, называют "гостем", а компьютер, отвечающий на запросы — сервером удаленного доступа RAS (RAS host). См. также *Remote Control.*

Remote boot — удаленная загрузка. Система, обеспечивающая запуск через сеть бездисковых компьютеров.

Remote Control — дистанционное управление. Соединение с другим компьютером с целью управления. Все приложения выполняются на удаленном компьютере, однако команды и данные вводятся с локального компьютера и результаты работы отображаются на его мониторе.

Remote Procedure Calls (RPC) — удаленный вызов процедур. Механизм сетевого взаимодействия процессов, позволяющий распределять выполнение одного приложения между несколькими компьютерами, работающими в одной сети. См. также *Interprocess Communications (IPC).*

Repeater — повторитель. Устройство, регенерирующее электрический или световой сигнал, обеспечивая увеличение дальности связи. Используется для расширения сетей Ethernet. См. также *Extender, Ethernet.*

Request for Comments (RFC) — запрос комментариев. Любой компонент набора принятых или предлагаемых стандартов, описывающих работу Internet.

Resource - ресурс. Любая часть компьютерной системы, которая может использоваться запущенной программой (например, общий сетевой каталог или принтер). См. также *Share.*

Ring Physical Topology — кольцевая топология. Физическая организация сети, при которой все компьютеры соединяются одним кабелем, замкнутым в кольцо. Используется в основном в оптоволоконных сетях, а также в сетях FDDI. См. также *Physical Topology, Fiber Distributed Data Interface (FDDI), Fibre Channel.*

RIP. см. *Routing Information Protocol.*

RISC. см. *Reduced Instruction Set Chip.*

Roaming User Profile — профиль мобильного пользователя. Профиль пользователя, сохраняемый для загрузки с сервера. Наличие сменных профилей позволяет пользователям получать доступ к собственным профилям с любого компьютера сети. См. также *User Profile.*

Root Bridge — корневой мост. Мост с самым низким приоритетом в сети. По отношению к нему ранжируются все остальные мосты. Корневой мост определяется при включении сети, когда все мосты обмениваются информацией о своих приоритетах и стоимости. См. также *Bridge.*

Router — маршрутизатор. Устройство, передающее пакеты данных между сетями, в которых использует общий протокол маршрутизации сетевого уровня. Маршрутизаторы обеспечивают организацию межсетевых соединений. См. также *Network Layer.*

Routing Information Protocol (RIP) — протокол передачи информации о маршрутизации. Входит в семейство протоколов TCP/IP, позволяет маршрутизаторам обмениваться информацией о маршруте с соседними маршрутизаторами, включая стоимость данного маршрута и статус маршрутизатора. Кроме того, существуют версии RIP для семейства протоколов IPX/SPX. См. также *Transmission Control Protocol/Internet Protocol (TCP/IP).*

Routing Table — таблица маршрутизации. Список адресов локального сегмента сети, поддерживаемых маршрутизатором. Если адрес места назначения, указанный в принятом маршрутизатором пакете, отсутствует в таблице маршрутизации, то он направит пакет далее.

RPCs. См. *Remote Procedure Calls.*

S

Safe Mode — защищенный режим. Режим работы операционной системы, при котором не загружается системный реестр, а также файлы CONFIG.SYS и AUTOEXEC.BAT. Не загружаются сетевые программы и драйверы защищенного режима. Система Windows 98 запускается в стандартном видеорежиме VGA (загружаются файлы HIMEM.SYS, IFSHLP.SYS, а также оператор Path (путь) из файла MSDOS.SYS). Защищенный режим полезен при поиске и устранении неполадок с помощью драйверов защищенного режима.

SAM. См. *Security Accounts Manager.*

SAP. См. *Service Advertisement Protocol.*

Scheduling — планирование. Процесс выбора исполняемого потока в соответствии с его приоритетом и прочими факторами. См. также *Preemptive Multitasking.*

Screw-Mounted Adapter (SMA) — соединитель с резьбовой оправкой. Тип соединителей оптоволоконных кабелей, в котором используется стыковочный механизм с навинчивающейся гайкой. Применяется реже, чем подпружиненная вкрутка (ST). См. также *Fiber Optic Cable, Spring-Loaded Twist.*

SCSI. см. *Small Computer Systems Interface.*

Search Engine — машина поиска. Узел Web, предназначенный для ответов на специфические запросы. С этой целью он просматривает локальные массивы баз данных Web-страниц и выдает URL страниц, соответствующих искомой фразе. См. также *World Wide Web, Uniform Resource Locator (URL).*

Sector — сектор. Физически наименьший элемент хранения информации на жестком диске. В файловых системах Microsoft секторы логически объединяются в кластеры. См. также *Cluster.*

Security — защита, система защиты. Набор мер, принимаемых для защиты системы от

случайной или намеренной утраты или искажения данных. Обычно реализован в форме процедур проверки учетных данных и наложения ограничений на доступ. См. также *Security Identifiers (SIDs), Security Account Manager (SAM).*

Security Account Manager (SAM) — диспетчер учетных записей системы защиты. Исполняемый модуль Windows NT, идентифицирующий имя и пароль пользователя. Для этого используется база данных учетных записей и генерируется маркер доступа, в который входит информация об уровне допуска пользователя. См. также *Security, Security Identifiers (SIDs).*

Security Identifiers (SID) — защитные коды. Идентифицируют конкретного пользователя или группу пользователей в системе защиты Windows NT. В защитных кодах содержится полный набор информации об уровнях допуска пользователей и группы в целом.

Segment — сегмент. Участок сети, отделенный от нее маршрутизатором. См. также *Router.*

Sequential Access — последовательный доступ. Метод доступа к данным, использование которого обеспечивает их получение только последовательно, в порядке записи на устройство хранения (например, стример). В соответствии с ним при поиске невозможно пропустить какую-либо часть данных.

Serial Line Internet Protocol (SLIP) — протокол последовательной межсетевой связи. Реализация протокола IP в последовательных линиях связи. SLIP в настоящее время вытеснен протоколом PPP. См. также *Point-to-Point Protocol (PPP), Internet Protocol (IP).*

Server — сервер. Сетевой компьютер для обслуживания запросов на предоставление ресурсов, поступающих от других сетевых компьютеров. См. также *Client, Resource.*

Server Element — серверный компонент. Часть программного обеспечения, используемая при удаленном доступе или управлении на компьютере, к которому выполняется подключение. См. также *Client Element, Remote Control, Remote Access, Thin Client Networking.*

Server Message Blocks (SMB) — блоки сообщений сервера. Сетевой протокол, применяемый в сетевых операционных системах Microsoft. Позволяет одному компьютеру использовать файлы и прочие ресурсы другого, точно так же, как если бы они были локальными. К сетям 8MB относятся LAN Manager, Windows for Workgroups, Windows NT, Windows 98 и LAN Server.

Service — обслуживание, служба, услуга. Набор программ для реализации конкретной функции другого процесса. К службам относится большинство компонентов пользовательских приложений Windows NT.

Service Advertisement Protocol (SAP) — протокол объявления доступных служб. Пакет NetWare, передаваемый по сети каждые 60 с. Содержит имя и список общедоступных ресурсов сервера. Система Windows 98 позволяет генерировать SAP, поэтому клиенты сети NetWare увидят окно Windows 98 как окно сервера NetWare.

Session Layer — сеансовый уровень. Уровень модели OSI, предназначенный для обеспечения и поддержки сеанса двусторонней связи между двумя компьютерами в течение требуемого промежутка времени. С этой целью на сеансовом уровне используются средства транспортного уровня. См. также *OSI Model, Transport Layer.*

Shadow Packets — теневые пакеты. Возникают при неправильном согласовании кабелей в

сети Ethernet. Подлинный пакет, дойдя до конца сегмента, отражается от него, не разрушаясь. Теневые пакеты ухудшают сетевой трафик. См. также *Ethernet, Terminate.*

Share — ресурс. Каталог или принтер, предоставленный в совместное использование сервером либо равным ему компонентом сети. См. также *Resource, Server, Peer.*

Share-Level Security — защита на уровне ресурсов. Стандартный уровень зашиты, предусмотренный в Windows 98. Защита на уровне ресурсов основана на паролях, назначенных для доступа к общим ресурсам.

Shielded Twisted Pair (STP) - экранированная витая пара. Разновидность кабеля типа витая пара. В нем проводники защищены от внешних воздействий не только за счет их скручивания, но и применением дополнительного экранирующего слоя металлической фольги. Обычно используется в сетях Token Ring. См. также *Twisted Pair, Token Ring.*

Shell — оболочка. Пользовательский интерфейс операционной системы. Обеспечивает запуск приложения и управление файловыми системами.

Security ID (SID). См. *Security Identifiers.*

Simple Network Management Protocol (SNMP) — простой протокол управления сетью. Протокол Internet, позволяющий управлять сетевым оборудованием, таким, как маршрутизаторы, коммутаторы, серверы и клиенты с единственного клиентного компьютера сети. См. также *Internet Protocol (IP).*

Small Computer Systems Interface (SCSI) — интерфейс малых вычислительных систем. Быстродействующий параллельный шинный интерфейс, используемый для подключения к компьютеру жестких дисков, приводов компакт-дисков, стримеров и прочих периферийных устройств. В SCSI реализован принцип параллельного интерфейса, применяемый в компьютерах Macintosh, PC и во многих системах UNIX для подключения к компьютеру периферийных устройств. Обеспечивает более высокую скорость передачи данных (до 80 Мбит/с), чем последовательные и параллельные порты или дисковые контроллеры IDE и EIDE. К одному SCSI-порту можно подключить несколько устройств, так что SCSI можно рассматривать скорее как шину ввода/вывода, а не просто интерфейс.

SneakerNet. Копирование данных с жесткого диска на гибкий, а затем транспортировка гибкого диска к другому компьютеру для отправления по сети ссылки или печати этого файла. Название (sneakers — спортивные туфли) указывает на необходимость перемещения носителя информации между компьютерами для передачи данных.

Socket — гнездо. 1. Часть межсетевого адреса узла IPX, отвечающая за представление целевого адреса в пакете IPX. Некоторые гнезда резервируются для отдельных приложений. Например все пакеты запросов NCP помещаются в гнездо 451h. 2. Двунаправленный канал связи для обмена данными между клиентным и серверным приложениями. См. *Remote Procedure Calls (RPCs).*

Solid Wire — одножильный провод. Конструктивное исполнение некоторых электрических кабелей. Состоит из единственного проводника.

Source Route Bridging — мостовая передача с маршрутизацией от источника.
Метод соединения с помощью мостов, используемый в сетях Token Ring для определения наилучшего пути к заданному пункту и сохранения записи о нем. Такая маршрутизация предпочтительнее применения метода STA, поскольку предполагает динамический поиск пути вместо выполнения обновления при повреждении ранее найденных путей (подобно

STA). См. также *Bridge, Spanning Tree Algorithm (STA), Router.*

Source Routing (SR)— маршрутизация от источника. Метод, при котором маршрутизатор сам определяет наилучший путь к пункту назначения пакета.

Spanning Tree Algorithm (STA) — алгоритм "остовного дерева". Алгоритм определения направления передачи данных через мосты. Используется в сетях Ethernet для определения наилучшего пути к любому заданному сегменту с последующим блокированием остальных путей. Если доступен единственный путь, мост не позволяет образовать петлю.

Spooler — спулер, программа буферизации. Перехватывает информацию, направляемую к драйверу медленного устройства (например, принтер), и записывает ее в буфер. Это делается для того, чтобы приложение, отправляющее данные на это устройство, не приостанавливало свою работу, ожидая завершения передачи данных.

Spring-Loaded Twist (SLT) — подпружиненная втулка. Тип разъемов для оптоволоконных кабелей. Используется чаще, чем соединители с резьбовой оправой (SMA). См. также *Fiber Optic Cable, Screw-Mounted Adapter (SMA).*

Star Physical Topology — сеть, построенная по схеме "звезда". Сетевая топология, имеющая звездообразное строение: каждый компьютер соединен отдельным кабелем с центральным концентратором, который обеспечивает связь всех узлов сети через центральный пункт коммутации. См. также *Physical Topology, Hub, Connected Star.*

Static RAM (SRAM) — статическая RAM (статическое ОЗУ). Тип микросхем памяти, используемых в качестве кэш-памяти CPU. Не требует регенерации содержимого. Сохраняет все поступившие данные до тех пор, пока не будут записаны новые или не будет выключен компьютер. См. также *Random Access Memory (RAM), Dynamic RAM (DRAM), Caching, Central Processing Unit (CPU).*

Step Index Cable - оптоволокно со ступенчатым изменением показателя преломления. Многомодовый оптоволоконный кабель, в котором световые лучи распространяются по зигзагообразным траекториям. См. также *Fiber Optic Cable, Mode, Modal Dispersion.*

Store-and-Forward Switching — коммутация с промежуточным хранением.
Процесс передачи данных, при котором коммутатор принимает весь фрейм (кадр), проверяет наличие в нем ошибок и только после этого направляет по указанному MAC-адресу. Пересылаются только те фреймы, в которых не обнаружено ошибок. Такой метод менее производителен, чем сквозная коммутация, однако обеспечивает более полный контроль ошибок. Коммутацию с промежуточным хранением поддерживают не только мосты, но и некоторые коммутаторы. См. также *Switch, Bridge, Cut-Through Switching.*

Stranded Wire — многожильный провод. Конструктивное исполнение некоторых электрических кабелей. Многожильные кабели состоят из нескольких переплетенных (combined) проводов определенного сечения. Отличаются большей гибкостью, чем одножильные, однако высокочастотный сигнал в них затухает быстрее.

Subnet — подсеть. Сегмент сети IP, идентифицируемый особой маской подсети. См. также *Internet Protocol (IP), Subnet Mask.*

Subnet Mask — маска подсети. Число, используемое для определения подсети, к которой относится IP-адрес. IP-адреса состоят из двух компонентов — сетевого адреса и адреса главной машины (host address). Обычно их записывают в десятичном формате (в виде разделенных точкой октетов), однако фактически IP-адреса представляют собой двоичные

числа. Маска подсети тоже двоичное число. У всех IP-адресов, относящихся к данной подсети, в сетевой части адреса цифра 1 должна стоять в одних и тех же местах (в двоичной записи).

Swap File — файл подкачки. Файл на жестком диске, в котором хранятся временно выгруженные из памяти (с целью ее высвобождения) части запущенных программ. Процессор может обрабатывать только те данные, которые хранятся в RAM. Чтобы сохранять больше данных, чем допускает RAM, в современных компьютерах используется *виртуальная память (virtual memory)*. В этом случае данные, которые не используются в текущий момент, сохраняются в специально выделенной области жесткого диска. При необходимости данные считываются с жесткого диска и загружаются в память. Такая область жесткого диска называется файлом подкачки *(swap file)* или страничным файлом *(page file)*. См. также *Virtual Memory*.

Switch — коммутатор. Интеллектуальный концентратор, считывающий физические адреса принимаемых пакетов, а затем передает пакет только в тот порт, через который можно получить доступ к этому адресу. См. также *Hub, Cut-Through Switching, Store-and-Forward Switching, Physical Address.*

Synchronized Graphics RAM (SGRAM) — синхронная графическая RAM.
Высокоскоростная однопортовая видеопамять.

System Policy - набор системных правил. Набор правил, создаваемый с помощью редактора системных правил (System Policy Editor). Используют для управления степенью свободы действий пользователя по изменению параметров своего окружения и выполнению каких-либо операций. Может применяться к конкретному пользователю или группе пользователей, компьютеру или сразу всем пользователям. Вводится путем замены текущих установок системного реестра установками из набора системных правил. См. также *Registry, System Policy Editor.*

System Policy Editor — редактор набора системных правил. Утилита из группы административных программных средств, использующаяся для создания набора системных правил. В Windows 98 данные утилиты устанавливают *только* вручную с помощью аплета Add/Remove Programs (Установка/удаление программ). См. также *System Policy*.

T

TAPI. См. *Telephony Application Program Interface.*

Taskbar — панель задач. Расположена в нижней части экрана, на которой отображаются пиктограммы запущенных программ, а также кнопка меню Start (Пуск), позволяющая получать или запускать другие приложения. Используется для переключения или запуска новых программ. Кроме того, на панели задач отображается информация о состоянии системы и сервисная информация, например, показания часов. Некоторые приложения также отображают информацию на панели задач, например, выводят значок принтера при печати документа или изображение письма при поступлении электронной почты.

TCP. См. *Transmission Control Protocol.*

TCP/IP. См. *Transmission Control Protocol/Internet Protocol.*

TDI. см. *Transport Driver Interface.*

Telephony Application Program Interface (TAPI) — интерфейс программирования

приложений телефонной связи. Стандартный метод, предусмотренный в Windows 98 для программирования интерактивных средств телефонной связи.

Templates — шаблоны. ASCII-файлы, хранящие соответствующие параметры и значения системного реестра. Файлы шаблонов (файлы .ADM) используют для создания системных правил.

Terminal Emulation — эмуляция терминала. Метод, с помощью которого персональные компьютеры эмулируют неинтеллектуальные терминалы (dumb terminal), используемые для связи с мэйнфреймами.

Terminal Server — сервер терминала. Сервер, программное обеспечение которого допускает локальный запуск приложений. При этом выводимые приложением данные отображаются на рабочем столе клиентного компьютера. Исходные данные, необходимые для работы программы вводятся клиентом. См. также *Thin Client Networking.*

Terminator — терминатор, заглушка. Устройство, устанавливаемое на конце коаксиального кабеля сети Ethernet, отмечает конец сегмента. Без правильного терминирования по сети будут распространяться теневые пакеты. См. также *Bus Physical Topology, Ethernet, Shadow Packets.*

Thicknet — "толстая" сеть. Толстый коаксиальный кабель, используемый в качестве магистрального в сетях 10Base5. Несмотря на меньшее затухание сигнала, чем в "тонких сетях", применяется редко из-за чрезмерной жесткости кабеля.

Thin Client Networking — тонкая клиентная сеть. Вариант сети, объединяющей сервер терминала с клиентными компьютерами. Каждый клиент проводит собственные сеансы с сервером терминала, на котором исполняет приложения. Вводимые данные генерируются на клиентном компьютере и загружаются на сервер терминала, а затем с помощью команд отображения (display commands) выводятся на монитор клиента. См. также *Terminal Server, Display Protocol.*

Thinnet — "тонкая" сеть. Коаксиальный кабель, используемый в сетях 10Base2. В настоящее время кабель такого типа используется чаще, чем кабель для "толстой" сети (Thicknet).

Thread — поток. Список инструкций (команд), выполняемых компьютером при решении конкретной задачи. Каждый поток создается в контексте соответствующего процесса, который содержит защищенную область памяти и окружение потоков. Многопоточные процессы предусматривают одновременное выполнение нескольких задач. См. также *Process, Preemptive Multitasking, Program.*

Throughput — пропускная способность. Фактическая скорость работы сети, вычисляемая путем перемножения полосы пропускания и сетевой скорости (network speed). См. также *Bandwidth.*

Token Master — задатчик маркера. Узел сети Token Ring, управляющий сетевыми маркерами. Называется также активным монитором. См. также *Token Ring, Token Packet.*

Token Packet — маркерный пакет. Административный маркер, используемый в сетях Token Ring для инициализации передачи данных. Пока компьютер не получит маркер, он не сможет приступить к передаче. См. также *Token Ring.*

Token Ring. Стандарт локальных сетей канального уровня, разработанный фирмой IBM. По

своей популярности занимает второе место. Для обеспечения доступа в сеть множества компьютеров в сетях Token Ring применяют метод передачи маркера *("token"}*. Сети Token Ring могут работать со скоростью до 16 Мбит/с. См. также *Data Link Layer.*

Transmission Control Protocol (TCP) — протокол управления передачей. Протокол транспортного уровня, гарантирующий отправку и получение пакетов по протоколу IP. См. *Internet Protocol (IP).*

Transmission Control Protocol/Internet Protocol (TCP/IP) — протокол управления передачей/протокол Internet. Набор сетевых протоколов, на основе использования которых создана глобальная сеть Internet. В настоящее время применяют также для создания множества корпоративных сетей. TCP/IP - общий термин, относящийся либо к протоколам TCP и IP, которые используются совместно, либо полному набору протоколов Internet. Протокол TCP/IP является стандартным протоколом Windows NT.

Transparent Bridging — прозрачный мост. Простой метод соединения с помощью мостов, при котором мост накапливает информацию о том, какие адреса доступны каждому конкретному порту. Когда на мост поступает пакет из сегмента сети, он сразу направляет его через соответствующий порт.

Transport Driver Interface (TDI) — интерфейс транспортных драйверов.
Спецификация транспортных протоколов Windows NT, используемых службами высшего уровня — программными интерфейсами, файловыми системами и механизмами взаимодействия процессов. См. также *Transport Protocol.*

Transport Layer — транспортный уровень. Уровень модели OSI, гарантирующий последовательное отправление и прием пакетов между двумя компьютерами в интерсетях. Например, протокол TCP является протоколом транспортного уровня для протокола TCP/IP.

Transport Protocol — транспортный протокол. Система организации отправления и приема дискретных информационных пакетов между любыми двумя сетевыми компьютерами. Транспортные протоколы могут работать на канальном, сетевом, транспортном или сеансовом уровнях модели OSI. В эти протоколы встроены соответствующие программные средства, ориентированные на установление соединений.

Truncated Binary Exponential Backoff — усеченный двоичный порядок выдержки времени. Метод, с помощью которого узлы Ethernet определяют порядок возобновления передачи данных после случившегося конфликта. См. также *Ethernet, Collision.*

Tunneling — туннелирование. Метод передачи пакетов с помощью протокола, не поддерживаемого сетью. На время прохождения по сети, не поддерживаемые пакеты "вкладываются" в поддерживаемые, а в месте назначения "извлекаются" из них.

Twisted Pair — витая пара. Кабель, состоящий из четырех изолированных проводов, попарно скрученных между собой. Эти витые пары проводов могут быть как экранированными, так и неэкранированными. Они подразделяются на пять категорий, различающиеся по типу проводов, числу витков на погонный фут, а также сложностью скруток. Для прокладки новых сетей чаще всего используют кабель категории 5 (высший стандарт). См. также *Radio Frequency Interference (REI), Solid Wire, Shielded Twisted Pair (STP), Unshielded Twisted Pair (UTP).*

U

UNC. См. *Universal Naming Convention.*

Uniform Resource Locator (URL) — универсальный локатор ресурсов.
Полный путь к конкретному документу или разделу на компьютере, подключенному к сети Internet, а также метод доступа к нему, т.е. протокол работы с программами сервера, функционирующими на удаленном компьютере. Например, http://www.microsoft.com представляет собой URL серверного узла World Wide Web фирмы Microsoft, в то время как ftp://ftp.mwmicro.com — узел загрузки файлов драйверов MidWest Micro. Использование URL позволяет вставлять в документ или сообщение электронной почты гипертекстовые ссылки на конкретный ресурс. См. также *HTTP, World Wide Web (WWW), Hypertext Transfer Protocol (HTTP).*

Universal Naming Convention (UNC) **— соглашение об универсальных именах.**
Соглашение, принятое многими продавцами и разработчиками, использующими различные платформы, для идентификации общедоступных сетевых ресурсов. См. также *Mandatory User Profile.*

UNIX. Многозадачная, многопользовательская, переносимая операционная система, разработанная фирмой AT&T в начале семидесятых годов. Первоначально бесплатно предоставлялась университетам как экспериментальная операционная система. Благодаря доступности, способности к масштабированию на многопроцессорных компьютерах и наличию сопутствующих сетевых протоколов, UNIX стала основной операционной системой, используемой в Internet. В наибольшей мере соответствует требованиям к универсальной операционной системе. Доступна широкому кругу вычислительных аппаратных средств, начиная от ПК и заканчивая суперкомпьютерами Cray. См. также *Multitasking, Internet.*

Unshielded Twisted Pair (UTP) — неэкранированная витая пара. Кабель, состоящий из двух изолированных проводов, попарно скрученных между собой. Часто используется в сетях 10BaseT. См. также *Twisted Pair, WBaseT.*

User Name — имя пользователя. Имя пользователя в учетной записи системы входной идентификации. См. также *Security.*

User Profile — профиль пользователя. Набор данных, описывающих конфигурацию рабочего стола каждого пользователя, включая информацию о цвете, ярлыках, приложениях, расположенных на рабочем столе, и другую информацию о настройках пользователя. См. также *Roaming User Profile, Mandatory User Profile.*

User-Level Security — защита на уровне пользователя. Тип метода управления доступом, применяемый при совместном использовании ресурсов Windows 98. Степень доступа определяется правами, зафиксированными в учетной записи конкретного пользователя или группы. Чтобы задействовать защиту на уровне пользователей, компьютер Windows 98 должен быть связан с сервером Windows NT или NetWare, на котором хранится база данных учетных записей пользователей сети.

UTP. См. *Unshielded Twisted Pair.*

V

Virtual Machines — виртуальные машины. Программное обеспечение, имитирующее работу физического устройства. В Windows 98 оно используются, чтобы "обманным путем" заставить программу считать, что она имеет монопольный доступ ко всем физическим устройствам системы. Виртуальные машины работают с уровнем защиты Ring 3 (см. *x86 Ring Architecture), а* для получения доступа к памяти и устройствам применяют методику передачи

сообщений (message passing technique).

Virtual Memory — виртуальная память. Система организации памяти, позволяющая приложению воспринимать участок памяти на жестком диске (файл подкачки) как большой непрерывный блок оперативной памяти. Таким образом освобождается занятая ими оперативная память, которую можно использовать для других задач. Виртуальная память "скрывает" процесс "подкачки" памяти от приложений и служб высшего уровня. См. также *Swap File, Kernel.*

Virtual Private Network (VPN) **- виртуальная частная сеть.** Создается "внутри" общедоступной сети (например, Internet). Для работы такой сети необходимо использовать туннельные протоколы такие, как PPTP. См. также *Point-to-Point Tunneling Protocol (PPTP), Internet, Tunneling, IP Security (IPSec), Layer 2 Tunneling Protocol (L2TP).*

Volume — том. Набор данных, упорядоченных по каталогам, содержащим файлы, и отмеченный буквенным обозначением диска. Как правило, тома входят в один раздел диска, однако в наборах томов и чередующихся наборах данных том может распределяться по нескольким разделам.

W

Wait State — режим ожидания. Цикл работы CPU, в течение которого он не выполняет никаких операций, поскольку ожидает получения данных от какого-либо компонента. См. также *Central Processing Unit (CPU).*

Web Browser — броузер Web. Приложение, создающее запросы в формате HTTP и форматирует полученные пользователем документы HTML. Большинство Web-броузеров "понимают" все стандартные протоколы Internet. См. также *Hypertext Transfer Protocol (HTTP), Hypertext Markup Language (HTML), Internet.*

Web Page — страница Web. Любой HTML-документ, хранящийся на сервере HTTP. См. также *Hypertext Transfer Protocol (HTTP), Hypertext Markup Language (HTML), Internet.*

Web Site — Web-узел. Связанный набор документов HTML, находящийся по одному адресу Internet. Обычно узел ориентирован на определенную тематику или вкус. См. также *Hypertext Markup Language (HTML), Internet.*

Wide-Area Network (WAN) — **глобальная сеть.** Сеть, выходящая за пределы одного здания.

Winl6. Набор программ-приложений, предоставляемый 16-битовыми версиями Microsoft Windows: Windows 3.1 и Windows for Workgroups 3.11.

Win32. Набор программ-приложений, предоставляемый 32-битовыми версиями Microsoft Windows: Windows 95, Windows 98 и Windows NT.

Windows 2000. Следующее поколение известной сетевой операционной системы Windows NT. Windows 2000 фактически представляет собой набор из четырех операционных систем, охватывающий как сетевых клиентов, так и серверные операционные системы, спроектированные для конкуренции с мэйнфреймами. См. также *Windows NT.*

Windows 3.11 for Workgroups. 16-битовая версия Windows, использующая интерфейс Windows 3.x, и предоставляющая средства для работы одноранговой сети. Позволяет запускать только 16-битовые приложения.

Windows 98. 32-битовая версия Windows, спроектированная для компьютеров среднего уровня, основанных на платформе x86. Предусмотрены средства для работы одноранговой сети, поддержка Internet, а также поддержка выполнения 16- и 32-битовых приложений.

Windows DRAM (WDRAM). Высокоскоростная двухпортовая оперативная память, оптимизированная для использования в подсистемах Windows (windowing sybsystems) откуда и произошло название.

Windows Internet Name Service (WINS) **— система присвоения имен Internet для Windows.** Предусмотренная в Windows NT для сетей Microsoft система установления соответствия между IP-адресами и именами NetBIOS. Это позволяет пользователям обращаться к компьютерам по легко запоминаемым именам NetBIOS, и в то же время работать с IP-адресами, необходимыми протоколу TCP/IP.

Windows NT. 32-битовая версия Microsoft Windows, предназначенная для мощных компьютеров, основанных на платформе x86 или Alpha. В эту операционную систему включены средства, для работы одноранговых сетей, серверные сетевые средства, клиентные и серверные средства Internet, а также большой набор утилит.

Windows Terminal — терминал Windows. Неинтеллектуальный терминал, используемый в тонкой клиентной сети (thin client networking) с операционной системой, поддерживающей графический пользовательский интерфейс, например, Windows NT. Его возможности по обработке данных и память рассчитаны на передачу изображений от приложений, исполняемых на сервере терминала, но не на локальный запуск приложений. См. также *Thin Client Networking, Terminal Server, Network Computer.*

WINS. см. *Windows Internet Name Service.*

Wireless Networking — беспроводная сеть. Сеть, в которой в качестве физической среды передачи используется не кабель, а эфир. Передача данных в беспроводных сетях обычно осуществляется средствами радиосвязи. Это придает сети огромную гибкость и расширяет зону действия, однако ее пропускная способность сравнительно невысока. Для обеспечения связи с внешними периферийными устройствами чаще используют более высокочастотные инфракрасные (оптические) сигналы. См. также *Radio Frequency Interference (RFI), Infrared Communications.*

Word Size — длина слова. Стандартная единица данных, используемая компьютером. Как правило, эта длина равна разрядности шины CPU. См. также *Central Processing Unit (CPU).*

Workgroup — рабочая группа. В сетях Microsoft так называют группу связанных компьютеров. Это может быть такая группа, для которой не требуется общей системы защиты и взаимодействия с доменом. В отличие от централизованного управления доменом в рабочих группах централизованное управление отсутствует. См. также *Domain.*

Workstation — рабочая станция. Мощный персональный компьютер, работающий под управлением операционной системы, использующей многозадачный режим с приоритетами, такой как UNIX или Windows NT. Кроме того, рабочей станцией часто называют клиентный компьютер.

World Wide Web (WWW). Семейство серверов Internet, предоставляющих документы с гипертекстовым форматированием клиентам Internet, использующим Web-броузеры. WWW дает возможность работать в Internet с простым графическим интерфейсом, чем в

значительной степени обусловлен взрывной рост Internet начиная с середины 90-х годов.

Write-Back Caching — кэширование с обратной записью. Метод оптимизации кэширования. Данные, записанные в медленное устройство хранения (жесткий диск), остаются кэшированными до тех пор, пока кэш не будет заполнен, либо до тех пор, пока в результате выполнения последовательных операций записи они не будут перезаписаны. Это позволяет значительно уменьшить число операций записи в медленное устройство хранения, поскольку по мере поступления новой информации отпадает необходимость в повторных обращениях к этому медленному устройству. Кроме того, данные, помещенные в кэш с обратной записью, доступны для считывания. Если же что-либо помешает процедуре кэширования записать данные в медленное устройство хранения, кэшированные данные будут утрачены. См. также *Caching, Write-Through Caching.*

Write-Through Caching — кэширование с прямой записью. Метод оптимизации кэширования, при котором данные, записанные в медленное устройство хранения (жесткий диск), сохраняются в КЭШе для последующего повторного считывания. В отличие от кэширования с обратной записью, данные сразу записываются в медленное устройство хранения. Поэтому кэширование с прямой записью не оптимально, однако более безопасно.

WWW. См. *World Wide Web.*

X

X.25. Стандарт, описывающий интерфейс (электрические соединения, протокол передачи данных, средства обнаружения и исправления ошибок и пр.) в сети с коммутацией пакетов. Принцип его работы подобен принципам работы *Frame Relay,* однако из-за наличия средств контроля ошибок этот метод работает несколько медленнее. При этом в ненадежных сетях он в большей мере гарантирует отсутствие ошибок.

X86 Ring Architecture - кольцевая архитектура X86. Термин, обозначающий систему защиты. Архитектура систем x86 поддерживает несколько уровней защиты исполняемых программ, предоставляемых процессором. Данные уровни называют кольцами (ring). Переходы между кольцами отнимают много времени и системных ресурсов. Поэтому для повышения быстродействия и снижения числа ошибок в Windows 98 используют только два кольца, а именно Ring 0 и Ring 3.